ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of

Cédric Laurant, Policy Counsel
Electronic Privacy Information Center

Public Workshop on Public/Private Partnerships
to Combat Cross-Border Fraud

Panel

Potential Partnerships among Consumer Protection Enforcement Agencies and ISPs and Web Hosting Companies

Before the

Federal Trade Commission

February 19-20, 2003
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC supports the Federal Trade Commission ("FTC")'s efforts to promote better cross-border enforcement of consumer fraud and launch an initiative that tries to improve cooperation between law enforcement, consumer protection agencies, the private sector, and consumer and other public interest groups.

EPIC and TACD encourage this FTC workshop as a step in the right direction

International consumer coalitions such as the Trans Atlantic Consumer Dialogue ("TACD")[1] have encouraged the FTC to address the issue of cross-border fraud. In July 2002, FTC Commissioner Mozelle Thompson testified that the FTC was working with the Organization for Economic Cooperation and Development ("OECD") and the International Marketing Supervision Network ("IMSN") and FTC's international counterparts to develop a common understanding of what constitutes core consumer protections and to work on cross-border fraud.[2] At the 5th annual TACD meeting in October 2002, both the US and EU governments agreed that it was important to develop new tools, e.g., by legislative cross-border enforcement, to fight spam at an international level. They expressed their willingness to work together towards this goal. On October 31, 2002, FTC Chairman Muris presented FTC's new plan for attacking cross-border fraud and stated that the FTC would advocate the adoption of an OECD Recommendation on cross-border fraud and seek legislative changes to improve the FTC's ability to fight it.[3] In a November 2002 resolution, TACD urged the US and the EU to protect consumers from fraud and serious deception across borders[4]. In a 2001 report, the OECD has recognized that, when governments face difficulties in defining and enforcing traditional geographically based jurisdictional boundaries, many consumer protection issues can be effectively addressed through international consultation and cooperation[5]. EPIC is delighted to see that the FTC is now addressing the issue of cross-

[1] TACD is a forum of 45 EU and 20 US consumer organizations which develops and agrees joint consumer policy recommendations to the US government and European Union to promote the consumer interest in EU and US policy making. *See* http://www.tacd.org.

[2] Testimony of FTC Commissioner Mozelle W. Thompson In Support of FTC Reauthorization before the Senate Committee on Commerce, Science and Transportation Subcommittee on Consumer Affairs, Foreign Commerce and Tourism ("Mozelle W. Thompson's Testimony"), July 17, 2002, http://www.ftc.gov/os/2002/07/mwtreauthtest.htm (last visited Feb. 10, 2003).

[3] FTC, *FTC Chairman Muris Presents the FTC's New Five-Point Plan For Attacking Cross-Border Fraud and Highlights Links Between Competition and Consumer Protection*, October 31, 2002, http://www.ftc.gov/opa/2002/10/fordham.htm (last visited Feb. 19, 2003).

[4] TACD, Resolution on Protecting Consumers From Fraud and Serious Deception Across Borders, Nov. 2002, http://tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=179.

[5] Organization for Economic Cooperation and Development, Directorate for Science, Technology and Industry, Committee on Consumer Policy, "Cross-Border Cooperation in Combatting Cross-border Fraud: The US/Canadian Experience,"

border fraud by organizing this workshop and focusing it on enforcement at an international level.

The FTC has a compelling interest in protecting consumers' privacy

The FTC's main duty is to protect consumers' interests. The FTC has several times showed in the past that it was willing to address consumer protection issues on an international level if it was vital to protect American consumers. Protecting consumers' interest implies safeguarding their privacy, particularly when their personal information is being transferred across borders. The FTC has often advocated that effective protection of consumers' privacy enhances consumer trust and that "consumer confidence is a necessary element for the global marketplace to thrive."[6] In its efforts to fight against consumer fraud, the FTC should, as a result, be particularly sensitive to privacy concerns.

The OECD Privacy Guidelines should be taken into account when the FTC addresses cross-border fraud enforcement efforts

EPIC supports FTC's efforts, especially if they can adequately articulate the protection against consumer fraud and consumers' privacy interests. In that regard, TACD has developed guidelines addressing cross-border enforcement. TACD has recommended that US and EU governments provide effective methods of obtaining redress for victims of cross-border fraud and serious deception, and that the OECD Privacy Guidelines be taken into account when promoting new solutions and better cooperation among law enforcement authorities. It particularly urged the US and EU governments to "actively promote the implementation of OECD guidelines to countries around the world"[7] in order for consumers everywhere to be protected from cross-border fraud.

It is worth emphasizing that the FTC played a critical role in the drafting of the OECD Privacy Guidelines and that it is currently actively engaged in working with the OECD on releasing a recommendation on governmental cooperation to protect consumers from fraudulent and deceptive commercial practices[8]. As the FTC has showed such commitment to protect privacy, it should therefore seriously consider the benefits the OECD Guidelines could bring to a supranational framework of cross-border fraud enforcement.

---

http://www.olis.oecd.org/olis/2000doc.nsf/c5ce8ffa41835d64c125685d005300b0/c125692700623b74c12569eb0059aec6/$FILE/JT00102297.PDF, p. 2 (last visited Feb. 10, 2003).

[6] Mozelle W. Thompson's Testimony, http://www.ftc.gov/os/2002/07/mwtreauthtest.htm (last visited Feb. 10, 2003).

[7] TACD, Resolution on Protecting Consumers From Fraud and Serious Deception Across Borders, DOC No. INTERNET-28-02 (Nov. 2002), http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=179 (last visited Feb. 10, 2003).

[8] FTC, *FTC Cross-Border Fraud Workshop to Address Trends, Partnerships*, February 19, 2003, http://www.ftc.gov/opa/2003/02/crossborder.htm.

More sharing of personal data among law enforcement agencies may increase the risk of identity theft

Identity theft is one of the most important consumer protection concerns facing the FTC today. The FTC has stated that consumers need to minimize the amount of information they share with businesses to reduce the risk that their personal information be stolen.[9] The FTC recommends that consumers adopt preventive steps (like checking credit history reports with credit scoring bureaus, opting-out of direct marketing schemes, refusing to disclose unnecessary information to banks, ISPs or government agencies,…) that ensure that their personal information is less likely to be abused by identity thieves, and by having recourse to available consumer protection laws.[10]

These recommendations show that the protection of consumers from identity theft is achieved by minimizing the information that one discloses to businesses and governmental agencies, and by developing regulations that protect consumers from unwarranted use of this information.

The same principles are applicable in the case of consumers' personal information that is used in the context of cross-border fraud investigations. If the FTC considers fighting against consumer fraud by facilitating cooperation and sharing of personal information between domestic and foreign law enforcement authorities and consumer protection agencies, the information that is shared between those authorities should be minimized to what is necessary to achieve effective enforcement. The FTC should therefore be keenly aware that, when establishing cross-border fraud enforcement guidelines, the sharing of consumers' personal information should be implemented by taking into account its potential for increasing the risk of identity theft and abuse.

Cross-border sharing of consumers' personal data decreases the national legal privacy safeguards and remedies consumers usually benefit from

Data that travels across borders does not always enjoy the protection it has when it only circulates at a national level, where consumers have more available and affordable means of seeking judicial or administrative redress with their national governmental agencies.

In order to address the various concerns raised above, EPIC makes the following general recommendations.

---

[9] *See, e.g.*, *FTC, Minimize your Risk*, http://www.consumer.gov/idtheft/risk.htm (last visited Feb. 19, 2003).
[10] FTC, *ID Theft: When Bad Things Happen To Your Good Name*, September 2002, http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf (last visited Feb. 19, 2003); FTC, *Privacy: Tips for Protecting Your Personal Information*, January 2002, http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.htm and http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.pdf (last visited: Feb. 19, 2003).

EPIC's general recommendations

1. The OECD Privacy Guidelines should be taken into account when promoting new solutions and better cooperation among domestic and foreign law enforcement authorities and their use and sharing of personal information for consumer fraud investigation purposes.

For governments to rely on very diverse national laws to guarantee that consumers' privacy will be protected is not enough to ensure an effective transnational cooperation in cross-border fraud cases. For the United States to only rely on US privacy rules to assure foreign countries that the privacy of their national consumers is safe in US law enforcement authorities' hands is probably idealistic. Cooperation between a few, mostly English-speaking, countries is a good step towards better enforcement of transnational consumer fraud cases, but it is not sufficient to prevent cross-border fraud taking place in other countries. This is why it seems necessary to rely on an international framework of privacy rules that would apply to any transfer of consumers' information collected for the purpose of cross-border fraud investigations.

The OECD Guidelines offer the best privacy framework to rely upon for cross-border transfer of consumer information. The Guidelines' principles, since their release in 1980, and notwithstanding their non-binding character, have been implemented in many countries' privacy laws.[11] They were adopted to prevent the danger that "disparities in national legislations could hamper the free flow of personal data across frontiers"[12] and to help harmonize national privacy legislation.

Partnerships and data sharing cooperation between US and foreign law enforcement agencies, governmental consumer protection agencies and the private sector against transnational consumer fraud could best be achieved if all actors were able to refer to a common set of privacy rules protecting their consumers the same way no matter where their personal data would be transferred to.[13]

This means, in practice, that some of the Guidelines principles could be incorporated into the various Memoranda of Understanding ("MOUs") signed between the United States and foreign countries that regulate the cooperation and sharing of

[11] Cfr EPIC and Privacy International, *Privacy and Human Rights* (2002), *available at* http://www.privacyinternational.org/survey/phr2002/.

[12] Preface of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines") (1980), http://www1.oecd.org/publications/e-book/9302011E.PDF (last visited Feb. 10, 2003). *See generally*, MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 324-52 (EPIC 2002) (Hereinafter "EPIC PRIVACY LAW SOURCEBOOK 2002").

[13] The OECD Guidelines provide in this regard a few recommendations for their implementation by recommending that Member countries should co-operate in the implementation of the Guidelines and agree on specific procedures of consultation and cooperation for their application.

information between law enforcement and consumer protection agencies.[14] Where MOUs provide for the creation of consumer fraud-related databases[15] for enforcement authorities, the confidentiality of information pertaining to consumer complaints should be protected. This could be done by providing appropriate remedies to people whose personal data is disclosed in violation of MOUs, and by establishing adequate penalties for breach of the confidentiality of their data, especially when it is sent abroad, pursuant to the Accountability and Security Safeguards Principles of the Guidelines.[16] Nothing in the MOUs currently provides for such penalties and remedies. If more cooperation is requested among law enforcement agencies and more sharing of consumer information is to take place, the consumers who provide data that is used for consumer fraud investigations deserve more confidentiality for their personal information.

The OECD Guidelines could also be implemented in MOUs or other multilateral data sharing cooperation agreements by:

- Providing that the amount of personal information that can be collected, used, shared, and, more generally processed by law enforcement, consumer protection agencies and the private sector, has to be systematically *minimized* according to what is strictly required for the investigation and relevant to the purposes for which the information is to be used.[17]

---

[14] Some of those MOUs include the *Memorandum of Understanding on Mutual Enforcement Assistance in Consumer Protection Matters Between the Federal Trade Commission of the United States of America and Her Majesty's Secretary of State for Trade and Industry and the Director General of Fair Trading in the United Kingdom* (October 31, 2000), http://www.ftc.gov/os/2000/10/ukmemo.pdf (last visited Feb. 10, 2003), and the *Memorandum of Understanding Among Certain Members of the International Marketing Supervision Network and Affiliated Agencies on Participation in the "econsumer.gov" Pilot Project* (April 24, 2001), http://www.ftc.gov/os/2001/04/econsumermou.htm (last visited Feb. 10, 2003).

[15] The "Consumer Sentinel Network information" is one of them. It was created in April 2001 by the *Memorandum of Understanding Among Certain Members of the International Marketing Supervision Network and Affiliated Agencies on Participation in the "econsumer.gov" Pilot Project*, and is maintained by the FTC and is made up of two databases: the "Consumer Sentinel" database, which stores consumer complaint data and other investigatory information provided by consumers, participating law enforcement agencies, and other contributors about consumer fraud and deception, and the "Identity Theft Data Clearinghouse", which is an automated database that stores investigatory information provided by consumers, participating law enforcement agencies, and other contributors about identity theft, http://www.ftc.gov/os/2001/04/econsumermou.htm (last visited Feb. 10, 2003). See also *United States and Twelve Countries Unveil e-consumer.gov*, April 24, 2001, http://www.ftc.gov/opa/2001/04/econsumer.htm (last visited Feb. 10, 2003).

[16] The Security Safeguards Principle provides that "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data" and the Accountability Principle provides that "A data controller should be accountable for complying with measures which give effect to the [other] principles", OECD Privacy Guidelines, http://www1.oecd.org/publications/e-book/9302011E.PDF (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 327.

[17] Following in this the OECD Guidelines' Data Quality Principle ("Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date") and Purpose Specification Principle ("The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose"), OECD Guidelines on the Protection of Privacy and

- Ensuring that the transborder flows of personal data are "uninterrupted and secure"[18], i.e. that they provide for sufficient security safeguards against unlawful access and interception, disclosure or abuse.

2. The FTC should establish appropriate oversight mechanisms aimed at addressing the new risks for consumers' privacy of transnational sharing of personal information for law enforcement purposes in the context of consumer fraud investigations.

Better oversight could be done by:

- developing a set of minimal reporting requirements, such as the recording of the type of data shared with domestic and foreign law enforcement and consumer agencies, and the disclosure of aggregate statistical data;

- the issuance of an annual report to Congress and the public that would evaluate the effectiveness of cross-border consumer fraud investigations; whether increased sharing of data and facilitated access have contributed or not to more efficient fraud investigations; how the data is used by the actors involved and how useful it is in investigations; whether the increased sharing of consumers' personal information contributes to identity theft.

3. Consumers should have legally enforceable remedies in those cases where the confidentiality of their personal information has been breached.

This would more particularly apply in the case of cross-border transfers of data since the Privacy Act[19] does not protect the personal information of non-US citizens held by US law government agencies. If foreign consumers have to entrust their data with US law enforcement agencies for the purpose of cross-border consumer fraud investigation, they should also get appropriate remedies equivalent to the ones available to US consumers. Giving them such remedies would, as a result, foster more trust of US citizens in having their own personal data transferred abroad in the context of a consumer fraud investigation, and, as a result, enhance cooperation between law enforcement authorities.

Transborder Flows of Personal Data (1980), http://www1.oecd.org/publications/e-book/9302011E.PDF (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 327.

[18] To follow OECD Guidelines' Security Safeguards Principle ("Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data") and Principle 16 ("Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure"), *id., cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 328.

[19] Privacy Act (1974), Public Law 93-579, 5 USC par. 552, http://www4.law.cornell.edu/uscode/5/552.html (last visited Feb. 10, 2003).

This would entail changing the language of some MOUs signed between the United States and foreign countries in order to provide for a *sui generis* right of relief for consumers whose privacy has been breached.

Specific questions

The Federal Trade Commission has asked us to provide comments on specific issues.

What are the record retention policies for foreign ISPs? Are there foreign regulations imposing record retention requirements? Could the retention policies be lengthened? Why not? Is there a way the FTC can ask a foreign ISP to preserve evidence? Why or why not? Are there regulations that govern?

In Europe, the legal framework that governs law enforcement access to foreign ISPs/web hosting companies' personal data[20] recognizes as its foremost principle people's right to privacy and secrecy of their correspondence.

The processing of personal data by ISPs and web hosting companies' data is regulated by two data protection directives[21] and, at the national level, by data protection laws implementing the EU directives. The Directive 2002/58, which applies data protection principles to electronic communications[22] data, generally ensures that the confidentiality of communications (including traffic data[23]) will be protected, and particularly prohibits listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data, by persons other than users and without their consent.[24] The Directive prohibits, as a general rule, the processing[25] of

[20] 'Personal data', as defined by Article 2 (a) of the Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with regard to the processing of Personal Data and on the Free Movement of such Data ("Data Protection Directive"), means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity", http://www.europa.eu.int/comm/internal_market/en/dataprot/law/index.htm (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 378.

[21] Data Protection Directive, *id.*, and Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ("Directive on Privacy and Electronic Communications"), http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 415.

[22] " 'Communications' means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information." Article 2(d), Directive on Privacy and Electronic Communications, *id.*

[23] " 'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". Article 2(b), Directive on Privacy and Electronic Communications, *id.*

[24] Article 5, Directive on Privacy and Electronic Communications, *id.*

traffic and location data[26] when they are no longer needed for the purpose of the transmission of a communication. Personal data can still be processed for billing purposes, but for no longer than is required for that purpose, and for marketing purposes, but on an opt-in basis.[27] However, Member States have the possibility, when implementing the EU Directive, and as an exception to the general principle of confidentiality, to restrict the protection users afford when they can show it is necessary, appropriate and proportionate to safeguard a limited number of values (national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of an electronic communications system).[28] To this end and on the same grounds, they may provide for the retention of data[29] for a limited period for the benefit of law enforcement authorities.

At the level of EU Member States, some countries have already started to provide for mandatory data retention regimes varying from a few weeks to 12 months. Others are considering whether retention is justified at all, while some others currently only provide for the preservation[30] of data.[31]

The crucial issue in the ongoing debate in Europe about the possibility to compel ISPs and web hosting companies to retain all their customers' data for fixed periods is not whether it is better to have a uniform regime applicable throughout Europe to the interception of data by law enforcement, but whether data retention is itself legitimate and compatible with international human rights instruments[32]. Many experts have

---

[25] 'Processing of personal data' ('processing') means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Article 2 (b), Data Protection Directive, http://www.europa.eu.int/comm/internal_market/en/dataprot/law/index.htm (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 378.

[26] " 'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Article 2 (c), Directive on Privacy and Electronic Communications, http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 425.

[27] *See* Articles 6 and 9, Directive on Privacy and Electronic Communications, *id.*, *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 427-8.

[28] Article 15 (1), Directive on Privacy and Electronic Communications, *id.*, *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 431.

[29] Data retention can be defined as the systematic and mandatory storage of large categories of data for a specified period.

[30] Data preservation refers to the storage for a specified period of time of specific data related to a particular criminal investigation of a specified individual, accessed according to legal and constitutional safeguards and subject to judicial review.

[31] *See* Council of the European Union, *Answers to questionnaire on data retention* (November 20, 2002) http://blubb.at/kuhm/temp/20112002tidy.html (last visited Feb. 10, 2003). (This document gathers EU Member States' comments with respect to the regulation, practice and experiences of traffic data retention in each EU country.)

[32] Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950), http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 321; Article 12 of the Universal Declaration of Human Rights (1948), http://www.un.org/Overview/rights.html (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY

asserted[33] in that regard that the principle of data retention may itself be in violation with the right to privacy as it is enshrined in the European Convention on Human Rights ("ECHR")[34] and further elaborated by the European Court of Human Rights. It is worth noting that the idea of a EU-wide uniform and mandatory data retention scheme that the European Council would propose every Member State to implement into their national legal system[35] prompted the European Data Protection Commissioners to strongly criticize that idea, and to implicitly recommend that the data preservation regime be kept, or that retention be strictly limited to short periods, and mandated only where it is necessary and appropriate.[36] Other serious barriers to implementing a data retention

---

LAW SOURCEBOOK 2002 at 314; Article 8 of the Charter of Fundamental Rights of the European Union. http://www.europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf (last visited Feb. 10, 2003).

[33] Working Party on the Protection of Individuals with regard to the processing of personal data ("Working Party Article 29"), Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime (March 22, 2001), http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm (last visited Feb. 10, 2003), *cited in* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 403-412 (EPIC 2001) (Hereinafter "EPIC PRIVACY LAW SOURCEBOOK 2001"); Working Party Article 29, Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385 (Nov. 2, 2000), http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp36en.pdf (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2001 at 432; Working Party Article 29, Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes (September 7, 1999), http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp25en.pdf (last visited Feb. 10, 2003), *cited in* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 468-474 (EPIC 2000) (Hereinafter "EPIC PRIVACY LAW SOURCEBOOK 2000"; Letter from Stefano Rodotà (Chairman of the Working Party Article 29) to Mr. Göran Persson (Acting President of the Council of the European Union) (June 7, 2001), at http://www.statewatch.org/news/2001/jun/07Rodota.pdf (last visited Feb. 10, 2003); Global Internet Liberties Campaign ("GILC")'s letter to Prime Minister Guy Verhofstadt, President, EU Council of Ministers (November 12, 2001), http://www.gilc.org/verhofstadt_letter.html (last visited Feb. 10, 2003); GILC, Open letter to Pat Cox, President of the European Parliament (May 22, 2002), http://www.gilc.org/cox_en.html (last visited Feb. 10, 2003).

[34] Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950), http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (last visited Feb. 10, 2003), *cited in* EPIC PRIVACY LAW SOURCEBOOK 2002 at 321.

[35] Statewatch, *Europol document confirms that the EU plans a 'common EU law enforcement viewpoint on data retention'*, May 18, 2002, http://www.statewatch.org/news/2002/may/18europol.htm (last visited Feb. 19, 2003); Richard Norton-Taylor and Stuart Millar, *Privacy fear over plan to store email*, The Guardian, August 20, 2002, http://media.guardian.co.uk/Print/0,3858,4484984,00.html (last visited Feb. 19, 2003); *Plan to store e-mail and phone data for two years*, Financial Times, August 21, 2002, http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1028185913365&p=1012571727166# (last visited August 22, 2002); Lee Dembart, *The End User Rights at risk*, International Herald Tribune, September 30, 2002, http://www.iht.com/cgi-bin/generic.cgi?template=articleprint.tmplh&ArticleId=72222 (last visited Feb. 19, 2003).

[36] "Where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case." Statement of the European Data Protection Commissioners on data retention. September 11, 2002, http://www.fipr.org/press/020911DataCommissioners.html (last visited Feb. 10, 2003).

regime lie in the tremendous technical and data retention management costs that ISPs and web hosting companies, and eventually consumers, would have to bear.[37]

Not only are legality and cost issues at stake in the data retention debate. It is also the growth of e-commerce that will be stalled if consumers have to bear the burden of the implementation of retention schemes. Their confidence in using the Internet to chat, communicate, purchase, sell, or otherwise carry out daily their online activities, is likely to be undermined if the vast amount of personal data that is retained is later subject to abuses.

If extensive sharing of data is to take place between US and EU law enforcement in the context of cross-border fraud investigations, it is not only Europeans' privacy which is at risk, but also Americans'. There is a significant risk that US law enforcement agencies will seek data stored in Europe (including data of Americans stored on servers located in the EU) that it could not obtain at home, either because it was not retained or because US law would not permit law enforcement access.

The amount of information that would be retained would cover data as sensitive as medical information, information revealing political opinions, religious, philosophical beliefs or sexual life that would otherwise be destroyed upon the completion of its intended use, and that would hardly have been collected in an offline context. This creates new privacy and security risks for citizens that far outweigh the benefits that collecting such information can bring for law enforcement. Data is likely to be misused by law enforcement, particularly because of the risk that authorities could be tempted to use their powers to conduct broad and arbitrary "fishing expeditions." Data retention, if implemented on a wide scale and through the use of sophisticated data mining tools would have the potential to reveal a surprisingly detailed image of a person's life.[38] New

[37] A recent report by a British parliamentary committee shows that one-year data retention, if implemented, would be impractical, that the costs have been underestimated and that the ISP and telecommunications industry have few incentives to implement any technical changes, not to mention the fact that the retention scheme appears to be in breach of the U.K. Human Rights legislation (which itself implements into British law the European Convention on Human Rights) (January 2003), http://www.apig.org.uk/APIGreport.pdf (last visited Feb. 10, 2003). A Canadian report considered the huge storage capabilities that ISPs would have to deploy and the uncertainty of associated costs if they had to implement data retention schemes: "(…) The average Internet customer produces between three to five gigabytes of traffic and message data per month. A small ISP with only 10,000 customers would need 300 terabytes of storage capacity to meet a traffic data retention requirement of six months. The EU proposals seeking retention for two years boost that storage need to the pica-byte range." *See* Lawrence Surtees and Warren Chaisatien, *Caught in the Web: Ottawa's Implementation of Cyber-crime Treaty Requires Online Surveillance by xSPs*, p. 23, http://www.idc.com/getdoc.jhtml?containerId=CA050TLJ&sectionId=tableofcontent&pageType=SECTION (last visited Feb. 19, 2003).

[38] *See, e.g.*, G8 Justice and Interior Ministers' Meeting in Mont-Tremblant (Canada), *Principles on the Availability of Data Essential to Protecting Public Safety*, 2002, http://www.g8j-i.ca/english/doc3.html (last visited Feb. 10, 2003) (this document sets out the data that the G8's law enforcement authorities would like to get access to and consider as traffic data; and Europol, *Expert meeting on cyber-crime: Data Retention*, April 11, 2002, http://www.gilc.org/europol.pdf (last visited Feb. 10, 2003) (this document details the type of traffic and localization data that Europol want EU law enforcement authorities to obtain from ISPs and telephone companies). *See also Europol document confirms that the EU plans a "common EU law*

retention requirements will create "new risks to personal privacy, political freedom, and public safety."[39]

Data retention is also very likely to threaten users and consumers' confidence in the Internet. If Internet users were told that everything they do online, all the data that is being generated by their surfing, purchases, and chatting is being preventively recorded for a long period (from a few months to a few years), they would probably react the same way as mail users would react to a requirement that every letter they send be identified with as much information as the sender's name, his or her credit card, the contents of the package, the time of posting, a writing sample of their signature, etc. Not only does the preventive retention of data of every Internet user contradict the criminal law principle that everyone is considered innocent until proven guilty, but it is also likely to indirectly chill speech occurring online.

What are the record retention policies for domestic ISPs? Could these be lengthened? Why not?

The interception regime of electronic communications in the United States is based on a "data preservation" framework, as opposed to "data retention". Where data preservation refers to the storage for a specified period of time of specific data related to a particular criminal investigation of a specified individual, accessed according to legal and constitutional safeguards and subject to judicial review[40], "data retention" instead can be defined as the systematic and mandatory storage of large categories of data for a specified period. Only a data preservation regime is permitted under U.S. law, and data retained under such regime is subject to statutory minimization requirements that limit the data collected and the uses to which such information can be put.[41]

US law does not mandate data retention. The US government has indeed always strongly opposed data retention.[42] Even though many providers routinely retain limited traffic data for billing or marketing purposes on a short-term basis, there are currently no government-imposed data retention requirements in any of the major industrialized

---

enforcement viewpoint on data retention, May 18, 2002, http://www.statewatch.org/news/2002/may/18europol.htm.

[39] *See* GILC's Open letter to Prime Minister Guy Verhofstadt (President, EU Council of Ministers), Nov. 12, 2001 (in response to US President George W. Bush's October 16, 2001 letter to Mr. Romano Prodi (President of the Commission of the European Communities)), http://www.gilc.org/verhofstadt_letter.html (last visited Feb. 19, 2003).

[40] *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 USC par. 2510 *et seq.*

[41] *See id.* Par. 2518.

[42] Comments of the United States on the European Commission Communication on Combating Computer Crime, presented at the European Union Forum on Cyber-Crime at Brussels (Nov. 27, 2001) at http://www.usdoj.gov/criminal/cybercrime/intl/MMR_Nov01_Forum.doc (last visited Feb. 10, 2003) ("The United States has serious reservations about broad mandatory data retention regimes and has articulated these reservations in multilateral for a such as the Council of Europe Cyber-Crime Convention negotiations and the G8.").

countries.[43] Furthermore, the recently enacted USA PATRIOT Act[44] does not provide for any data retention requirements, probably because the Department of Justice and security agencies did not think that retaining all communications preventively would be necessary to combat terrorism.

How can public-private cooperation between law enforcement agencies, ISPs, and web hosting companies be improved? What are some constraints on cooperation, and how can these constraints be overcome?

A uniform interception regime of ISPs' data would probably improve the cooperation between Member State law enforcement authorities and their foreign counterparts in the combat against online consumer fraud. Such a regime, because of its uniformity, would have to be respectful of the highest level of privacy available to consumers in any of the countries participating to law enforcement cooperation agreements.

We recommend that the FTC, because its goal is to foster consumer confidence in the electronic commerce marketplace while protecting American consumers' privacy, should only co-operate with law enforcement authorities that do not obtain data through data retention schemes. If US and EU law enforcement authorities intend to improve their cross-border cooperation on consumer fraud cases, it ought not to be done at the expense of consumers' privacy.

* *
*

Consumers expect consumer protection agencies to investigate fraud, deceptive and unfair marketing practices. In some circumstances, consumers provide personal information for complaints that can result in better enforcement of consumer protection laws. However, they also expect that their data will not be misused and that their privacy will be safeguarded.

EPIC has, in that regard, proposed a set of recommendations to ensure that privacy, as a right, is adequately protected with law enforcement's legitimate concerns for protecting consumers from fraud. Even if consumer protection against fraud is an important value to take into account, consumer privacy is another one that deserves equal consideration. Protecting both values, by adopting rules that allow for improved and

[43] *See, e.g.*, the Council of Europe Convention on Cyber-Crime that only permits the *preservation*, and not *retention*, of data, ETS No. 185, *opened for signature* Nov. 23, 2001, http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1&DF=13/02/03 (last visited Feb. 10, 2003). The Convention is not in force, but has been signed by the United States government in November 2001.

[44] USA-PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), also available at http://www.epic.org/privacy/terrorism/hr3162.html (last visited Feb. 10, 2003).

more effective law enforcement while, at the same time, being respectful of consumers' privacy interests, should be FTC's main task.

EPIC remains committed to educate the public about the privacy issues related to cross-border fraud and, therefore, welcomes the opportunity to develop with the Federal Trade Commission and other governmental consumer protection agencies effective ways to combat fraudulent practices while developing the appropriate tools and legal frameworks to protect consumers' privacy.

Respectfully submitted,

Cédric Laurant
Policy Counsel
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009 – U.S.A.