Testimony and Statement for the Record of

Marc Rotenberg
Electronic Privacy Information Center, Executive Director
Georgetown University Law Center, Adjunct Professor

Hearing on
Consumer Fraud,
the International Consumer Protection Enforcement Act of 2003,
and FTC Reauthorization

Before the

Subcommittee on Competition, Foreign Commerce, and Infrastructure
Committee on Commerce, Science and Transportation,
United States Senate

June 11, 2003
253 Russell Senate Office Building

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today regarding consumer fraud and the reauthorization for the Federal Trade Commission. My name is Marc Rotenberg and I am the executive director of the Electronic Privacy Information Center (EPIC). EPIC works with a wide range of consumer and civil liberties organizations both in the United States and around the world.

I would like to begin by thanking the Committee for focusing on the issue of cross-border fraud. One of the consequences of the rapid growth of the Internet has been the dramatic expansion of both commercial opportunity online and of commercial fraud. It is clearly in the interests of businesses and consumers to ensure a stable, growing, and fair online marketplace. Fraudulent and deceptive business practices that would otherwise be prosecuted in the United States should not be beyond the reach of United States law enforcement simply because an operator sets up shop outside the country. In similar fashion, government agencies seeking to protect the interests of consumers in their jurisdictions should expect the cooperation of the Federal Trade Commission when cross-border problems emerge.

I would also like to thank the FTC Chairman and the other members of the Commission for their efforts to address this new challenge and for the workshop in February that provided a wide range of important perspectives on this topic. Chairman Muris outlined the plan to pursue cross-border fraud in November of last year. He said that the FTC would advocate the adoption of a recommendation of the Organization for Economic Cooperation and Development (OECD) on cross-border fraud and would seek appropriate legislation. Commissioner Thompson, working through the International Marketing Supervision Network and in cooperation with the FTC's international counterparts, has helped develop a common understanding of what constitutes core consumer protection in the international realm.

The February workshop, organized by the FTC, set out the views of consumer and privacy organizations, businesses and foreign agency officials. Chairman Muris noted that cross-border complaints by US consumers rose from 13,905 in 2001 to 24,313 in 2002. Canadian consumers also report a near doubling of complaints with online commerce between 2001 and 2002. The *Consumer Sentinel*, the FTC's central complaint database, records over 72 million dollars lost by U.S. consumers to cross-border fraud in 2002, nearly seventeen percent of all money lost to fraud. According to the FTC, 68% of all fraudulent foreign money offers come from companies located in Africa; 41% of fraudulent advance-fee loans come from Canadian companies, and 61% of fraudulent prize and sweepstakes offers are from companies located in Canada.

There was consensus at the February FTC workshop on the need to tackle the problem of cross-border fraud and to enable better cooperation between the FTC and its counterparts. The FTC proposal grows out of the work of the February meeting, the OECD, and the continued efforts to promote international cooperation.

EPIC has a particular interest in the protection of consumers in the global economy. We have successfully pursued privacy complaints on behalf of consumers under Section 5 of the FTC Act that have international implications. For example, our earlier work on the privacy implications of Microsoft Passport, the online authentication scheme, was considered favorably by both the Federal Trade Commission and the European Commission. EPIC also work closely with consumer and civil liberties organizations on the development of international policy. In particular, the Trans Atlantic Consumer Dialogue (TACD), a coalition of sixty consumer organizations in the United States and Europe, has urged officials on both sides of the Atlantic to address this challenge. Similar views have been expressed by consumer organizations in other parts of the world. We have also worked with the OECD for more than a decade, in areas such as privacy protection, consumer protection, cryptography, and electronic commerce, to promote the development of policies that promote economic growth and safeguard democratic values. We are pleased that these efforts have come together in the current proposal before the Committee to combat cross-border fraud.

In the statement today, I will recommend passage of legislation that will enable the Federal Trade Commission to work more closely with consumer protection agencies in other countries to safeguard the interests of consumers and users of new online services. Nevertheless, in creating these new enforcement authorities, there is a clear need to safeguard important legal safeguards that are central to the US form of government. In particular, certain provisions of the draft International Consumer Protection Enforcement Act, put forward by the FTC, should be revised to safeguard privacy, promote government accountability, and enable the development of reporting standards that will allow this Committee and the public to assess how well the FTC is doing its job and whether further steps may eventually be necessary. Without these changes, the legislation opens the door to abuse in that it creates new enforcement authority without corresponding safeguards. Civil liberties groups in both the United States and Europe have already expressed strong opposition to a proposal of this type that was put forward by the Council of Europe to combat cyber crime.

It is particularly important to understand that when the United States provides information about consumers and business in the United States to foreign law enforcement agencies it opens the door to prosecution that may not satisfy the substantive requirements or safeguard the procedural rights that would be available in this country.

SPECIFIC PROVISIONS IN THE FTC PROPOSAL

Information Disclosure to Foreign Governments (Sections 3 and 4)

We recognize that the cross border enforcement of consumer fraud will require cooperation between the FTC and sister agencies in other jurisdictions. To some extent, the sharing of information between agencies will be necessary to pursue violators and enforce judgments. At the same time, it is critical to ensure that only the necessary

information is disclosed and that appropriate safeguards are established when such information is disclosed.

In our view, the FTC proposal creates too few restrictions on the disclosure of information concerning individuals and entities within the United States. One particular provision is simply offensive. A proposed amendment to Section 6 of the FTC Act that enables the FTC to assist foreign law enforcement agencies states that "such assistance may be provided without regard to whether the conduct identified in the request would also constitute a violation of the laws of the United States."

This provision further should be removed. We further recommend that the disclosure be only to "appropriate" foreign agencies, not "any" foreign agency as is currently specified in the bill, and we urge the FTC to post the names and contact information for any foreign agency that it considers appropriate to receive information. Not only should the FTC share information with appropriate agencies, it should share information only at appropriate times and in connection with a specific investigation. The Custom Service, for example, limits the exchange of information and documents with foreign customs and law enforcement to those instances where the Commissioner "reasonably believes the exchange of information is necessary . . ." 19 C.F.R. sect. 103.33. The FTC should not permit disclosures to any foreign government agency where the public and concerned parties cannot readily identify the agency.

We further recommend the recognition of a dual criminality provision to ensure that the United States assists in the prosecution of individuals and entities within the United States only in those circumstances where the crime charged would also be a crime under United States law. Absent such a provision, it is conceivable that a bookseller or music publisher in the United States could be subject to prosecution under foreign law where such government does not provide for strong protections for freedom of expression. This problem could arise in particular with publications that criticize state governments.

Amendments to US Privacy Statues (Sections 6 and 7)

The FTC legislative proposal would amend two critical US privacy statutes to reduce the likelihood that the target of an investigation would be notified of the investigation. In particular, the International Consumer Protection Enforcement Act would amend the Electronic Communications Privacy Act, and the Right to Financial Privacy Act. But the arguments for denying notice to the target of an investigation could too easily be made with respect to targets in the United States. The proposed changes here not only set a bad precedent but would also send a bad message to consumer protection agencies in other countries about the conduct of investigative actions by democratic governments.

We recommend that the provisions that reduce procedural safeguards be removed.

Disclosure of Financial Information (Section 8)

This provision would give the FTC authority to access financial bank reports and other financial data under the guise of fighting against cross-border consumer fraud and deception. However, there are no reporting or notification requirements that record the exchange of information; there are no audit provisions that oversee the exchange of the information; there is no limit on who within the authorized agencies can exchange information, and there is no limit on what the content of the reports, records or other information shall consist off.

These provisions make it too easy for the listed agencies to share financial information. The provision would give the FTC discretion to share financial information without any oversight to make sure it is shared appropriately. This discretion leaves the exchange of information open to abuse. Moreover, there is no limit on what sort of information can be exchanged. There is no provision that states that records or information cannot consist of information identifiable to a particular customer. In this way, the authorized agencies could examine records about customers of financial institutions, without notification requirements, under the guise of examining records regarding the financial condition of the institution.

Although the objective of the proposed amendment, to ease the sharing of information amongst agencies involved in protecting consumers against fraud, is laudable, the amendment should include provisions that ensure that personal financial information is shared in an accountable and transparent manner. Acknowledging the FTC's desire to be able to share information appropriate to real-time law enforcement needs, the following additions to the amendment may be appropriate:

- a provision that information exchanged under 1112(e) cannot contain information identifiable to any one individual without triggering a reporting requirement.
- a provision that a designated official at the authorized agencies have a log of all personal information that is exchanged under 1112(e).
- a provision that such a log is available to the public under FOIA, unless there is a compelling law enforcement reason to exempt it.

Adding such provisions would allow an appropriate amount of accountability into the information exchange process, while still allowing the FTC and the other listed agencies to have the flexible use of information for their law enforcement needs.

Freedom of Information Act Exemptions (Sections 5 and 7)

The FTC proposes to exempt itself from certain open record obligations under the Freedom of Information Act. We believe this change is unnecessary and, if enacted, will reduce government accountability.

The current FOIA exemptions for ongoing criminal investigation, § 552(b)(7)(A), and for the protection of confidential sources, (b)(7)(D), would likely prevent the

disclosure of information that the FTC seeks to protect without any further amendment. Moreover, three other exemptions may also apply to information collected by the Commission; the exemption for business information under § 552(b)(4); for personal privacy under § 552(b)(6); and for records of financial institutions under § 552(b)(8).

EPIC has already pursued an extensive FOIA request with the FTC involving the investigation of privacy complaints under Section 5 of the FTC Act. In that case, the FTC has demonstrated its willingness to apply the current statutory exemptions. Some of the information we sought concerning current matters was withheld. The FTC cited the (b)(7)(A) exemption.

Since the existing exemptions already provide adequate protection for the Commission, a new exemption is not necessary and only adds confusion to a long-standing statutory scheme that has been subject to judicial interpretation for almost thirty years. Therefore, we recommend that provisions to limit the application of the Freedom of Information Act be stricken from the FTC proposal, or at the least that a thorough analysis be done to determine whether the current exemptions combined with current case law are sufficient before any new exemption is created.

Access to Criminal Justice Records (Section 12)

Section 12 of the proposed Act would grant the FTC access to the National Crime Information Center, the nation's most extensive computerized criminal history database, following an agreement with the Attorney General to (A) establish the scope and conditions of the FTC's access to the database, and (B) establish the conditions for the use of the data. Section 12 would further permit the FTC to disclose NCIC data to foreign law enforcement agencies pursuant to procedures that require at least prior certification that such information will be maintained in confidence and will be used only for official law enforcement purposes.

While we recognize the interest that the FTC may have in accessing the NCIC record systems, there are three problems with this proposal. First, it was never anticipated that the FTC would have access to this record system and it was also never anticipated that the FTC could allow foreign law enforcement agencies access to this record system. This is precisely the type of mission creep that results from the creation of criminal justice databases lacking adequate statutory constraints that civil liberties groups on both the right and the left have opposed.

Second, this proposal to expand access to the NCIC follows just a few months after a decision by the FBI to exempt itself from the data quality obligations that would otherwise apply to this system of records under the 1974 Privacy Act. More than 90 organizations and 5,000 individuals across the United States expressed their opposition to this decision by the Bureau. The lack of data quality obligations for the NCIC increases the likelihood that individuals will be wrongly stopped and detained, perhaps even placed in dangerous law enforcement interdictions, because of errors in the most important criminal history record system in the United States that the Department of Justice no

longer feels obliged to keep accurate. The further expansion of NCIC use, while this issue remains unresolved, should be postponed until the data accuracy obligation is restored.

Finally, it is important to note, particularly in the context of transborder data flows that the NCIC record system does not meet all of the international standards for privacy protection. Most significantly, the proposal does not provide for access by the record subject to inspect and correct records concerning the individual. Further amendments may be necessary to enable first party access to NCIC records.

We recommend against providing the FTC with access to the NCIC until the data quality obligation is restored and some right of first party access to the record system is established. In the alternative, we would recommend revisions to the proposed bill that would add a new provision that would require the FTC to "establish with a high degree of confidence that the data obtained by the FTC from the NCIC is accurate." We further recommend that section 12 more accurately specify the purposes for which the FTC may use NCIC data. In particular, the FTC should be required to show that evidence gathered from the NCIC would likely reveal that the data subject has previously committed an act that would fall within the FTC's jurisdiction or that the data subject may have moved assets across national borders to avoid prosecution.

GENERAL RECOMMENDATIONS

Reporting

We recommend the creation of new reporting requirements that would focus specifically on the FTC's activities undertaken pursuant to this new legislative authority. There should be an annual report provided to the Congress and made available to the public at the web site of the FTC. This report should include such information as the number of complaints received during the past year, the number of investigations pursued, and the outcome of these investigations including whether any damages were assessed and whether any relief was provided to consumers as a result of the investigation. The report should also indicate which foreign agencies the FTC cooperated with and the nature of the information provided and the information received.

The FTC has already begun the process of making some of this information available with the Consumer Sentinel web site. Canada, Australia and the United States, have also established eConsumer project that helps provide similar information on the international front. While both projects are important, we believe that formalizing reporting requirements for investigations as well as complains will make it easier to assess how well the FTC and other agencies are responding to the challenges of cross-border fraud.

We would also urge the FTC to consider the creation of an advisory council for the major multilateral law enforcement groups, such as the International Consumer Protection and Enforcement Network, that would allow the participation for a US

consumer representative and a US business representative. Participation by representatives of the consumer and business community will help ensure oversight and reduce the risk of unaccountable activities.

International Privacy Framework

The OECD proposal for protecting consumers in the global economy is consistent with other efforts of the OECD to promote economic growth while safeguarding democratic values. In this spirit, we would like to underscore the need to ensure that new efforts undertaken by the United States in cooperation with other governments should be consistent also with the OECD recommendation on privacy protection. The FTC has already worked to ensure that principles similar to those contained in the OECD Privacy Guidelines were established for transborder data flows between the United States and Europe in the context of the Safe Harbor proposal. That arrangement allows US firms to enter European markets and process data on European consumers on the condition that they follow and enforce strong privacy standards.

We urge the adoption of a similar framework to regulate the transfer and use of personal information that will occur between national governments as they pursue joint investigations and prosecutions. Governments, no less than the private sector, should be held to high standards in their use of personal information, particularly because the misuse of such information may subject individuals to unfair and unfounded prosecutions.

Continued Focus in Privacy Issues in the United States

Even as the Federal Trade Commission pursues its efforts to address the challenge of crossborder fraud, it is important not to lose sight of the important work that must still be done in the United States to safeguard the interests of consumers. We commend the Commission for its leadership in the creation of a national telemarketing "Do-Not-Call" list, and for its victories for consumer privacy in the two Trans Union cases upholding protections in the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act.

However, as the top consumer watchdog in the government, the Commission must continue to set a high standard to protect individuals' privacy. The Commission only recognizes four Fair Information Practices (notice, choice, access, security) to evaluate individuals' privacy rights. This falls short of the standard set by the Privacy Act of 1974, which recognizes additional rights including use limitations, data destruction, and rights of correction. Internationally, consumer protection watchdogs have adopted eight Fair Information Practices (collection limitation, data quality, purpose specification, use limitations, security, openness, individual participation, and accountability) in order to establish rights and responsibilities in the use of individuals' data.

We believe the Commission should endorse best practices for Internet mailing lists and support the opt-in approach. This will have a significant impact in the efforts to

reduce spam, or unsolicited commercial e-mail. We also note that the Commission has failed to endorse strong consumer safeguards for the Fair Credit Reporting Act, which is a critical consumer statute now under review by the Congress. Strong leadership on the FCRA is important for the mission of the FTC.

Furthermore, the Commission should begin to consider new technologies that have significant privacy implications for consumers in the marketplace. For instance, RFID, or "Radio Frequency Identification" chips may enable tracking of individuals in the physical world the same way that cookies do on the Internet. This week Microsoft announced that it plans to support RFID applications in future versions of its software. It would be appropriate for the FTC to begin the process of exploring how these new tracking techniques may affect consumer confidence and whether new safeguards may be required.

CONCLUSION

There is a clear need to enable the Federal Trade Commission to work in cooperation with consumer protection agencies in other countries to investigate and prosecute cross-border fraud and deceptive marketing practices. New legislation will be necessary to accomplish the goal. Nevertheless, the bill should be drafted in such a way so as to safeguard important American values, including procedural fairness, privacy protection, and open government. These principles of good government will assist consumer protection agencies around the world combat cyber fraud, and will help strengthen democratic institutions.

REFERENCES

Statement of Cedric Laurant, EPIC Policy Counsel, on "Potential Partnerships among Consumer Protection Enforcement Agencies and ISPs and Web Hosting Companies" for the Public Workshop on Public/Private Partnerships to Combat Cross-Border Fraud, before the Federal Trade Commission (February 19, 2003)

EPIC, "Joint Letter and Online Petition: Require Accuracy for Nation's Largest Criminal Justice Database"

Federal Trade Commission, Consumer Sentinel, Cross-Border Fraud Trends, January – December 2002, (February 19, 2003)

Federal Trade Commission, Budget Summary, Fiscal Year 2004, Congressional Justification

Federal Trade Commission, Budget Summary, Fiscal Year 2003, Congressional Justification

Federal Trade Commission, Consumer Sentinel web site

Federal Trade Commission, Cross Border Fraud web site

Federal Trade Commission, "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)

In the Matter of Microsoft Corporation, No. 012-3240, before the Federal Trade Commission

International Consumer Protection Enforcement Act of 2003, draft, May 21, 2003

Organization for Economic Cooperation and Development (OECD), Directorate for Science, Technology and Industry, Committee on Consumer Policy, "Cross-Border Co-operation in Combating Cross-Border Fraud: The US/Canadian Experience." (February 6, 2001)

Organization for Economic Cooperation and Development (OECD), Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"), reprinted in Marc Rotenberg, ed., *Privacy Law Sourcebook: United States Law, International and Recent Developments* 324-352 (EPIC 2002)

Transatlantic Consumer Dialogue, "Resolution on Protecting Consumers from Fraud and Serious Deception Across Borders," Doc No. Internet-28-02 (November 2002)

ABOUT EPIC

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 to promote the Public Voice in decisions concerning the future of the Internet. More information is available online at www.epic.org.