BY FAX (202-224-0836 / 202-224-5011)

June 17, 2004

Chairman Richard G. Lugar
Ranking Member Joseph R. Biden, Jr.
Senate Committee on Foreign Relations
United States Senate
Washington, DC 20510

Dear Chairman Lugar and Senator Biden,

We are writing on behalf of the Electronic Privacy Information Center (EPIC) to urge opposition of ratification of Treaty 108-11, the Council of Europe's Convention on Cybercrime ("the Cybercrime Convention"). EPIC is a leading civil liberties organization that has reported on developments in privacy and human rights around the world for several years.[1] We believe for the reasons stated below that it would be a mistake for the United States to support adoption of this treaty. We ask that this statement be included in the June 17, 2004 hearing record of the Senate Committee.

The Convention Threatens Core United States Civil Liberties Interests

The Convention Lacks Adequate Safeguards For Privacy

We object to the ratification of the Cybercrime Convention because it threatens core legal protections, in the United States Constitution, for persons in the United States. The treaty would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards, and specifically lacking judicial review and probable cause determinations required under the Fourth Amendment. A significant number of provisions grant sweeping investigative powers of computer search and seizure and government surveillance of voice, e-mail, and data communications in the interests of law enforcement agencies, but are not counterbalanced by accompanying protections of individual rights or limit on governments' use of these powers.

Individual Privacy Is Fundamental to Good Security Practices

The Cybercrime Convention sets out a strong commitment to security measures, while failing to acknowledge the commonly held position that the protection of individual

[1] *See, e.g.,* PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (EPIC 2003) (A 545 page report on recent developments in over fifty-five countries around the world), available online at http://www.privacyinternational.org/survey/phr2003/. *See also* EPIC, *Cybercrime Convention*, available online at http://www.epic.org/privacy/intl/ccc.html.

privacy is in fact fundamental to good security practices,[2] and the fact that many of the Convention's provisions, when put into practice, may actually detract from security.[3] For example, Article 14 (Search and Seizure of Stored Computer Data) requires countries to enact legislation compelling individuals to disclose their decryption keys in order to allow for law enforcement access to computer data.[4] Besides the contradiction between this requirement and the prevalent right against self-incrimination, which would otherwise be safeguarded under the United States Constitution, the disclosure of these keys can drastically reduce the security of a wide range of computer systems.[5]

Vague and Weak Privacy Protections

In response to objections from privacy and human rights groups, the working group added Article 15 (Conditions and Safeguards), which provides, *inter alia*, that each party must ensure that "the establishment, implementation, and application of the powers and procedures provided for in this Section [Procedural Law] are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties."[6] This provision is quite vague, and is not reiterated with specific and detailed protections within any of the specific provisions. For example, provisions on expedited preservation of stored computer data[7] and expedited preservation and partial disclosure of traffic data[8] make no mention of limitations on the use of these techniques with an eye to protection of privacy and human rights. Furthermore, the vagueness of this provision (and others) introduces the risk of enhancement of the flaws and benefits of the Cybercrime Convention overall, as the Convention is transposed into the laws of ratifying countries which may have drastically different pre-existing privacy and human rights protections.[9]

---

[2] David Banisar & Gus Hosein, *A Draft Commentary on the Council of Europe Cybercrime Convention*, Oct. 2002, available online at <http://privacy.openflows.org/pdf/coe_analysis.pdf>.

[3] *Id.*

[4] Council of Europe: Convention on Cybercrime, Nov. 23, 2001, 41 I.L.M 282, Art. 14. Article 14, para. 4 provides, *inter alia*, that participating countries shall enact legislation that would empower law enforcement authorities "to order for the purposes of criminal investigations or proceedings any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking" of the seizure of such data.

[5] Banisar, *supra* note 1, at 32.

[6] Convention on Cybercrime, *supra* note 3, at Art. 15.

[7] *Id.* at Art. 16.

[8] *Id.* at Art. 17.

[9] Giovanni Buttarelli, Remarks in Washington, D.C., *Promoting Freedom and Democracy: A European Perspective*, May 21, 2004, available online at http://www.epic.org/privacy/intl/buttarelli-052104.html.

Insufficient Recognition of International Human Rights Obligations

References to the protection of human rights, including the right to privacy, are brief at best, especially when compared with myriad espousals of the importance of serving the interests of law enforcement agencies.[10] Examination of the Preamble is extremely illuminating on this point, with eight clauses related to the interests of law enforcement, crime-prevention, and national security, and only two oriented toward protection of privacy and human rights.[11]

Coupled with the lack of consideration of, and compliance with, important international conventions on human rights, it becomes clear that the Cybercrime Convention is much more like a law enforcement "wish list" than an international instrument truly respectful of human rights. The Cybercrime Convention fails to respect fundamental tenets of human rights espoused in previous international Conventions, such as the 1948 Universal Declaration of Human Rights[12] and the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms.[13] The Cybercrime Convention also ignores a multitude of treaties relating to privacy and data protection, including the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data,[14] and the European Union's 1995 Data Protection Directive.[15]

The Cybercrime Convention Lacks a Dual-Criminality Requirement

Article 25 (General Principles Relating to Mutual Assistance) introduces broad principles of mutual assistance across international borders, but lacks a "dual-criminality" provision, under which an activity must be considered a crime in both countries before one state could demand cooperation from another. Thus, the treaty would require U.S. law enforcement authorities to cooperate with a foreign police force even when such an agency is investigating an activity that, while constituting a crime in their territory, is perfectly legal in the U.S. No government should be put in the position of undertaking an

---

[10] Convention on Cybercrime, *supra* note 3, at Preamble.
[11] *Id.*
[12] Available online at <http://www.un.org/Overview/rights.html>, *reprinted in* MARC ROTENBERG, ED., PRIVACY LAW SOURCEBOOK: UNITED STATES LAW, INTERNATIONAL LAW AND RECENT DEVELOPMENTS 316-21 (EPIC 2003).
[13] Available at <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>.
[14] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, available online at <http://www.coe.fr/eng/legaltxt/108e.htm>.
[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, available at http://europa.eu.int/comm./internal_market/en/media/dataprot/law/index.html.

investigation of a citizen who is acting lawfully, regardless of mutual assistance provisions and the laws of other countries.[16]

The Cybercrime Convention Was Drafted in a Secretive and Un-Democratic Manner

The drafting of the treaty has been conducted in a very secretive and undemocratic manner. The Council of Europe's Committee of Experts on Crime in Cyberspace ("the Committee") completed nineteen drafts of the Convention before the document was released to the public.[17] Between 1997 and 2000, no draft was released and no public input was solicited.[18] The Convention was drafted by persons and groups primarily concerned with law enforcement, and reflects their concerns almost exclusively, to the detriment of privacy and civil liberties interests.[19] Since the release of Draft 19, the Committee has made little effort to acknowledge and incorporate concerns and suggestions of privacy and human rights groups. The Council of Europe set up an e-mail address only late in the negotiation process (after the release of Draft 19), to which members of the public could submit comments. However, few of these suggestions appear to have been translated into substantive changes to the document.[20]

We also note that, as with the process of drafting the Cybercrime Convention, there is markedly one-sided representation at today's hearing, as all three witnesses are government officials. For legislation that so touches on individual rights and freedoms, there should be a broader range of voices heard on this topic.

Most European Countries Have Failed to Ratify the Cybercrime Convention

Despite the ceremonial act of thirty-eight countries in signing the Convention, only six countries have yet ratified the Cybercrime Convention.[21] As of June 16, 2004, only Albania, Croatia, Estonia, Hungary, Lithuania, and Romania ratified the Cybercrime Convention. The Cybercrime Convention remains very controversial in Europe, in particular the provisions relating to the lack of protections for the use, collection, and distribution of personal data. In Europe, personal data protection has come to be considered a fundamental right, and Europe's legislators are committed to safeguarding this right.[22] Europeans are concerned that while the Cybercrime Convention aims to

---

[16] *See* Greg Taylor, *The Council of Europe Cybercrime Convention: A Civil Liberties Perspective*, Electronic Frontiers Australia, available online at <http://www.crime-research.org/eng/library/CoE_Cybercrime.html>.
[17] *Id.*
[18] Banisar, *supra* note 1, at 5.
[19] *Id.* at 2.
[20] *Id.* at 5.
[21] Council of Europe, Convention on Cybercrime, Status as of 16/6/2004, at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.
[22] Buttarelli, *supra* note 8.

achieve a noble end of fighting cyber-crime, the extensive surveillance tools that are being shaped to achieve this end are threats to a democratic society.[23]

In summary, the Cybercrime Convention threatens core legal rights established by the United States Constitution. It constructs a sweeping structure of vast and invasive law enforcement activity without a corresponding means of oversight and accountability. It speaks in very specific terms about the new authorities to pursue investigations but in only generalities with regard to legal rights.

The Cybercrime Convention is the result of a process that excluded legal experts and human rights advocates. It is a one-sided document that fails to reflect the broad commitment to the rule of law and the protection of democratic institutions that has otherwise characterized the treaties proposed by the Council of Europe.

It is therefore not surprising that the vast majority of the countries of the Council of Europe have thus far failed to ratify the Cybercrime Convention. We urge the United States not to support this deeply flawed proposal.

Sincerely yours,

Marc Rotenberg,
EPIC President

Cédric Laurant,
EPIC Policy Counsel

Tara Wheatland,
EPIC IPIOP Law Clerk

[23] *Id.*