ECOMMERCE NEWS

June 30, 2001

CONVENTION ON CYBERCRIME

The European Committee on Crime Problems has voted to approve the final draft of a Convention on Cybercrime. This was an unsurprising move, and takes the Convention one step closer to finalization by the Council of Europe. From the point of view of U.S. industry, one problem with the Convention may be that it encourages countries to create a patchwork of data retention laws. The U.S. Department of Justice is continuing to take comments on the draft text of the Convention, and is concerned that federalism issues won't be taken into account. Here is a summary of the Convention and its possible effects.

Background. The Convention on Cybercrime is the first international treaty addressing crime committed online. Drafted by the 43 member states of the Council of Europe, and incorporating contributions from the United States, Canada, Japan, and South Africa, the Convention has been revised over a four-year period. The European Committee on Crime Problems ("CDCP"), an intergovernmental expert body reporting to the Committee of Ministers of the Council of Europe, voted to adopt the final draft on Friday, June 22, 2001, and it was posted online on Friday, June 29 [http://conventions.coe.int/treaty/en/projets/FinalCybercrime.htm].

Following approval by the CDCP, the Committee of Ministers must review the Convention before adopting it. The Council of Europe estimates that this could occur as early as September 2001. Thereafter, the Convention will take effect when five states, including at least three Council of Europe member states, ratify it.

How have commentators reacted to the Convention? One of the most frequent criticisms of the Convention relates to the non-public manner in which it was promulgated. Public interest groups, business interests, and advocacy groups have had little opportunity to contribute to the drafting process or to have their input incorporated, although the U.S. Department of Justice has solicited outside comment. This was particularly troublesome in light of the composition of the working party drafting the Convention, which heavily favored law enforcement and excluded industry or non-governmental organization representatives.

Another concern relates to costs. Under Article 15.3, countries have no obligation to reimburse third parties for the cost of surveillance, notwithstanding repeated requests by industry that the Convention incorporate such a provision. Industry spokespeople predict that the high costs of compliance with law enforcement investigations could bankrupt smaller ISPs and lead to increased user fees.

The Convention may also encourage countries to create widely-varying data retention laws. (The EU recently approved a data retention directive.) Law enforcement interests benefit from data retention requirements, but data retention is financially burdensome. With no requirement of cost reimbursement for data retention, and no uniform proposal on the issue in the Convention, ISPs and industry interests on the one hand, and law enforcement interests on the other, are likely to compete for enactment of laws favorable to their respective

positions in their own countries. The result might be a panoply of different laws that could undermine the benefits of uniformity promised by the Convention.

Yet another consistent complaint pertains to the authority Article 19 grants to law enforcement to coerce Internet users to disclose encryption keys and the plain text of encrypted files. Up until now, only a handful of countries — Singapore, Malaysia, India, and the UK — have implemented such laws, and commentators suggest that they implicate both rights against self-incrimination and the European Convention on Human Rights.

Commentators have also used the U.S. experience with Carnivore — which compromised the network integrity of Earthlink, *see* http://stopcarnivore.org/carnfreeisps.htm — to suggest that certain practices sanctioned by the Convention (specifically, the real time collection of traffic data and interception of content data provisions) are a threat to providers' network integrity.

Moreover, many feel the Convention will hamstring security efforts. Internet security software companies frequently use tools of the hacking trade and virus programs to locate weak spots in computer systems. Earlier drafts of the Convention inadvertently criminalized innocent use of these tools, though the final draft may have allayed these concerns.

Perhaps the issue most relevant to ratification of the Convention in the United States is the Convention's inconsistency in requiring dual criminality as a condition for mutual assistance. To obtain aid investigating a citizen in another country, the acts under investigation need not be illegal in both countries.

Meanwhile, the U.S Department of Justice is anxious to ensure that a clause recognizing the different commitment to the Convention's principles that would be made on behalf of federal forms of government (in which states are free to enact their own criminal laws) is inserted. France is opposed to inclusion of such a clause, and the issue will be reviewed by a group of national government specialists in international legal cooperation.

What substantive crimes does the Convention prohibit? The Convention establishes two preliminary conditions that qualify an act as criminal under the Convention. First, an individual must commit an offense *intentionally*. Second, an individual must act *"without right."* The Convention defines "without right" broadly so as not to impair countries in their attempts to implement the concept within their own legal systems. Generally speaking, "without right" appears to mean an act taken without authority or an established legal defense or justification.

The Convention outlines four categories of offenses:

- offenses against the confidentiality, integrity, and availability of computer data and systems;
- computer-related offenses;
- content-related offenses; and
- offenses related to infringements of copyright and related rights.

The Convention requires signatories to adopt whatever laws may be necessary to establish these offenses as crimes under their domestic laws. The U.S. Department of Justice has indicated that no changes to U.S. law will be needed. In a report issued just over six months ago, the Department explained that this was possible because the Convention was largely consistent with existing U.S. law. Moreover, flexibility was built into the Convention: signatory countries can take reservations on certain provisions.

Offenses against the confidentiality, integrity and availability of computer data and systems. Five varieties of offenses exist under this subdivision. They are:

- illegal access;
- illegal interception;
- data interference;
- system interference; and
- misuse of devices.

These categories are broadly designed to outlaw computer hacking, including certain instances of

intercepting non-public transmissions of computer data, altering or deleting computer data, and selling devices (e.g., computer programs) that are designed primarily to accomplish any of the foregoing.

Computer-related offenses. The Convention groups computer-related forgery and fraud under this category. Both require the unauthorized "input, alteration, deletion, or suppression of computer data." Forgery occurs when this tampering results in inauthentic data that the individual intends should be "considered or acted upon for legal purposes as if it were authentic." Fraud, on the other hand, requires that the wrongful conduct be committed with "the intent of procuring, without right, an economic benefit for oneself or for another" and that the tampering result in property loss to another.

Content-related offenses. This includes production, distribution, procurement, and possession of child pornography. The Convention defines "child pornography" to include "realistic images representing a minor engaged in sexually explicit conduct," which would criminalize images that did not use real children at any point in the process of their creation. However, the Convention permits signatory countries to reserve the right not to apply that provision. According to the Council of Europe website's summary of the Convention, a protocol will also regulate the online propagation of racist and xenophobic ideas.

Offenses related to infringements of copyright and related rights. The Convention requires the criminalization of infringement "committed willfully, on a commercial scale and by means of a computer system." Neither the Convention, nor the Explanatory Memorandum Related Thereto prepared by the Committee of Experts on Crime in Cyberspace, defines the term "commercial scale," which leaves some question about whether the Convention criminalizes widespread online filesharing for personal use.

What procedures does the Convention establish? The Convention provides for the following:

- expedited preservation and rapid disclosure of data, both stored and traffic data,
- production of computer data and subscriber information,
- search and seizure of stored computer data, and
- real-time collection of traffic data and interception of content data.

However, the Convention also mandates conditions and safeguards against abuse of these procedures. Article 15 applies domestic laws, international treaties on human rights, and other international instruments "incorporat[ing] the principle of proportionality" to these procedures. In appropriate circumstances, before proceeding under these articles, law enforcement officials must obtain prior authorization by a judge or a comparable independent authority.

Who has jurisdiction? Notwithstanding the virtual nature of the location of cybercrime, the jurisdictional rules set forth in the Convention are earth-bound. A country has jurisdiction over any offense outlawed by Articles 2-11 if the crime occurred:

- in its territory;
- on board a ship flying its flag;
- on board an aircraft registered under its laws;
- by one of its nationals if the offense is punishable under the law of the country where it was committed or where it occurs outside the territorial jurisdiction of any country.

The Convention does not trump criminal jurisdiction exercised pursuant to domestic law. When more than one country asserts jurisdiction, the Convention calls for consultation between the parties to determine the most suitable jurisdiction.

What rules does the Convention adopt for international cooperation among signatory countries? The Convention articulates both general and specific principles for international cooperation.

General Principles. Article 23 provides generally for cooperation through the application of existing international agreements, agreements premised on uniform laws and reciprocity, and domestic laws.

Article 24 sets forth principles relating to extradition. Basically, if the laws of both countries implicated provide for punishment of at least a year for the offenses established under Articles 2-11, then the Convention authorizes extradition.

Article 25 announces general principles relating to mutual assistance. Unless otherwise specified, requests for mutual assistance are subject to conditions set forth in existing treaties, including the grounds on which a country can refuse assistance. Moreover, where the Convention specifies that a country may condition mutual assistance on dual criminality (that is, that the offense is criminal in both jurisdictions), Article 25(5) deems that condition satisfied so long as the offense is a crime in the requested country, regardless of whether it is a crime within the same category of offense (e.g., felony, misdemeanor).

In the absence of a relevant mutual assistance treaty or other arrangement, requests for mutual assistance must conform to the procedure outlined in Article 27. Article 27 mandates that signatory countries establish central authorities through which requests for mutual assistance must be cleared.

Article 26 permits countries spontaneously to produce information uncovered in the course of their investigations to another country.

Specific Principles. Articles 29-34 set forth specific procedures for requesting mutual assistance in executing the procedures established in Articles 16-21: expedited preservation of data, real-time collection of traffic data, interception of traffic data, etc.

Article 35 decrees that signatory countries establish a point of contact available 24 hours a day, seven days a week, to provide help with technical issues, inquiries about legal information, preservation of data, collection of evidence, and location of suspects.

ECommerce News is a publication of WCP's EGroup.

ECommerce News is also available at www.wilmer.com