



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 5, No. 41, 10/16/2006, pp. 1450-1454. Copyright © 2006 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Convention on Cybercrime

The United States recently ratified the Council of Europe Convention on Cybercrime, which not only deals with computer-related crime, but also provides for mutual assistance to foreign police agencies in gathering and sharing electronic evidence of any kind of crime. Banks, Internet service providers, and other businesses holding information of interest to law enforcement may want to anticipate the effects of the treaty's entry into force in the United States on Jan. 1, 2007, writes Jeffrey F. Pryce, of Steptoe & Johnson.

The Globalization of Electronic Evidence Gathering: U.S. Joins Council of Europe Convention on Cybercrime

JEFFREY F. PRYCE

In a significant step toward the internationalization of electronic evidence-gathering, on Sept. 29, 2006, the United States ratified the Council of Europe (CoE) Convention on Cybercrime (the CoE Convention or Convention), the first multilateral regime governing electronic surveillance, evidence sharing and computer crime. The treaty will enter into force in the United States on Jan. 1, 2007.

The United States joins 15 European countries, including France and a large number of Central and Eastern European countries, that have ratified the treaty. The United States is the first non-European country to

join the Convention. Some 27 other countries—including the United Kingdom, Germany, Italy, Spain, Sweden and the Netherlands—have signed the treaty but not yet ratified it. (See chart on the treaty at the end of this article).

I. Drafting history.

When the treaty made its public debut, it appeared to be against the backdrop of something of a clash of cultures. Given that the CoE treaty drafters were primarily government officials from law enforcement agencies, working by tradition behind closed doors, there was a perceived need for input from sectors with more expertise in the technologies involved. The Council of Europe negotiators may have gotten more (and more pointed) input than they anticipated. When a draft of the treaty was first published for comment in 2000, at the behest of U.S. officials participating in the negotiations, it was presented as a European project to harmonize and in-

Jeffrey F. Pryce, Steptoe & Johnson LLP, can be reached at jpryce@steptoe.com or (202) 429-8121.

ternationalize the law of cybercrime and of electronic surveillance. From the perspective of the U.S. Internet community, which often tended to see pan-European institutions as a source of more regulation than innovation, it presented cause for concern, and considerable commentary on the treaty ensued from a number of U.S. companies in the information sector and privacy groups.

In later drafts of the treaty, a number of provisions which had occasioned comment and criticism were revised and, from the perspective of Internet stakeholders, improved. This process resulted in provisions clarifying that the treaty would not be read to mandate data retention or the use of specific interception technology. Other revisions sought to protect the ability to develop and deploy security testing technology; limit vicarious liability; and better balance the burdens and risks that would be imposed on Internet service providers (ISPs) and communications networks generally.

Nevertheless, the final treaty was met with outright opposition from many privacy groups while receiving more nuanced, if mixed, reactions from industry. Many copyright holders were enthusiastic and consistent supporters, while some ISPs and other network operators, who expected to bear the burdens and risks of the additional data and surveillance requests that are expected to come from foreign police agencies, were more able to contain their enthusiasm. Although opinions differ as to what impact the various private sector reactions had on the timeframe for approval, it took nearly two years for the Bush administration to send the treaty to the Senate for its consent to ratification, and the better part of three more years for the Senate to give it.

From Infrastructure to Information. While the Convention has not changed in the last five years, the environment of the Internet clearly has evolved. When the treaty was drafted, a principal focus was on vandalous attacks against information technology infrastructure in general, and the Internet in particular. Malicious viruses and distributed denial of service attacks on computers were among the most salient problems, and the infrastructure-threatening Y2K “millennium bug” was fresh in the public mind.

At the same time, many experts in the U.S. information security sector felt that the most effective response to such technological threats was the deployment of technological countermeasures. While law enforcement played an essential role in deterring vandalous infrastructure attacks, this response alone had limited effectiveness in dealing with amateur hackers not easily deterred by the prospect of prosecution (which would generally occur only after the damage was done in any event). Prevention and rapid response to attacks were seen as more effective means of protecting the infrastructure.¹

In this regard, one major concern was that the treaty’s provisions on hacking devices were written so broadly that they might have the unintended consequence of prohibiting, or at least chilling, forms of legitimate security testing that information security experts used to protect networks against attack, or might develop in the future. In response, a specific provision

¹ For more on this subject, see the author’s testimony before the European Commission Hearing on Information Security and Computer-Related Crime, Brussels, March 7, 2001, available at <http://www.steptoe.com/professionals-349.html>.

was included in the treaty to provide a safe harbor for legitimate security testing.

In the five years since the Convention was drafted, much of the focus has shifted from attacks directed against information infrastructure, toward attacks directed at information itself. While the threat of Internet vandalism has by no means gone away, its impact has in fact been limited in the last five years, primarily by technological defenses. By comparison, one of the most salient concerns today is the compromise of private information in computer networks and databanks—whether unintentionally by its legitimate holders, maliciously by bad actors, or both.

Meanwhile, another trend which has continued undiminished is the dramatic increase in information that is transmitted and stored electronically. Given the extremely rich sources of data available in electronic networks and databanks, particularly in the United States, it is likely that law enforcement may find the most important use of the CoE Convention is more as a sword than a shield, since it provides a framework to gather electronic evidence on an international level, for use in the investigation and prosecution of any form of crime.

II. The Treaty

A. Scope of Treaty.

The CoE Convention has a multi-part structure, and broader impact than might appear from its name alone. First, the “Cybercrime” title significantly understates the Convention’s scope and impact. The treaty does contain an initial section requiring the enactment of a series of specific substantive computer crime laws, including illegal access and hacking; fraud; child pornography; and copyright offenses. Probably more important, however, are the sections that follow, which contain significant provisions providing for the gathering and sharing of electronic evidence regarding any sort of crime—not just computer crimes.

By its terms, the scope of the treaty is quite broad. For example, “Service provider” is defined as:

- i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Similarly, “computer data” is defined broadly as well, to include “any representation of facts, information or concepts in a form suitable for processing in a computer system”

B. Substantive Provisions.

The first substantive part of the treaty requires government parties to enact laws against a number of crimes, including cybercrimes such as hacking and illegal access; computer-related fraud and forgery; content and copyright crimes; and aiding and abetting.

1. *Hacking, unauthorized access, security testing.*

The first crimes the treaty requires governments to criminalize relate to offenses against the confidentiality, integrity and availability of computer systems and data. These include crimes of (1) illegal access to a computer (which governments may, or may not, require be committed by infringing security measures; with dishonest intent; or with regard to a computer connected to a network); (2) illegal interception; (3) interference

with data; (4) interfering with the functioning of a computer system; or (5) use or possession of hacking devices and code. The hacking device provision raised serious concerns about constraining the use and development of legitimate security testing devices, which were addressed by inclusion of a specific provision clarifying that it was not meant to apply to such activities.

2. *Fraud and Forgery.*

The treaty also contains broadly written provisions requiring the criminalization of computer-related forgery and computer related fraud, which includes causing loss of property to another by “any input, alteration, deletion or suppression of computer data . . . with fraudulent or dishonest intent of procuring, without right, an economic benefit. . . .”

3. *Content and Copyright Offenses*

The treaty requires the criminalization of a range of child pornography offenses, including producing, offering or making available, distributing or transmitting, procuring, or possessing child pornography. It also requires parties to prohibit infringement of copyright and related rights, though there is a limited exemption allowing for the application of non-criminal penalties in limited circumstances.

4. *Aiding and Abetting, Attempt, and Corporate Liability.*

The treaty also contains crimes of aiding and abetting; attempt; and provisions establishing corporate liability. Many U.S. ISPs had particular concerns about intermediary liability—not diminished by some widely reported instances of ISPs being held liable for third-party content by European authorities. While these were ameliorated by language in the treaty and Explanatory Report, lingering concerns about intermediary liability are never far from the surface.

C. Investigative Powers.

The second part of the treaty requires governments party to the treaty to enact measures giving themselves a wide range of powers to conduct electronic surveillance and electronic evidence-gathering. These kinds of authorities are already available to the U.S. government, and the Senate was at pains to emphasize that the U.S. did not need to rely on authorities in the USA PATRIOT Act to implement its obligations under the treaty.

D. International Assistance.

In its third part, the treaty provides for governments to request, and provide, mutual assistance in the investigation and prosecution of the crimes in the treaty—and any other crime as well.

The treaty is meant to supplement, not supplant, existing arrangements for international law enforcement cooperation, like Mutual Legal Assistance Treaties (MLATs), and contains provisions explicitly preserving such arrangements. Similarly, the substantive crimes in Part 1 of the Convention will not create an independent basis for extradition by the United States, but will be added to the offenses for which extradition is available under existing extradition treaties.

One of the most significant parts of the treaty provides for gathering and sharing electronic data and evidence at the request of foreign law enforcement agencies. Forms of international evidence-gathering assistance established in the treaty include:

Provisional measures, including:

(1) expedited preservation of stored computer data, pending a request for search, seizure or disclosure of the data;

(2) expedited disclosure of traffic data, when the execution of a request to preserve traffic data indicates that another country was involved in the transmission of the communication;

Collection and Disclosure of Data, including:

(3) search, seizure and disclosure of stored data;

(4) real-time collection of traffic data; and

(5) interception of the content of specified communications.

The treaty generally does not require dual criminality (i.e., that the crime being investigated is also a crime in the country providing assistance) for the sharing of electronic evidence at the request of foreign law enforcement agencies, and provides specifically that assistance with regard to the substantive computer-related crimes required by the first part of the treaty may not be denied on the basis of lack of dual criminality. The invocation of dual criminality as a ground for refusal is limited in certain other instances, including expedited preservation of data. The treaty also provides that assistance may not be refused in the investigation of the computer-related crimes set out in its Articles 2 through 11—including fraud committed with computers—on the ground that they are tax offenses. See CoE Convention, Art. 25(4).

The treaty gives governments greater flexibility in setting limits on their cooperation in the collection of real-time traffic data and interception of the content of communications, reflecting the sensitivity of these forms of surveillance. Thus, parties are obligated to assist with intercepting content data “to the extent permitted under their applicable treaties and domestic laws.” CoE Convention, Art. 34. As the Senate Foreign Relations Committee noted in its Report on the treaty, there is currently no authority to intercept communications based solely on the request of a foreign government; a parallel or related investigation in the United States would be required. Senate Exec. Rept. 109-6 (Nov. 8, 2005). Of course, nothing prevents U.S. authorities from opening such a parallel investigation, if they considered it appropriate, and there would then be statutory authority for the sharing of fruits of such an investigation with foreign law enforcement agencies. See 18 U.S.C. § 2517(7).

With regard to the real-time collection of traffic data, parties are obligated to provide assistance at least regarding offenses for which real-time collection of traffic data would be available under their domestic law. Art. 33(2). As in domestic cases, U.S. execution of foreign government requests for collection or disclosure of electronic evidence would require judicial oversight. Senate Exec Rept. at 6. However, the treaty does provide more limited flexibility for governments in other areas, such as the expedited disclosure of stored traffic data, when it indicates that a transmission went through a third country. (This will, of course, usually be through ISPs.) Procedures regarding real-time collection of traffic data are more restrictive.

III. Potential Impact of the Convention

Since the treaty will not enter into force until two and a half months from now, the full significance of the

treaty's implementation in the United States remains to be seen. However, the potential implications of the application of this new international regime in the United States are significant.

Significance of Substantive Criminal Law Provisions. One legal consequence of joining the Convention, which is unlikely to be felt immediately, but which stands in contrast with the Bush administration's general attitude toward multilateral treaty regimes, is the ceding of some autonomy by the United States. Hailing the Senate's consent to ratification, Attorney General Alberto R. Gonzales said that the treaty was consistent with constitutional privacy guarantees, and will not require changes in U.S. law. What he did not say is that it may not allow some changes in U.S. law, either. By joining a treaty regime which internationalizes key substantive laws of cybercrime, the United States has ceded some flexibility (and sovereignty) in changing U.S. criminal law to respond to evolving technologies or changing circumstances.

Significance of Electronic Evidence-Gathering Provisions. More attention is likely to be paid to the immediate effects of electronic evidence-gathering provisions. The U.S. Justice Department took the position that no implementing legislation is necessary, since existing U.S. legal authorities were sufficient to implement the treaty. (Of course, some parts of the treaty are "self-executing," and do not require implementing legislation.) Moreover, assurances were given that the Justice Department will be the conduit for all foreign requests for stored data. However, U.S. ISPs, and other holders of data, should be prepared for those authorities to get some additional use. This new framework for international assistance was created to be utilized by foreign as well as U.S. law enforcement. It is probably true that in many situations, foreign law enforcement agencies might have been able to request assistance from the U.S. government even before it joined the Convention—provided they knew that such assistance was available, and had established internal mechanisms through which to request it. But the entry into force of an international convention, which creates obligations to provide assistance to foreign governments, can certainly be expected to make a difference. This is all the more true

because of the rich sources of data and evidence that are available in electronic networks and databanks in the United States.

The effects of the CoE Convention could be felt quite broadly. Banks and other institutions holding information useful to criminal investigations may find themselves subject to new kinds of data requests originating with foreign police agencies. And, in areas such as money-laundering and foreign corruption law, the growing international reach of criminal regulation—European as well as from the United States—may be further encouraged by the availability of tools that enhance the international reach of investigation.

The most immediate impact, though, will likely be noted by ISPs in particular. The Senate report recommending approval of the Convention stated that it is not expected to create "an undue burden" on ISPs, although they may be required to collect, preserve or disclose specified data in specific cases. How undue that added burden will be, ISPs will soon find out, but if the Convention did not result in an increase in the data collected, preserved and disclosed at the request of foreign law enforcement agencies, it would seem to have limited purpose. Nor are foreign police agencies subject to all of the public policy constraints which serve to limit the demands that U.S. law enforcement places on domestic ISPs. And, in addition to new levels of data requests, ISPs may also be sensitive to receiving new kinds of requests, since customers and the public may have a different reaction to the disclosure of information to foreign law enforcement than to U.S. authorities.

The full extent to which U.S. ISPs and data-holders will experience a significant increase in requests for data as a result of the Convention's entry into force on Jan. 1, 2007, remains to be seen, as do many other details regarding its implementation. What is certain is that business' increasing reliance on electronic commerce, communication and data, is being accompanied by an increasing internationalization of the legal regimes governing their activities and information. With the CoE Convention's entry into force, that growing globalization clearly applies to criminal evidence-gathering as well.

Convention on Cybercrime

Status as of: 11/10/2006

[All dates are in European style: date/month/year]

Member States of the Council of Europe

States	Signature	Ratification	Entry into force
Albania	23/11/2001	20/6/2002	1/7/2004
Andorra			
Armenia	23/11/2001		
Austria	23/11/2001		
Azerbaijan			
Belgium	23/11/2001		
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006
Bulgaria	23/11/2001	7/4/2005	1/8/2005
Croatia	23/11/2001	17/10/2002	1/7/2004
Cyprus	23/11/2001	19/1/2005	1/5/2005

States	Signature	Ratification	Entry into force
Czech Republic	9/2/2005		
Denmark	22/4/2003	21/6/2005	1/10/2005
Estonia	23/11/2001	12/5/2003	1/7/2004
Finland	23/11/2001		
France	23/11/2001	10/1/2006	1/5/2006
Georgia			
Germany	23/11/2001		
Greece	23/11/2001		
Hungary	23/11/2001	4/12/2003	1/7/2004
Iceland	30/11/2001		
Ireland	28/2/2002		
Italy	23/11/2001		
Latvia	5/5/2004		
Liechtenstein			
Lithuania	23/6/2003	18/3/2004	1/7/2004
Luxembourg	28/1/2003		
Malta	17/1/2002		
Moldova	23/11/2001		
Monaco			
Netherlands	23/11/2001		
Norway	23/11/2001	30/6/2006	1/10/2006
Poland	23/11/2001		
Portugal	23/11/2001		
Romania	23/11/2001	12/5/2004	1/9/2004
Russia			
San Marino			
Serbia	7/4/2005		
Slovakia	4/2/2005		
Slovenia	24/7/2002	8/9/2004	1/1/2005
Spain	23/11/2001 r		
Sweden	23/11/2001		
Switzerland	23/11/2001		
the former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005
Turkey			
Ukraine	23/11/2001	10/3/2006	1/7/2006
United Kingdom	23/11/2001		

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force
Canada	23/11/2001		
Japan	23/11/2001		
Montenegro	7/4/2005		
South Africa	23/11/2001		
United States	23/11/2001	29/9/2006	1/1/2007

Total number of signatures not followed by ratifications:	27
Total number of ratifications/accessions:	16

Notes: r: Signature "ad referendum."

Source : Treaty Office on <http://conventions.coe.int>