CONVENTION RAISES ISSUES FOR ISPs

Jonathan Band

Morrison & Foerster, LLP

On November 23, 2001, the United States and 29 other countries signed the Council of Europe (CoE) Convention on Cyber-Crime. The Convention requires parties to adopt substantive criminal law provisions relating to cyber-crime; to enact procedural provisions necessary for the investigation and prosecution of cyber-crime; and to provide one another with mutual assistance concerning cyber-crime violations. Language in early drafts raised significant concerns among Internet Service Providers (ISPs) that the Convention could increase their exposure to liability for the actions of their subscribers and other third parties.[1] Many of these concerns were mollified by the official explanatory report prepared by the CoE's Committee of Experts on Cyber-Crime.

While the CoE was considering the Convention, several parties expressed interest in including a substantive prohibition on the distribution of hate speech over the Internet. When the United States made it clear that the First Amendment would prohibit it from signing a Convention with such a provision, the negotiating parties agreed to prepare a Protocol to the Convention that would address hate speech. Thus, the United States would be able to sign the underlying Convention without becoming a party to the Protocol.

The early drafts of the Protocol raised many of the same ISP liability concerns as the early drafts of the Convention. Like the Convention's explanatory report, the Protocol's explanatory report addressed many of these liability concerns.[2]

This article discusses the ISP liability concerns posed by the Convention and Protocol, and their resolution by the explanatory reports.

The Convention

Article 9 of the Convention addresses offenses related to child pornography. Each party must establish "as criminal offenses…when committed intentionally and without right, … offering or making available child pornography through a computer system; [or] distributing or transmitting child pornography through a computer system." A service provider that designs its system to distribute automatically material provided by its subscribers arguably is intentionally distributing the material, even if the ISP does not know the specific content of the material.

Fortunately, the explanatory report interprets Article 9 in a manner favorable to ISPs. Paragraph 95 of the report explains that "'[m]aking available' is intended to cover the placing of child pornography on line for the use of others e.g. by means of creating child pornography websites." Similarly, paragraph 96 states that "'[d]istribution' is the

---

[1] The Convention defines a service provider as "any public or private entity that provides users of its service the ability to communicate by means of a computer system; and … any other entity that processes or stores computer data on behalf of such communication service or users of such service."

[2] At the writing of this article, the Protocol and its explanatory report have been adopted by the Committee of Experts on the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems, but have not yet been officially adopted by the CoE. This is expected to occur by November, 2002.

active dissemination of the material. Sending child pornography through a computer system to another would be captured by the offence of 'transmitting' child pornography." In short, the explanatory report makes clear that Article 9's terms "making available," "distributing," and "transmitting" refer to the active dissemination by the subscriber, not the passive technical enablement of the dissemination by the ISP.

The explanatory report makes this even more explicit in the context of Article 11. Article 11 requires the imposition of criminal sanctions on the intentional "aiding or abetting the commission of any of the offenses" mandated by the Convention.[3] An ISP that provides its facilities to a person committing an offense such as copyright infringement perhaps could be said to aid and abet the offense. However, paragraph 119 of the explanatory report expresses that "[l]iability arises for aiding and abetting where the person who commits a crime established in the Convention is aided by another person *who also intends that the crime be committed*." (Emphasis supplied.) The example used by the explanatory report concerns ISPs. "[A]lthough the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section." The report then adds that "there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision."

[3] These include: illegal access to computer systems; illegal interception of transmissions of computer data; interference with computer data; interference with computer systems; misuse of devices and access codes; computer-related forgery; computer-related fraud; child pornography; and infringement of copyrights and related rights.

This paragraph makes two critical points. First, an ISP will not be considered an aider or an abettor unless it shares the criminal intent of the person perpetrating the crime. Mere provision of services, by itself, does not satisfy the intent requirement. Second, following from this first point, an ISP need not monitor its service in order to avoid liability. Because it is not liable for the actions of its subscribers, an ISP does not need to take affirmative steps to police these actions.

The explanatory report also discusses ISP liability in the context of Article 12. Article 12 requires parties to hold a legal person – a corporate entity – liable for acts committed for its benefit by a natural person "acting under its authority." Paragraph 125 of the explanatory reports hastens to add that "[a] service provider does not incur liability by virtue of the fact that a crime was committed on its system by a customer, user, or third person, because the term 'acting under its authority' applies exclusively to employees and agents acting within the scope of their authority.'"

In sum, three different provisions of the Convention could be read to expose ISPs to liability. In all three cases, the explanatory report clarifies that the drafters do not intend to impose liability on service providers that do not share the criminal intent of the person committing the crime.

The Protocol

Paragraph 25 of the Protocol's explanatory report discusses the required level of intent for all the offenses established under the Protocol. The report echoes themes from

the Convention report's treatment of aiding and abetting, stating that "[I]t is not sufficient ... for a service provider to be held criminally liable under this provision, that such service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case." Like the Convention report, the Protocol report stresses that "a service provider is not required to monitor conduct to avoid criminal liability."

Protocol Article 3 targets intentionally "distributing or otherwise making available racist and xenophobic material to the public through a computer system." The formulation of Protocol Article 3 is similar to that of Convention Article 9 concerning child pornography, and raises the same concern with respect to ISPs. Could an ISP that makes it facilities available to a person who disseminates racist material be considered to have intentionally distributed the material? Protocol report paragraph 27 clarifies that "the act of distributing or making available is only criminal if the intent is also directed to the racist and xenophobic character of the material." In other words, the distributor must know that the material is racist.

Further, Protocol report paragraph 28 uses language similar to Convention report paragraphs 95-96 when defining distribution and making available: "'Distribution refers to the active dissemination of racist and xenophobic material ... while making available refers to the placing on line of racist and xenophobic material for the use of others." In short, the Protocol report, like the Convention report before it, makes clear that the terms

“making available” and “distributing” refer to the active dissemination by the subscriber, not the passive technical enablement of the dissemination by the ISP.

Protocol Article 7 requires the criminalization of the aiding and abetting of offenses established by the Protocol. Protocol report paragraph 45, like Convention report paragraph 119, states that "although the transmission of racist and xenophobic material through the Internet requires the assistance of service providers as a conduit, the service provider that does not have the criminal intent cannot incur liability under this section.” Protocol report paragraph 45 also repeats Convention report paragraph 119’s conclusion regarding monitoring: “there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision."

Finally, Protocol Article 8(1) provides that Convention Article 12, concerning corporate liability, applies with equal force to the Protocol. Presumably the favorable language in Convention report paragraph 125 limiting ISP liability for “a crime … committed on its system by a customer, user, or other third person” also applies to the Protocol.

Thus, like the Convention, the Protocol contains provisions that could be interpreted to impose liability on ISPs. And like the Convention report, the Protocol report unambiguously states that the drafters do not intend to impose such liability.

Conclusion

The Convention's and Protocol's explanatory reports go a long way to eliminating the concerns of ISPs that the Convention and Protocol could require parties to hold ISPs liable for the criminal activities of their subscribers. Nonetheless, the Convention and Protocol could still pose problems for ISPs in several respects.

First, the explanatory reports do not have the force of the black letter of the Convention or the Protocol. Parties can ignore the reports' interpretations when they implement the Convention's and Protocol's requirements into domestic law.

Second, the Convention and the Protocol set minimum requirements concerning cyber-crime and hate speech – a floor rather than a ceiling. Thus, even if a party understood that the Convention did not require imposition of liability on service providers, the party could still decide that imposition of liability on ISPs was an appropriate and effective means of combating cyber-crime. The party could decide to exceed the Convention's and Protocol's requirements.

Third, the Convention may impose other burdens on service providers. The Convention requires enactment of "domestic criminal procedural law powers necessary for investigation and prosecution of [cyber-crime] offenses as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form…." Convention report paragraph 16. Parties must adopt procedures that permit law enforcement authorities: 1) to order ISPs to preserve stored computer and

traffic data; 2) to search and seize stored computer data in the possession of ISPs; and 3) to compel real-time collection of traffic and content data by ISPs.

To be sure, the Convention report states that the obligation to ensure preservation of data does not require service providers "to implement new technical capabilities…." Paragraph 152. Likewise, Articles 20 and 21 concerning the real-time collection of traffic and content data would only compel a service provider to perform collection functions "within its existing technical capability." The Convention report explains that "[t]he article does not obligate service providers to ensure that they have the technical capability to provide such collection, recording, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Paragraph 220. Nonetheless, "if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to take the necessary measures to engage such capability." *Id.* This cooperation and assistance could be extremely costly to the ISP.

The U.S. government has taken the position that U.S. law already conforms to the Convention's procedural requirements, and thus they will not impose an additional burden on U.S. ISPs. However, other jurisdictions may have to change their procedures, and U.S. ISPs operating in those jurisdictions may have to comply with a higher volume of government requests. Moreover, the Convention's mutual assistance provisions may

lead foreign governments to request the U.S. government to obtain more information from U.S. ISPs.

Of course, these burdens must be weighed against the potential benefits of the Convention to ISPs. The Convention requires parties to establish criminal sanctions against illegal access to computer systems, illegal interception of transmissions of computer data, interference with computer data, and interference with computer systems. Because ISPs are frequent victims of these offenses, the Convention could significantly assist ISPs by helping eradicate these forms of cyber-crime.