



**WORLD INFORMATION TECHNOLOGY AND SERVICES ALLIANCE
(WITSA) STATEMENT ON THE
COUNCIL OF EUROPE DRAFT CONVENTION ON CYBER-CRIME**

November 2000

The World Information Technology and Services Alliance (WITSA) welcomes the opportunity to participate in the crucial dialogue on how to most constructively and effectively enforce criminal law in the increasingly international law enforcement environment fostered by the Internet and other information networks. Because efforts to improve law enforcement in the digital environment can have both positive and negative effects on the health and growth of the international information economy, it is essential that such efforts be based on the close consultation and cooperation between government, industry and civil society that can generate consensus among all interested parties, and ensure that new measures are carefully crafted and effectively applied.

The evolving information age requires a minimalist approach to regulation of information technology and information systems, particularly in the criminal realm. The Internet and information technology thrive in a relatively unconstrained environment which fosters rapid innovation and free dissemination of information. Moreover, since a principal function served by the Internet is to enable the free exchange of information, efforts to target regulation specifically at activities on the Internet touch on sensitive issues of individual liberty as well as cultural tradition. Criminal law must be available to prevent and counteract harmful illegal activity on the Internet, but regulation specifically aimed at the information sector can and should be very narrowly tailored.

The majority of what are termed “cyber-crimes” is really violations of long-standing criminal law, perpetrated through the use of computers or information networks. The problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and more effective means of international cooperation to enforce existing laws. On the other hand, there are new and serious problems posed by attacks against computers and information systems, such as malicious hacking, dissemination of viruses, and denial-of-service attacks. Such attacks should be effectively prohibited, wherever they may originate. At the same time, it bears remembering that often the most effective way to counter such attacks is to quickly deploy technical countermeasures; therefore, to the extent that well-meaning but overbroad criminal regulations diminish the technical edge of legitimate information

security research and engineering, they could have the unintended consequence of actually undermining information security.

Although WITSA supports the objectives of improving international law enforcement cooperation and mutual legal assistance to keep pace with the increasingly international environment, it has serious concerns with many of the provisions of the draft cyber-crime convention. In its current form, the draft convention could impose burdensome data preservation requirements on Internet service providers (ISPs); make ISPs liable for third party actions; and restrict legitimate activities on the Internet.

I. World Information Technology and Services Alliance (WITSA)

The World Information Technology and Services Alliance (WITSA) is a consortium of 41 information technology (IT) industry associations from economies around the world (list attached). As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information;
- providing members with a vast network of contacts in nearly every geographic region of the world; and
- hosting the World Congress on IT, the only industry sponsored global IT event.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including:

- increasing competition through open markets and regulatory reform;
- protecting intellectual property;
- reducing tariff and non-tariff trade barriers to IT goods and services; and safeguarding the viability and continued growth of the Internet and electronic commerce.

More information on WITSA can be found online at <http://www.witsa.org>.

II. Burdensome Record Keeping

On May 15, 2000, the Group of Eight (G8) countries held a cybercrime meeting in Paris in an effort to start a discussion on combating Internet crime and closing “digital havens” that protect hackers.’” One of the issues discussed at that meeting was the Council of Europe’s draft convention. WITSA issued a statement to the G-8 in opposition to controversial provisions which permitted some governments to interpret Article 15 (16) (Expedited preservation of data stored in a computer system) and Article 16 (17) (Expedited preservation and disclosure of traffic data) as requiring parties to mandate that ISPs preserve and maintain the integrity of traffic data for Internet transmissions for

significant periods. Even if this was interpreted as only requiring prospective preservation on demand, it could impose burdensome and intrusive requirements on ISPs. WITSA encourages governments to avoid imposing new requirements on ISPs that result in significant financial burdens on their operations. Such added costs will ultimately affect the access costs of end users, and may negatively impact the growth of Internet usage.

Further, even if information of this sort could be collected and stored, this requirement raises serious privacy concerns. Given the debate going on around the world on the need to protect the privacy of Internet users, it makes little sense to require ISPs to collect and store more information than ever before.

WITSA believes revisiting this provision in consultation with the IT industry would benefit all the parties concerned.

III. Liability for Third Party Actions.

The draft convention requires parties to enact a variety of criminal laws (Articles 2-10), and then to criminalize aiding and abetting the commission of those offenses (Article 11). Because these offenses are committed via ISPs' systems, ISPs properly are concerned that they may be found to have aided and abetted the commission of the offenses. This is particularly the case with respect to Article 10, concerning copyright. Balancing the rights and interests of copyright holders and Internet service providers has been the subject of long and intensive negotiation in many countries, yielding hard-won and carefully crafted compromise legislation providing detailed, workable guidelines to address the problem of infringement. Under the text of the CoE treaty, an ISP may receive a vague notice from a content provider that somewhere in the ISP's service some infringing material has been uploaded by a subscriber.

WITSA believes it is critical that liability not be imposed on ISPs for the criminal acts of third parties using their facilities.

IV. Restriction of Legitimate Activities

The Internet flourishes in an environment in which regulatory minimalism fosters innovation and initiative. Accordingly, it is of particular concern that some offenses defined in the text are drafted so broadly that they might prohibit legitimate activities. For example, Article 2 requires a prohibition on access to a computer system "without right." Would this prohibit the use of "cookies"? Would it preclude or inhibit third party testing and evaluation of software, security systems or reverse engineering? Would this criminalize the use of search engine bots? Would this preclude instant messaging between competing ISPs? Clearly, these sorts of activities should not be treated as criminal offenses -- certainly not at this early stage of the Internet's development. Doing so will not only harm ISPs; it would also retard the growth of the Internet, to the detriment of hundreds of millions of users.

WITSA supports language that carefully and clearly defines harmful illegal behavior and does not criminalize legitimate activity.

Conclusion

The international enforcement problems implicated by crime using information systems, as well as the substantive problem of crimes committed against information systems, require close cooperation and dialogue between government and the information industry. The reactions to the draft Council of Europe Convention on Cyber-Crime indicate that this important process is just beginning. WITSA is committed to participation in that dialogue, and to reaching a consensus on carefully tailored measures that will both support effective international law enforcement and foster continued growth and innovation in the information sector.