

Prepared Remarks of
Jeffrey Pryce
Steptoe & Johnson LLP
at the Public Hearing of the
Commission of the European Communities
on its Communication:
**Creating a Safer Information Society by
Improving the Security of Information Infrastructures and
Combating Computer-Related Crime**
Brussels
7 March 2001

Thank you for the invitation to participate in this hearing on the Commission's Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime. Information security and cyber-crime -- and regulation responding to these problems -- are of deep importance to a broad range of economic and citizens' interests. This initial public hearing is an important and constructive part of addressing these critical issues.

My name is Jeffrey Pryce, and I am an international lawyer with the firm of Steptoe and Johnson. I should note at the outset that I advise several clients concerned with these issues, including the Working Group on International Cyber Security, which in turn participates in a broad coalition of communications and information industry and civil liberties groups with an interest in an international legal environment that fosters the vitality, security, integrity, and reliability of communications and information networks. I do not pretend to speak for any particular organization today; nonetheless, in the following comments I will attempt to include an explanation of some of the issues that have been raised, and concerns expressed, by organizations participating in discussions related to the topic of this hearing.

I. The Dual Subject of the Communication.

In addressing its Communication to the dual topic of information security and computer-related crime, the Commission has identified two very different but deeply interrelated aspects of the essential effort to secure the benefits of the emerging information age.

Governments have been concerned for some time about the threats as well as the opportunities presented by the revolutionary advances in technology and communications. The borderless nature of communication on the Internet has caused law enforcement to focus more on international issues, both because of the new ways in which crime can be committed and, perhaps more significant, the new possibilities for electronic investigation and evidence-gathering. Meanwhile, the increasing significance of the communications infrastructure in critical areas of national life has led governments to treat its protection as a matter of national security. Over the past few years, different initiatives have been launched in several key intergovernmental organizations, including the G-8, the OECD, and the Council of Europe. The

European Commission's Communication is one further manifestation of this development.

In some discussions, the themes of "cyber crime," "cyber security," "cyber terrorism," and "protection of critical communications infrastructures" can be wrapped in a single envelope. That is not necessarily the best approach. While responses to these various challenges can and should work in harmony, experience cautions against confusing very different categories of problems merely because they involve computer and communications systems.

II. Protecting the Security of Communications and Information Systems.

One area where shared concern and shared responsibility among government and industry create particular opportunities is in information security and the protection of critical communications infrastructures. There is a strong sense that those are areas in which particular progress can be made by government and industry working together.

Among the core challenges in information security and cyber-crime is the problem of purposeful attacks against communications networks and information systems – such as viruses, malicious hacking, and denial-of-service attacks.

There are three aspects to protecting information and communication systems from such attacks:

1. Prevention and Awareness:

- Pre-emptive security measures, such as firewalls, information security procedures and technology, PKI technology and the like are essential elements in prevention. No less important are the trained individuals who routinely use these procedures in their operation of information systems. And it is also essential to ensure that users – organizations as well as individuals -- are educated and participate in preventing breaches. This is an area in which industry and other users must play a leadership role. However, this does not mean mandated standards or criteria in these areas.

2. Response.

- When an attack does occur, there are important responsive measures that can limit the damage it causes, including warning of an attack and disseminating measures to protect against or defeat it. Industry and other users of networks and computer systems are becoming more aware of their need to respond quickly. One industry-wide example of this sort of measure in the U.S. is the establishment of Information Sharing and Analysis Centers (ISACS) by the information technology, financial services and other critical infrastructure sectors. These mechanisms enable rapid sharing of information, with limitations and protections against risks such as anti-trust claims or the public exposure of proprietary information. Similar mechanisms could be considered to ensure international sharing of information when attacks occur or when there is information that such an attack might occur. This, again, is an area where government might cooperate with industry, but should be careful not seek to control or

mandate criteria. Industry is also concerned that governments take care not to create undue and costly or invasive reporting mechanisms.

3. **Deterrence/investigation and prosecution:**

- Finally, it is important to be able to find and prosecute those who commit attacks against communications networks and information systems. An essential element of this is a well trained, up-to-date, and easy to reach law enforcement system, which is fully prepared to respond quickly and efficiently to reports of crimes. It should be noted, however, that given the number of attacks by adolescent hackers whose motivation is not economic, deterrence alone is unlikely to be an effective means of protecting information systems. What is essential is that the information sector maintain a technological edge over those who attack information systems. There is also a role for joint efforts, like the joint program of the U.S. Department of Justice and the Information Technology Association of America regarding Cyber Ethics, which hopes to change the view that “hacking” is cool for teenagers.

One fundamental lesson here is the critical need for industry to retain the flexibility and agility to develop and deploy effective technical means to prevent and respond to attacks against information systems, and to stay one step ahead of the ingenuity of the malicious hacker.

III. Traditional Crimes on the Internet.

In addition to criminal behavior directed against communications networks and information systems, the information revolution also has had two important but different effects on more traditional types of crime, and punishment.

Clearly, it has given criminals new technical means which can be used in the commission of crimes generally. Besides the obvious increase in ability to use communication systems to conduct many crimes at greater distances, the advent of new information networks has added complexities of scope, scale, and identity.

On the other hand, the information revolution also has given law enforcement and prosecutors dramatically expanded technical means which can be used in the investigation and prosecution of crimes in general -- not just online crime. In particular, because the vast majority of written evidence is now processed electronically, law enforcement enjoys a dramatic increase in its technical ability to intercept, seize, and process evidence.

These effects also have increased law enforcement’s interest in and need for the ability to intercept and seize communications and data that travel over an increasingly international system of communication networks and information systems.

Balancing interests.

In this area, as well as that of information security, the interests of law enforcement in investigating and prosecuting crime are deeply shared by industry.

Crime is bad for business. However, it is essential that any provision for interception, preservation or seizure of data also carefully respect the important economic and human rights interests that will of necessity be implicated. Such surveillance should be restricted to essential requirements, compensated, respectful of human rights and constrained by clear procedures.

The effective, enforceable protection of privacy, human rights and lawful procedure (or “due process”) has been made all the more important by recent technological and legal developments. While existing international human rights instruments deal with these issues generally, many of the most often cited treaties were written before the electronic transmission era, and unsurprisingly, they may lack the specificity required to effectively protect the rights of citizens and industry with regard to electronic surveillance and seizure. Any new instrument creating government power in this area should include corresponding specific and enforceable protection of the rights of private parties vis-à-vis the government.

The Communication properly points out that all EU Member States have a legal framework allowing law enforcement to obtain judicial orders (or a warrant personally authorized by a senior Minister) for interception of communications on the public telecommunications network. Such fundamental legal safeguards and protections must be preserved in the evolving environment. However, we must bear in mind that the Internet and new communications media are fundamentally different from previous telecommunications networks, and we must guard against the simplistic or inappropriate extension of inapposite old models into new media. The legal framework for interception of communications on the Internet must be carefully crafted, and must take into account the unique nature of this medium, in order to prevent the undermining of privacy and human rights protections.

The Communication also refers to the important EU Mutual Assistance Convention. Article 21 of this Convention provides:

“Costs which are incurred by telecommunications operators or service providers in executing requests pursuant to Article 18 [regarding international requests for telecommunications interception] shall be borne by the requesting Member State.”

The reimbursement requirement is an important protection not just for industry, but also for the fundamental rights of citizens. Requiring governments to bear the cost of the communication interceptions they request provides an important discipline on the number of requests that might otherwise be made. Here, as elsewhere, the protection of industry and fundamental human rights are intertwined. Moreover, the burden of compelled interception can be quite extensive and problematic for private organizations, both commercial and non-commercial. The burden is not limited to the direct financial costs of compliance; in many cases, it will represent significant time or operational burdens as well. Industry will seek to support law enforcement’s needs, since it is clearly in industry’s interest to support effective investigations and prosecutions. Again, crime is bad for business. However, the impact on the enterprise should be given great weight in crafting surveillance obligations, and reimbursement for reasonable costs should be provided.

IV. Process for International Response to Issues of Information Security and Computer-Related Crime.

While clear substantive analysis of the issues involved in information security and computer-related crime is essential, recent dialogue emphasizes that it is equally important to follow an appropriate process in order to arrive at successful responsive measures, including legislation and regulation.

While there is no question that attention to the international aspects of information security and computer-related crime is required, it is also clear that it is critical to address these issues in the right way, and with a process which is inclusive of industry, particularly the sectors that create, operate and utilize communications and information systems, as well as the public. Trying to resolve these challenges without this in-depth consultation will result in a poorly crafted vehicles, counterproductive process, or both – easily creating unintended consequences. This could run the risk of undermining rather than supporting the security of information systems, choking the creativity and agility of information sector that has created such vast economic benefits, and impinging upon the privacy and fundamental rights of citizens. It could also result in a new patchwork of conflicting obligations and liabilities for industry, causing delay in investment or build-out in areas currently not fully benefiting from the Internet and e-Commerce and denying the accompanying economic benefits to those who might otherwise enjoy them.

Accordingly, it will be important at the outset to identify the appropriate process and vehicle to address the problem at hand.

Broad and inclusive Participation. First, it is critical that all interested sectors have meaningful participation throughout the process. As an example on the private level, the coalition which I mentioned earlier has sought out the active participation of the privacy community, along with the educational and non-profit communities, in addition to a broad set of industries.

Analysis and foundational consensus-building. One critical first step, before launching into drafting of proposed instruments for regulation, particularly criminal regulation, is the establishment of a consensus of affected parties on the precise nature and contours of the problem. It is helpful to move beyond anecdotal discussion to concrete and quantifiable analysis wherever possible.

Identification of Responsive Vehicle. After analysis and initial consensus-building, it is essential to identify an effective and agreed to means to address them. In many cases, the appropriate means may be general guidelines, information on best practices, broadened awareness of both the problems and the work that is being done to deal with them, and the like. There will also be a role for enhanced mechanisms for cooperation – be they intergovernmental, between industry groups, between government and industry, or among other players. There will also be areas which are appropriate for regulation, legislation, or international instruments, but the nature of the technology at issue will usually counsel seeking the most flexible tool available first.

Finally, there should be some considered agreement on the scope of measures to be proposed. Categories are frequently muddled in this area, and measures which seem to be directed against attacks on information infrastructure often end up covering far broader problems, and sometimes as a consequence do not do so in the way that might not have been intended at the outset.

V. Ideas Emerging from Ongoing Discussions.

Since the issues that the Communication addresses are the subject of a continuing, broad and serious discussion between all three affected sectors, it may be helpful to offer, on a non-exhaustive basis, some of the themes that have developed in that process, at least for many of the private sector players principally concerned with the security, integrity and vitality of information and communications networks. Some of the general ideas this sector has gleaned from ongoing discussions, which may be of relevance to the Commission as it considers developing of regulation or laws affecting cyber crime, include the following:

- Every state may need to determine whether it has the appropriate laws to criminalize intentional attacks against information systems; however, crimes of such as those of unauthorized access should be carefully and narrowly drafted.
- Restraint should be shown in creating new forms of “online crime”. If conduct is a crime offline, and is committed with the assistance of a computer or information system, there should be a presumption in favor of relying on existing law. This serves the interests of uniformity and judicial economy as well as of technological neutrality.
- Innocent third parties should not be exposed to criminal liability for actions of others or to undue burdens to comply with required cooperation with law enforcement.
- Private parties who are required to conduct surveillance, retention or seizure on behalf of governments should be fully compensated for their costs.
- Frameworks enabling the use of new technology to conduct surveillance and seizure of data should be accompanied by correspondingly specific and enforceable safeguards for the rights of privacy and human rights.
- Surveillance measures should be carefully defined, restrained, and conducted pursuant to clear procedures.
- Private parties who comply in good faith with compelled interception or seizure requirements should not be otherwise liable for such compliance.
- Surveillance measures should not create requirements for industry to deploy particular technology, or to generally monitor or retain data on their networks.

Finally, the Commission’s Communication makes reference to the CoE draft Convention on Cyber Crime, which, as the first such attempt to create an international

convention in this area, has become a central subject of the debate. It is no secret that the private sector has expressed significant concerns about several aspects of the treaty. In broad strokes, these concerns include the fact that it was drafted in a closed process without the participation of representatives of industry or citizens' interests, despite the significant operational and financial impact it would have on industry and other private organizations and its implications for privacy and human rights; that its provisions have not been drafted narrowly, precisely, or in a manner that takes account of the relevant technology; and that it lacks the necessary safeguards and protections for private organizations and citizens that would appropriately balance the burdens and liabilities it would mandate. That said, there is broad agreement that improved means of international cooperation among law enforcement are appropriate to take account of technical developments. Private organizations have strongly supported such cooperation, even as they have expressed significant reservations about other parts of the treaty, and are currently continuing to work to provide comments to the CoE drafters that will help address these problems.

The nature of the instrument of a convention reinforces the importance of getting it right the first time. Treaties by their nature move slowly. This creates severe limitations when dealing with rapidly evolving information technology, and reinforces the need for restraint and careful, narrow drafting. For that and other reasons, there is an important interest in continuing to work toward preventing duplication, overbreadth, or premature action.

VI. Conclusion.

Ensuring security of networks and computer systems is first and foremost the responsibility of the private sector. Dealing with detection, investigation and prosecution of crime is a governmental issue. Both require a cooperative and productive relationship between the private sector and governmental agencies. The issues identified in the Communication are issues of enormous importance and difficulty. To address them properly will require the engagement of considerable technical knowledge and legal expertise. Moreover, to address them successfully will require the participation of a broad range of interested parties in an open, constructive and serious dialogue. The Commission, in this hearing, has taken a well-considered and commendable opening step in that dialogue.

Thank you again for your invitation to this hearing. I look forward to continuing conversations on these important issues.