Fighting Cybercrime - What are the Challenges facing Europe?
Meeting Before the European Parliament

September 19, 2000

Remarks of Kevin DiGregory

Introduction

Good afternoon. My name is Kevin DiGregory. I am one of five Deputy Assistant Attorneys General in the Criminal Division at the U.S. Department of Justice in Washington, D.C.

I would like to thank the chair for inviting me to this important meeting to discuss the significant challenges of cyber crime that face all of us. I am especially pleased to meet with my esteemed colleagues in the European Union, and with the distinguished high-tech experts from both industry and government here today, to discuss our shared goal of making cyber space safe and secure for everyone.

The Three Prongs of Cooperation

The recent denial-of-service attacks on prominent commercial Internet sites and the dissemination of the "I Love You" virus that damaged computers around the world brought into stark relief how dependent the world has become on global computer networks. They also highlighted the fact that computer-related crimes are international in nature, and that important public safety issues must be considered as we work to harness the Internet's power to communicate, engage in commerce, and expand people's educational opportunities across the globe. Thus, our success in securing our networks depends on our ability to develop a coordinated response to criminal activities on our computer systems. That response requires cooperation on three levels. First, law enforcement agents must have the legal tools and practices in place to provide each other prompt mutual assistance in investigating and prosecuting computer-related crimes. Second, we have much to gain from direct collaboration between those in government charged with advancing the growth and security of e-commerce, and those charged with protecting the safety of the public. Finally, the private sector plays a critical role in assuring security and confidence in our shared networks, and government must work closely with industry at a variety of levels to respond to the problems associated with cyber crime.

Law Enforcement Cooperation

Cyber criminals are not confined by national borders or geography. An individual armed with nothing more than a computer and a modem can victimize people, businesses, and governments anywhere in the world without ever stepping outside his home. This can happen for nearly any type of crime, from violent crime, to terrorism, to drug-trafficking, to the distribution of child pornography, to identity theft, theft of intellectual property, and attacks on e-commerce merchants. Such criminals can also weave their communications through service providers in a number of countries to hide their tracks. For example, consider a computer hacker in Paris on the Left Bank of the Seine

who disrupts a corporation's communications network on the Right Bank. Before accessing his victim's computer, he routes his communication through providers in Romania, Australia, and Argentina. In this case, French police will need assistance from law enforcement authorities in Bucharest, Canberra, and Buenos Aires, before discovering that the criminal is right in their midst.

In these cases law enforcement is impeded by national borders in ways that criminals simply are not. While the Internet may be borderless for criminals, law enforcement agencies must respect the sovereignty of other nations. As a result, we are increasingly dependent on cooperation with foreign law enforcement agencies in fighting computer crime. Unfortunately, differing legal systems and disparities in the law often present major obstacles in our efforts.

The failure of a country to criminalize computer-related offenses is one such obstacle. When one country's laws criminalize certain activities on computers and another country's laws do not, cooperation in solving a crime and prosecuting the perpetrator may not be possible. That is, when a criminal weaves his communications through three, four, or five countries before reaching his intended victims, inadequate laws in just one of those countries can, in effect, shield that criminal from law enforcement around the world. Take the recent investigation of the "Love Bug" virus, for example. Although our investigators continue to work closely with investigators in the Philippines, international coordination would have proceeded more quickly and effectively had there existed common computer crime laws between our countries.

Harmonization of the laws defining criminal behavior is not enough. To enforce substantive computer crime laws, law enforcement authorities also need appropriate tools for detecting and investigating such unlawful activities. Many criminal cases today are investigated and solved through electronic evidence, which is highly perishable, and can be easily deleted or modified from half-a-world away. New technologies enable criminals to hide their identity through anonymous services, encrypt their communications, and commit crimes remotely from almost anywhere in the world. Thus, to the extent existing investigative processes are tied to particular technologies, they may need to be modified or clarified to apply to emerging technologies and challenges.

Take, for example, the importance of traceability. Often, to succeed in identifying a criminal, investigators must quickly follow a trail of communications from one point, such as a victim computer in a computer hacking case, to the computer where the criminal is located, often by tracing the communication through a number of "hops" in the communication chain. To trace this communication, law enforcement often must rely on historical transactional records - that is, stored records of the source and destination of a communication. To succeed, law enforcement must have the authority to compel industry to access or preserve log files, electronic mail records, and other critical evidence, and to do so quickly, before critical information is altered or deleted. If we cannot get this information from service providers and use it to match a crime with a source computer, the investigation may be frustrated.

When relying on historical data, we often find one of several impediments to our work. Sometimes technologies deployed in the communications infrastructure are not designed to generate the traffic data that is critical to an investigation. If that data is capable of being generated, it may not in fact be generated or, if it is generated, it may not be stored in such a manner that it exists at the time when law enforcement needs to see it.

Governments may also unintentionally hinder law enforcement efforts. When Internet service providers are required by law to delete traffic data, for example, evidence critical to a criminal investigation can be lost forever. In this regard, we are concerned by the recent proposal to extend the 1997 data protection directive to electronic communications and to expressly require service providers to delete network traffic data. While the proposed directive exempts service providers from having to destroy traffic data where there is a billing purpose for retaining it, the billing exception would rarely apply to computer traffic data. Although the billing exception, which is included in the original 1997 data directive covering telecommunications, may apply to telephone service providers because calls are generally billed on a per call basis, the same exception would rarely be applicable to Internet services - Internet services are generally sold on a flat fee or are offered for free, and therefore, Internet traffic data is not used for billing purposes. Thus, the proposed directive would result in the deletion of critical, irretrievable traffic data.

Let me briefly discuss the Article 15 law enforcement exception contained in the EU's 1997 data protection directive as well. As we have been discussing, because cyber criminals do not recognize national boundaries, inadequate investigative tools in just one country can undermine multijurisdictional law enforcement efforts. Thus, we urge the EU to ensure that public safety issues, including this important law enforcement exception, are addressed at the EU level, rather than left to the discretion of member states. Full implementation of the data protection provisions, absent adoption of consistent and strong law enforcement exceptions among member states will present significant obstacles to law enforcement, including the destruction of critical evidence and the inability to locate criminals in real time. Moreover, even with a strong law enforcement exception, the data protection provisions applied to traffic data may hinder industry's ability to protect its own systems. The transactional logs that would be covered by the mandatory deletion proposal are an invaluable tool for the private sector to monitor the integrity of their computer systems and protect them from misuse. Therefore, a critical tool for network protection would be unavailable to industry if they were required to delete logs files.

When historic transaction records are not available, investigators may also try to trace a communication in real time -- that is, attempt to identify a criminal while he or she is in the midst of communicating or committing the crime. Tracing in real time can be very complicated, particularly where the communication traverses multiple providers. Many communications technologies are not designed to facilitate tracing. The victim's computer only receives the address of the computer connected directly to it, not the address of the communication's source, and this address can be false or temporarily

hijacked. Moreover, the infrastructure of the Internet does not normally provide an automated mechanism for identifying the true source. Therefore, investigators will often have to contact individually each communications provider in the chain, to determine the source of the prior communication. When these investigations cross national borders, they often cross time zones as well. This often means that it is nighttime in at least one jurisdiction, and critical personnel may simply not be available to respond in a timely fashion to requests for information. Unfortunately, when qualified personnel are not available, the tracing operation usually ceases and the opportunity to obtain the necessary information may be lost forever.

In addition to harmonizing substantive laws and empowering law enforcement with appropriate procedural authority, countries must develop new mutual assistance regimes for investigating and prosecuting cyber crimes. Because of the perishability of evidence and the mobility of people, evidence must be gathered quickly. Existing mutual legal assistance regimes between governments are generally slow and anticipate sharing evidence among only two countries, that is, the victim's country and the offender's country. But when a criminal sends his communications through multiple countries, the processes for international assistance involve successive periods of time before law enforcement can reach data in those latter countries, increasing the chances the data will be unavailable or lost, and the criminal will remain free to attack again. Thus, we must consider new paradigms for cooperation between multiple countries and develop intergovernmental emergency networks so that investigators can communicate to other experts around the clock.

The United States and many of the EU Member States are already working hard in a number of international fora to foster better international understanding and response to computer crimes. In the Council of Europe, member states and observer states, such as the United States, Canada, and Japan, have been working hard over the last three years to draft the Convention on Cyber Crime - the first multilateral instrument drafted specifically to address the problems posed by the spread of criminal activity to global computer networks. The Convention makes progress in this area by: (1) Harmonizing the substantive laws in the area of computer crime; (2) Empowering domestic law enforcement with the procedural authority to obtain electronic evidence within their territory; and (3) Developing mechanisms for expedited international legal assistance in the investigation and prosecution of computer crimes. The Convention is scheduled to be completed by the end of this year.

The G8 nations have been interested in cooperation on cyber crime since at least January 1997. In December 1997, the G8 Justice and Interior Ministers met in Washington, D.C. and adopted 10 Principles and a 10-point Action Plan to fight cyber crime. When the Heads of the G8 nations endorsed the Principles and Plans a few months later, it was the first time that a group of Presidents and Prime Ministers agreed to a joint plan to fight cyber crime.

Participants in the G8's high-tech crime experts' group, which was founded and chaired by Scott Charney before his departure from government, have begun to develop a

comprehensive set of options for improving abilities to locate and identify criminals who abuse information technologies. These options will address such issues as data preservation and data retention, real- time tracing of communications, provider cooperation with each other and with law enforcement, and user authentication.

The G8 also established the 24/7 Point-of-Contact network, which requires participating countries to designate a 24 hour, 7 days per week Point of Contact for the purposes of providing investigative assistance in computer crime cases. Currently, almost 20 countries are participating in the network The COE Convention would expand the membership of this important international law enforcement effort.
The United States desires regular consultation with the EU in this area as well. Although representatives of the European Commission participate in the G8 Lyon Group, and Commissioner Vitorino participated in last year's G8 Ministerial, we would like to increase direct, forward-leaning dialogue between the Department of Justice and the EU on all types of high tech issues. We are particularly interested in collaborating early in the deliberative process should the EU decide to move forward on its own mutual legal assistance convention on cyber crime. We were heartened by the meeting last October during the Finnish Presidency between Attorney General Reno and the Finnish Prime Minister to discuss the results of the Tampere Summit. The Attorney General also has had the pleasure of meeting with Commissioner Vitorino several times, most recently in Brussels in July. As the Attorney General has made clear, we value our relationship with our European partners, and believe we can all benefit from early collaboration in responding to the significant challenges facing us all.

Coordination Between Components of Government
Of course, establishing mutual assistance regimes between law enforcement is not enough. Internal government policies on a range of communications, technology and e-commerce issues necessarily impact law enforcement and industry efforts to secure our networks. We believe that as these policies are developed important public safety equities must be taken into account. Positions that are nominally internal to the EU and which concern apparently non-governmental matters can nevertheless affect the practices and positions that Member States take in other international negotiations on cyber crime. For example, the data protection laws that were adopted by the EU to protect data acquired by industry in the course of transacting businesses, have recently been introduced in the Council of Europe Group of Experts on cyber crime. Such provisions are in our judgment, not appropriate to the needs of law enforcement in fighting crime. Law enforcement may have to maintain information over longer periods of time in order to understand criminal activities, develop additional leads, and corroborate information. Perhaps in recognition of these law enforcement equities, existing data protection instruments generally contain law enforcement and other "important public interest" exemptions. Moreover, regulations adopted in the EU are not necessarily appropriate for the large and diverse group of countries that belong to the Council of Europe, who have different legal frameworks and institutions on these sensitive, complex issues.

We realize, however, that rules and regulations designed to protect public safety must also be carefully tailored to accomplish their objectives without unintended consequences, such as stifling the growth of the Internet or chilling open communication. Triumph over network crime cannot and must not come at the price of the much-cherished individual liberties of the citizens of our respective countries. We must strive to avoid a hollow victory over crime at the price of lost privacy and individual freedom. Therefore, the different components in our governments who lead the charge in protecting privacy, supporting legitimate commerce, and investigating and prosecuting cyber crimes, must work together to achieve the delicate balance between these sometimes competing interests.

In this regard, the Department of Justice would welcome regular discussions with the European Union at all levels. Moreover, we pledge reciprocal willingness to discuss U.S. law enforcement proposals that may implicate your concerns. By consulting with each other early in the deliberative processes, we can learn from each other's experiences and share our ideas.

Forging a Partnership with Industry

Governments, even working together, cannot meet these challenges alone. Cooperation with industry is critical. Government and the private sector each have important roles to play in ensuring a safe and secure online environment. Industry can and should take the lead in protecting private computer networks through vigilant security efforts and cooperation with government agencies. Not only does industry design, build and operate the infrastructure, systems, and related technologies that connect us, it has the know-how and resources to address these needs. Government, in turn, must take steps to protect its own computer systems, and to ensure that unnecessary legal barriers to industry's efforts are removed. When cyber crimes occur, which they will, law enforcement is responsible for investigating and bringing those responsible to justice. To investigate these cases effectively, however, governments may be dependent on industry for its expertise and for sharing information. Thus, the success of our partnership will depend on the trust, expertise and support of the private sector.

Finally, we must also form a partnership to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. In the United States, industry and government formed the Cybercitizen Partnership last year to focus national attention on cyber social behavior and the importance of teaching young computer users to recognize that, in addition to protecting themselves from potentially dangerous threats on the Internet, the same standards of ethics expected in the off-line world apply to the online world. In short, our citizenry must understand that, when online, they are responsible for their own actions and that these actions have consequences both for themselves and others.

Conclusion

As I conclude, I note that in this room this afternoon are many of the distinguished industry experts and government leaders who must play a role in meeting the challenges of cyber crime. Although we often serve different societal interests, we meet here today

with one common goal: to keep our countries' computer networks safe, secure and reliable for our citizens and businesses. I hope that we can keep these lines of communications open and consult more regularly. Thank you.