KEYNOTE ADDRESS BY
U.S. ATTORNEY GENERAL JANET RENO ON
HIGH-TECH AND COMPUATE CRIME

Delivered at the Meeting of the P8 Senior
Experts' Group on
Transnational Organized Crime

Tuesday, January 21, 1997
Chantilly, Virginia

ATTORNEY GENERAL RENO: Thank you, Mark. I'm very touchedby that introduction and I hope I can live up to it. I want towelcome you all to the United States for this first Plenary sessionof 1997. I am very pleased to be with you today.

Not only is this meeting the first P8 meeting under the U.S.Presidency, it is the first multilateral meeting of PresidentClinton's second Administration.

As you know, yesterday the President took the oath of officefor his second term. His reelection brings with it the opportunityfor me to continue to work with international and domestic lawenforcement to bring security to the citizens of our countries,and I consider this a very special privilege.

Besides the historic significance of this day, I want toshare with you the excitement and the enthusiasm I feel aboutand toward the P8. I view this group like no other: The P8 countriesare a special group made up of the world's most powerful democracies. We are global leaders in so many ways economically, technologically,legally, and politically. Our small number allows us to act quickly,and our unique membership offers an opportunity to lead the worldcommunity that is rarely found in our history. And we are oftenon the cutting edge for example in responding to internationalterrorism, to international money laundering, to precursor chemicals. This group has so much promise. Through your work, giant stridesare being made in several critical areas that have significantglobal implications.

No area of criminal activity is more on the cutting edgeor has greater global implications than crime involving technologyand computers. The importance of emerging technologies and thesignificance of global computer networks cannot be overstated. If properly developed and properly protected, they will be usedin virtually all personal communications, financial transactions,information sharing, medical care, and a myriad of other applications. It is, indeed, a very exciting time.

But while new technologies allow us to do things that werepreviously impossible, they can also be misused in creative waysto threaten public safety and national security. The same technologiesthat facilitate lightningfast and ultrareliable transactions betweencomputers can be misused by hackers, that is, by those who accesscomputers without or in excess of authority. They can accessconfidential information, steal economic data, disrupt telephonenetworks, and interfere with the delivery of government and othervital services.

So while the information age holds great promise, law enforcementhas a responsibility to ensure that the users of networks arenot victimized in new ways.
To protect honest, law abiding citizens, law enforcementmust keep pace with advances in computer and telecommunicationstechnologies. We must work to ensure that the international lawenforcement community can keep pace with the criminals. Thisis especially true in the case of computer offenses, which differfrom traditional crimes in a number of ways and, as a result,create new and very challenging problems:
First, international computer crimes are easier to commit. Hackers are not hampered by the existence of international boundaries,since information and property can be transmitted covertly viatelephone and data networks. A hacker needs no passport and passesno checkpoints. He simply types a command to gain entry. Andthere is little need for manpower since a sole hacker, workingalone, can effectively steal or erase as much information as hecan read, or he can cause extensive damage to global networks.
Secondly, until recently, computer crime has not receivedthe emphasis that other international crimes have engendered. Even now, not all affected nations recognize the threat it posesto public safety or the need for international cooperation toeffectively respond to the problem. Consequently, many countrieshave weak laws, or no laws, against computer hacking a majorobstacle to solving and to prosecuting computer crimes.
Thirdly, law enforcement faces new procedural challenges,many of which are impossible to address without internationalconsensus and cooperation. Consider, if you will, merely locatinga hacker whose transmission passes from his computer to a localservice provider, then through a telephone network, then crossesan ocean via satellite, and then passes through a university computeron its way to a corporate victim. To make matters worse, thishacker could be in his car, using wireless communications. Howdo we go about finding this individual? How do we collect theevidence and preserve it in a way that will be useful at trial?
Fourth, law enforcement will be faced with significant technicalchallenges, such as the widespread use of encryption. In suchcases, we will have to find innovative and effective ways to preservegovernment access to the plain text of encrypted data. We cando this, in part, by supporting international efforts and nationalpolicies which promote the development of the emerging key managementinfrastructure and the use of products which allow for data recovery,as well as by assisting each other in this very difficult area.
I think that these threats and these problems call for theparticular experience and the expertise of this group. Whileimportant work in the high-tech area is being done under the auspicesof other organizations, one thing that sets the P8 apart fromother multilateral groups is its commonsense focus on practicalsolutions.
And the great thing about practical solutions is that theyusually produce real results.
Since computer crime is so importantto all of our interests, there are several areas that I hope P8Experts will address. First, we need adequate laws which willallow us to prosecute hackers and other computer criminals. Second,we need the technical ability to find these individuals, whereverlocated. Third, we must develop legal procedures that permittimely cooperation in the collection of evidence. And fourth,we need to train law enforcement personnel and devote these technicallyliterate experts to the task at hand.
When countries have inadequate legal structures to combatcomputer crimes, they provide safe havens for computer criminals,and they can create a major obstacle to obtaining internationalassistance in multijurisdictional cases. As you know, in 1990,the Council of

Europe recommended that European nations adoptharmonious computer crime laws. As a result, several P8 countrieshave enacted new laws and joined international efforts to encourageother countries to enact or to strengthen their computer crimelaws. However, much work remains to be done in this area.

We need to reach a consensus as to which computer and technologyrelatedactivities should be criminalized, and then commit to taking appropriatedomestic actions. This would also aid in providing the inevitablelegal assistance required to investigate and prosecute these cases. I think it is also important to think about a global legal supportregime, which could be used to avoid ad hoc approaches to multipleprosecutions. The unique nature of computer crimes and the unusualproblems that can result would make such a regime very useful. Further, it would provide practical solutions as countries determinethe best place for a prosecution, the order of prosecutions ina case where multiple countries are affected, and the most fairway to vindicate interests when a crime affects a large numberof nations.

When a hacker attacks, the first investigative step is tolocate the source of the attack. To do so requires tracing theelectronic trail from the victim back to the attacker. However,in today's communications environment, one telecommunicationscarrier does not carry a communication from end to end. As inthe example I mentioned before, a hacker's communication willpass through an array of carriers, often in less than a second,and tracing the electronic trail from victim back to attackermay be difficult or impossible unless the hacker is actually online.

One practical solution that our technologically advancedcountries should pursue is maintaining access to source informationfor each link in the chain of transmission. Some countries, includingthe United States, have required that technical standards be adoptedwhich ensure that "call setup information" for normaltelephone calls is accessible, so that the source of the callcan be identified. I think it would be productive for P8 Expertsto consider whether all carriers should carry this kind of information,whether other communications technologies should be similarlydesigned, and what would be required for countries to share thisinformation with one another. This is a critical time for thisissue, as all of us are upgrading our telecommunications systems,because it is far easier to build such requirements into new machinesrather than to retrofit existing equipment.

Finding a criminal who plies his craft through an array ofcarriers becomes much more challenging when wireless communicationsare used. In the past, when a perpetrator used a phone to commita crime, law enforcement could easily find out the exact locationthat the call came from. They could find out the name of theperson who was being billed for the phone line, because the callerwould be physically attached to a telephone wire. But today,mobile phones can allow an individual to commit crimes while roamingaround a city or even a country.

Even identifying the owner of a particular mobile phone maybe difficult, because mobile phones can be altered to transmitphony identifying information. Here, as in most of the areaswe discuss, governments would be wellserved to work on this problemwith the help of industry. Our technical experts tell us thatthere are practical solutions to the problems created by wirelesscommunications, such as encouraging the encryption of cellularelectronic identifiers. I hope that P8 Experts will work to seethat law enforcement is not overtaken by technology in this area,but instead uses technology to thwart crime.

As the globalization of computer networks continues, andas computer criminals become more sophisticated, law enforcementincreasingly will need timely access to computer or telecommunicationsinformation in all our countries. Up until this point, our regimeof mutual legal assistance has served our countries well. Butin a hacker case, the trail of evidence sometimes ends abruptlyand permanently as soon as the hacker goes offline. We shouldconsider whether mutual legal assistance treaties and lettersrogatory need to be supplemented with procedures that will facilitatethe immediate collection and review of evidence, or whether otheravenues should be explored. As mechanisms are developed, speciallytrained lawyers within countries' Central Authorities may be necessaryto ensure rapid response to requests for assistance, particularlywhile a hacker is online. Again, the experience and the expertiseof the P8 makes it wellsuited to tackle these very difficult problems.Practical solutions are out there we must work together to findthem.

One idea I believe worthy of consideration is formalizinginternational expedited procedures that protect electronic evidenceon foreign soil from alteration or destruction. These could bein the form of "preservation of evidence requests,"or "protected seizures," whereby an international requestfreezes a scene until a domestic judicial search mechanism canbe used. Just like technological advances are the product ofcreativity and ingenuity, our legal work in this area must likewisebe imaginative and forwardleaning. Also in the area of evidence collection, I encourage thisgroup to address the issues involved in analyzing electronic evidence evidence which can be easily altered or destroyed. We must beable to analyze this evidence in ways that preserve its integrityand make its authenticity irrefutable, both for purposes of domesticprosecution and international cooperation. The ease with whichdigital evidence can be manipulated has already led to the developmentof scientific protocols for searching computers and for analyzingdata. But we now must strive to ensure that such procedures areinternationally accepted.

None of the advances I have discussed are possible withoutensuring that law enforcement personnel are capable of addressinghigh-tech crime by understanding two emerging and converging technologiessimultaneously: Computers and telecommunications. The complexityof these technologies, and their constant and rapid change, suggestthat countries need to designate investigators and prosecutorsto receive appropriate and ongoing training. They, in turn, needto work these cases on a fulltime basis, immersing themselvesin computerrelated investigations and prosecutions. Efforts alongthese lines will dramatically expand enforcement capabilitiesto solve high-tech crimes. I hope that when you return home, eachof you will strongly advocate devoting significant resources tothis area, and that we can share our expertise through internationaltraining and coordination efforts.

The issues confronting us are very, very difficult, but wecan solve them. What will make it all come together in a cohesiveway is law enforcement's continued willingness to recognize thenew challenges that lay ahead in cyberspace. Whether the challengeis protecting trade secret information, defending intellectualproperty rights, prosecuting an international hacker, if we doour job right, the people of the world will enjoy the benefitsof the information age without becoming its victims.

In closing, I pledge to you my full support in this verycritical area. I consider high-tech crime to be one of the mostserious issues demanding my attention, and I am doing everythingin my power to ensure that the United States actively respondsto these

challenges. I have instructed Mark Richard to keep meapprised of your work, and I would enjoy the opportunity to contactmy counterparts in your countries, if and when the need arises. In fact, this past November, I discussed the threat of high-techcrime with the British Home Secretary, Michael Howard, and heenthusiastically pledged his support to P8 efforts in this area. Likewise, our Deputy Attorney General had a similar meeting withthe German State Secretary of the Interior, Professor Doctor KurtSchelter, in October of last year. It's an old cliche, but unitedwe stand; divided we fall, and we look forward to working withyou in every way we can to address this very important and verycomplex issue.

Thank you.