Email this Document!

Computer Crime and Intellectual Property Section (CCIPS)

Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001

Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations

Previous law: Under previous law, investigators could not obtain a wiretap order to intercept wire communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). For example, in several investigations, hackers have stolen teleconferencing services from a telephone company and used this mode of communication to plan and execute hacking attacks.

Amendment: Section 202 amends 18 U.S.C. § 2516(1) the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications by adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses.1 This provision will sunset December 31, 2005.

Section 209 Obtaining Voice-mail and Other Stored Voice Communications

Previous law: Under previous law, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal s home.

Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

Moreover, in large part, the statutory framework envisions a world in which technology-mediated voice communications (such as telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might co-exist in a single transaction, it did not anticipate the convergence of these two kinds of communications typical of today s telecommunications networks. With the advent of MIME Multipurpose Internet Mail Extensions and similar features, an e-mail may include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect s unopened e-mail from an ISP by

means of a search warrant (as required under 18 U.S.C. § 2703(a)) had no way of knowing whether the inbox messages include voice attachments (i.e., wire communications) which could not be compelled using a search warrant.

Amendment: Section 209 of the Act alters the way in which the wiretap statute and ECPA apply to stored voice communications.2 The amendments delete "electronic storage" of wire communications from the definition of "wire communication" in section 2510 and insert language in section 2703 to ensure that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

This provision will sunset December 31, 2005.

Section 210 Scope of Subpoenas for Electronic Evidence

Previous law: Subsection2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer s name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer s true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity.

Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included "local and long distance telephone toll billing records," but did not include parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the previous list allowed the government to use a subpoena to obtain the customer s "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet communications.

Amendment: Amendments to section 2703(c) update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

Moreover, the amendments clarify that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number." 18 U.S.C. §2703(c)(2)(F). While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users biographical information. (This section is not subject to the sunset provision in section 224 of the Act).

Section 211 Clarifying the Scope of the Cable Act

Previous law: The law contains two different sets of rules regarding privacy protection of communications and their disclosure to law enforcement: one governing cable service (the "Cable Act") (47 U.S.C. § 551), and the other applying to the use of telephone service and Internet access (the wiretap statute, 18 U.S.C. § 2510 et seq.; ECPA, 18 U.S.C. § 2701 et seq.; and the pen register and trap and trace statute (the "pen/trap" statute), 18 U.S.C. § 3121 et seq.).

Prior to the amendments in Section 211 of the Act, the Cable Act set out an extremely restrictive system of rules governing law enforcement access to most records possessed by a cable company. For example, the Cable Act did not allow the use of subpoenas or even search warrants to obtain such records. Instead, the cable company had to provide prior notice to the customer (even if he or she were the target of the investigation), and the government had to allow the customer to appear in court with an attorney and then justify to the court the investigative need to obtain the records. The court could then order disclosure of the records only if it found by "clear and convincing evidence" a standard greater than probable cause or even a preponderance of the evidence that the subscriber was "reasonably suspected" of engaging in criminal activity. This procedure was completely unworkable for virtually any criminal investigation.

The legal regime created by the Cable Act caused grave difficulties in criminal investigations because today, unlike in 1984 when Congress passed the Cable Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. In recent years, some cable companies have refused to accept subpoenas and court orders pursuant to the pen/trap statute and ECPA, noting the seeming inconsistency of these statutes with the Cable Act s harsh restrictions. See In re Application of United States, 36 F. Supp. 2d 430 (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) for records from cable company providing Internet service). Treating identical records differently depending on the technology used to access the Internet made little sense. Moreover, these complications at times delayed or ended important investigations.

Amendment: Section 211 of the Act amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services such as telephone and Internet services. The amendment preserves, however, the Cable Act s primacy with respect to records revealing what ordinary cable television programing a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can use legal process under ECPA to compel the provider to disclose only those customer records relating to Internet service. (This section is not subject to the sunset provision in Section 224 of the Act).

Section 212 Emergency Disclosures by Communications Providers

Previous law: Previous law relating to voluntary disclosures by communication service providers was inadequate in two respects. First, it contained no special provision allowing providers to disclose customer records or communications in emergencies. If, for example, an Internet service provider ("ISP") independently learned that one of its customers was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the account information to law enforcement could save lives. Since providing this information did not fall within one of the statutory exceptions, however, an ISP making such a disclosure could be sued civilly.

Second, prior to the Act, the law did not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber s login records) to law enforcement for purposes of self-protection, even though providers could disclose the content of communications for this reason. See 18 U.S.C. § 2702(b)(5), 2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company s authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter, providers must have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP s customer hacks into the ISP s network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime to law enforcement.

Amendment: Section 212 corrects both of these inadequacies in previous law. Section 212 amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers.

The amendments in Section 212 of the Act also change ECPA to allow providers to disclose information to protect their rights and property. It accomplishes this change by two related sets of amendments. First, amendments to sections 2702 and 2703 of title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers do have the statutory authority to disclose non-content records to protect their rights and property. All of these changes will sunset December 31, 2005.

Section 216 Pen Register and Trap and Trace Statute

The pen register and trap and trace statute (the "pen/trap" statute) governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI s DCS1000) on computers belonging to a public provider. The following sections discuss these provisions in greater detail. (This section is not subject to the sunset provision in Section 224 of the Act).

A. Using pen/trap orders to trace communications on computer networks

Previous law: When Congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks.3 Although numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute s telephone-specific language.

Amendment: Section 216 of the Act amends sections 3121, 3123, 3124, and 3127 of title 18 to clarify that the pen/trap statute applies to a broad variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, amendments to section 3123(b)(1)(C) now allow applicants for pen/trap orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information all "dialing, routing, addressing, and signaling information" utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Agents and prosecutors with questions about whether a particular type of information constitutes

content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Further, because the pen register or trap and trace "device" often cannot be physically "attached" to the target facility, Section 216 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap and trace device to be "attached or applied" to the target facility. Likewise, Section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

B. Nationwide effect of pen/trap orders

Previous law: Under previous law, a court could only authorize the installation of a pen/trap device "within the jurisdiction of the court." Because of deregulation in the telecommunications industry, however, a single communication may be carried by many providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a string of providers located throughout the country each requiring a separate order.

Moreover, since, under previous law, a court could only authorize the installation of a pen/trap device within its own jurisdiction, when one provider indicated that the source of a communication was a different carrier in another district, a second order in the new district became necessary. This order had to be acquired by a supporting prosecutor in the new district from a local federal judge neither of whom had any other interest in the case. Indeed, in one case investigators needed three separate orders to trace a hacker s communications. This duplicative process of obtaining a separate order for each link in the communications chain has delayed or given the difficulty of real-time tracing completely thwarted important investigations.

Amendment: Section 216 of the Act divides section 3123 of title 18 into two separate provisions. New subsection (a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor s local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication s path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

The amendments in Section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia

uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

Consistent with the change above, Section 216 of the Act modifies section 3123(b)(1)(C) of title 18 to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal pen/trap orders, an amendment to section 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

C. Reports for use of law enforcement pen/trap devices on computer networks

Section 216 of the Act also contains an additional requirement for the use of pen/trap devices in a narrow class of cases. Generally, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, the provider itself should be able to collect the needed information and provide it to law enforcement. In certain rare cases, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI s DCS1000) to collect the information. In these infrequent cases, the amendments in section 216 require the law enforcement agency to provide the following information to the court under seal within thirty days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. 18 U.S.C. § 3123(a)(3).

Section 217 Intercepting the Communications of Computer Trespassers

Prior law: Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a "wire or electronic communication" according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a "bizarre result," in which a "computer hacker s undeserved statutory privacy right trumps the legitimate privacy rights of the hacker s victims." Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Amendment: To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser s communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth,

section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of "computer trespasser." Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18)4 without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider s terms of service, but would not qualify as trespassers both because they are authorized users and because they have an existing contractual relationship with the provider. These provisions will sunset December 31, 2005.

Section 220 Nationwide Search Warrants for E-mail

Previous law: Section 2703(a) requires the government to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. Because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained be "within the district" of the issuing court, however, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations.

Amendment: Section 220 of the Act amends section 2703(a) of title 18 (and parallel provisions elsewhere in section 2703) to allow investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d). This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located. This provision will sunset December 31, 2005.

Section 814 Deterrence and Prevention of Cyberterrorism

Section 814 makes a number of changes to improve 18 U.S.C. § 1030, the Computer Fraud and Abuse Act. This section increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker s course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold.

The following discussion analyzes these and other provisions in more detail.

A. Section 1030(c) - Raising the maximum penalty for hackers that damage protected computers and eliminating mandatory minimums

Previous law: Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no

more than five years imprisonment, while repeat offenders could receive up to ten years. Certain offenders, however, can cause such severe damage to protected computers that this five-year maximum did not adequately take into account the seriousness of their crimes. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times that amount.

In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

Amendment: Section 814 of the Act raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders. 18 U.S.C. § 1030(c)(4). Congress chose, however, to eliminate all mandatory minimum guidelines sentencing for section 1030 violations.

B. Subsection 1030(c)(2)(C) and (e)(8) - Hackers need only intend to cause damage, not a particular consequence or degree of damage

Previous law: Under previous law, in order to violate subsections (a)(5)(A), an offender had to "intentionally [cause] damage without authorization." Section 1030 defined "damage" as impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least $5,000; (2) modified or impairs medical treatment; (3) caused physical injury; or (4) threatened public health or safety.

The question repeatedly arose, however, whether an offender must *intend* the $5,000 loss or other special harm, or whether a violation occurs if the person only intends to damage the computer, *that in fact* ends up causing the $5,000 loss or harming the individuals. It appears that Congress never intended that the language contained in the definition of "damage" would create additional elements of proof of the actor s mental state. Moreover, in most cases, it would be almost impossible to prove this additional intent.

Amendment: Section 814 of the Act restructures the statute to make clear that an individual need only intend to damage the computer or the information on it, and not a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8) (emphasis supplied). Under this clarified structure, in order for the government to prove a violation of 1030(a)(5), it must show that the actor caused damage to a protected computer (with one of the listed mental states), and that the actor s conduct caused either loss exceeding $5,000, impairment of medical records, harm to a person, or threat to public safety. 18 U.S.C. § 1030(a)(5)(B).

C. Section 1030(c) - Aggregating the damage caused by a hacker s entire course of conduct

Previous law: Previous law was unclear about whether the government could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional threshold of $5,000 in loss. For example, an individual could unlawfully access five computers on a network on ten different dates as part of a related course of conduct but cause only $1,000 loss to each computer during each intrusion. If previous law were interpreted not to allow aggregation, then that person would not have committed a federal crime at all since he or she had not caused over $5,000 to any particular computer.

Amendment: Under the amendments in Section 814 of the Act, the government may now aggregate "loss resulting from a related course of conduct affecting one or more other protected computers" that occurs within a one year

period in proving the $5,000 jurisdictional threshold for damaging a protected computer. 18 U.S.C. § 1030(a)(5)(B)(i).

D. 1030(c)(2)(C) - New offense for damaging computers used for national security and criminal justice

Previous law: Section 1030 previously had no special provision that would enhance punishment for hackers who damage computers used in furtherance of the administration of justice, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over $5,000 loss (or meet one of the other special requirements). Yet these systems serve critical functions and merit felony prosecutions even where the damage is relatively slight. Indeed, attacks on computers used in the national defense that occur during periods of active military engagement are particularly serious even if they do not cause extensive damage or disrupt the war-fighting capabilities of the military because they divert time and attention away from the military s proper objectives. Similarly, disruption of court computer systems and data could seriously impair the integrity of the criminal justice system.

Amendment: Amendments in Section 814 of the Act create section 1030(a)(5)(B)(v) to solve this inadequacy. Under this provision, a hacker violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over $5,000.

E. Subsection 1030(e)(2) - expanding the definition of "protected computer" to include computers in foreign countries

Previous law: Before the amendments in Section 814 of the Act, section 1030 of title 18 defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). The definition did not explicitly include computers outside the United States.

Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Amendment: Section 814 of the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.

In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.

F. Subsection 1030(e)(10) - counting state convictions as "prior offenses"

Previous law: Under previous law, the court at sentencing could, of course, consider the offender s prior convictions for State computer crime offenses. State convictions, however, did not trigger the recidivist sentencing

provisions of section 1030, which double the maximum penalties available under the statute.

Amendment: Section 814 of the Act alters the definition of "conviction" so that it includes convictions for serious computer hacking crimes under State law i.e., State felonies where an element of the offense is "unauthorized access, or exceeding authorized access, to a computer." 18 U.S.C. § 1030(e)(10).

G. Subsection 1030(e)(11) -- Definition of "loss"

Previous law: Calculating "loss" is important where the government seeks to prove that an individual caused over $5,000 loss in order to meet the jurisdictional requirements found in 1030(a)(5)(B)(i). Yet prior to the amendments in Section 814 of the Act, section 1030 of title 18 had no definition of "loss." The only court to address the scope of the definition of loss adopted an inclusive reading of what costs the government may include. In United States v. Middleton, 231 F.3d 1207, 1210-11 (9th Cir. 2000), the court held that the definition of loss includes a wide range of harms typically suffered by the victims of computer crimes, including costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of interruption of service.

Amendments: Amendments in Section 814 codify the appropriately broad definition of loss adopted in Middleton. 18 U.S.C. § 1030(e)(11).

Section 815 Additional Defense to Civil Actions Relating to Preserving Records in Response to government Requests

Section 815 added to an existing defense to a cause for damages for violations of the Electronic Communications Privacy Act, Chapter 121 of Title 18. Under prior law it was a defense to such a cause of action to rely in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. This amendment makes clear that the "statutory authorization" defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. § 2703(f).

Section 816 Development and Support of Cybersecurity Forensic Capabilities

Section 816 requires the Attorney General to establish such regional computer forensic laboratories as he considers appropriate, and to provide support for existing computer forensic laboratories, to enable them to provide certain forensic and training capabilities. The provision also authorizes the spending of money to support those laboratories.

###

- **More information on: Computer Crime Laws**
- **More information on: Computer Crime Guidance**
- **More information on: Searching and Seizing Computers**
- **More information on: Federal Code Related to Cybercrime**

Go to . . . **CCIPS Home Page** || **Justice Department Home Page**

Last updated November 05, 2001 usdoj-crm/mis/jam