Field Guidance on New Authorities (Redacted)
Enacted in the 2001 Anti-Terrorism Legislation

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

[1] This amendment does not affect applications to intercept *electronic* communications in hacking investigations. As before, investigators may base an application to intercept electronic communications on any federal felony criminal violation. 18 U.S.C. § 2516(3).

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: Subsection 2703(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.

---

[2] Note that these changes do not apply to voice messages in the possession of the user, such as the answering machine tape in a person's home. Those types of records remain outside of the statute.

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 213 Authority for Delaying Notice of the Execution of a Warrant

Prior law governing the delayed provision of notice that a warrant had been executed was a mix of inconsistent rules, practices, and court decisions varying widely from jurisdiction to jurisdiction across the country. The lack of uniformity hindered the investigation of terrorism cases and other nationwide investigations.

Section 213 resolved this problem by amending 18 U.S.C. § 3103a to create a uniform statutory standard authorizing courts to delay the provision of required notice if the court finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have an adverse result as defined by 18 U.S.C. § 2705 (including endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial). The section provides for the giving of notice within a "reasonable period" of a warrant's execution, which period can be further extended by a court for good cause.

This section is primarily designed to authorize delayed notice of *searches*, rather than delayed notice of *seizures*: the provision requires that any warrant issued under it must prohibit the seizure of any tangible property, any wire or electronic communication, or, except as expressly provided in chapter 121, any stored wire or electronic information, unless the court finds "reasonable necessity" for the seizure.

The "reasonable cause" standard adopted by the provision is in accord with prevailing caselaw for delayed notice of warrants. *See United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants). It is also in accord with the standards for exceptions to the general requirements that agents knock and announce themselves before entering and that warrants be executed during the daytime. *See Richards v. Wisconsin*, 520 U.S. 385 (1997) (no-knock entry to execute warrant is justified when the police have "reasonable suspicion" that knocking and announcing their presence would be dangerous or futile or would inhibit the effective investigation); Fed. R. Crim. P. 41(c)(1) ("The warrant shall be served in the daytime unless the issuing authority, by appropriate provision of the warrants, and for reasonable cause shown, authorizes its execution at times other than daytime.").

The requirement of notice within a "reasonable period" is a flexible standard to meet the circumstances of the case. *Villegas*, 899 F.2d at 1337 ("What constitutes a reasonable time will depend on the circumstances of each individual case"). Analogy to other statutes suggest that the period of delay could be substantial if circumstances warrant. *See* 18 U.S.C. § 2518(8)(d) (notice of a wiretap may be delayed for "a reasonable time" but not more than 90 days after the termination of the wiretap); *cf. United States v. Allie*, 978 F.2d 1401, 1405 (5th Cir. 1992) (suggesting that 60 days is a "reasonable period" for purposes of detaining a material witness under 18 U.S.C. § 3144). Caselaw regarding a "reasonable" period for delayed notice of warrants is still developing. The Second Circuit has interpreted it to ordinarily mean a seven-day initial delay, although subject to additional extensions. *Villegas*, 899 F.2d at 1337. The Ninth Circuit, although relying on the argument that the Constitution itself required prompt notice (*but see United States v. Pangburn*, 983 F.2d 449, 454-455 (2d Cir.1993); *Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (45-day delay in notice of execution of warrant does not render search unconstitutional)), also has held that delays ordinarily should not exceed seven days. *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) ("Such time should not exceed seven days

except upon a strong showing of necessity."). Other courts have suggested that a "reasonable period" could be significantly longer. *Cf. Simons*, 206 F.3d 392, 403 (45-day delay in notice of execution of search warrant did not render search unconstitutional).

The "reasonable necessity" standard for seizing items during the search is not well developed in the caselaw. The Second Circuit and other courts have equated the phrase "reasonable necessity" with "good reason" in the context of delayed notice. *Villegas*, 899 F.2d at 1337; *United States v. Ludwig*, 902 F. Supp 121, 126 (W.D. Tex. 1995); *accord United States v. Ibarra*, 725 F. Supp. 1195, 1200 (D. Wyo. 1989) ("reasonable necessity" to impound a vehicle).

In the weeks ahead, the Department may be providing additional guidance with respect to the use of this delayed notice provision. The Department expects that delayed notice will continue to be an infrequent exception to the general rule that notice of the execution of a warrant will be provided promptly.

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.

[3] For example, the statute defined "pen register" as "a device which records or decodes electronic or other impulses which identify the *numbers dialed* or otherwise transmitted on the *telephone line* to which such device is *attached*." 18 U.S.C. § 3127(3) (emphasis supplied).

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.

A. 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 219 Single-Jurisdiction Search Warrants for Terrorism

Under prior law, Rule 41(a) of the Federal Rules of Criminal Procedure required that a search warrant be obtained within a district for searches within that district. The only exception was for cases in which property or a person within the district might leave the district prior to execution of the warrant. The rule created unnecessary delays and burdens for the government in the investigation of terrorist activities and networks that spanned a number of districts, since warrants must be separately obtained in each district.

Section 219 resolves that problem by providing that, in domestic or international terrorism cases, a search warrant may be issued by a magistrate judge in any district in which activities related to the terrorism have occurred for a search of property or persons located within or outside of the district.

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

[4] Section 1030 defines a protected computer as any computer used in interstate or foreign commerce, as well as most computers used by financial institutions or the U.S. Government. Thus, almost any computer connected to the Internet qualifies as a "protected computer."

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 315 Inclusion of Foreign Corruption Offenses as Money Laundering Crimes

Until now, the only foreign crimes listed as predicates for money laundering under 18 U.S.C. §§ 1956 and 1957 were drug trafficking, bank fraud, and certain crimes of violence including murder, kidnaping, robbery, extortion and use of explosives. *See* 18 U.S.C. § 1956(c)(7)(B). Section 315 expands the list to include any crime of violence, bribery of a public official or misappropriation of public funds, smuggling munitions or technology with military applications, and any "offense with respect to which the United States would be obligated by multilateral treaty" to extradite or prosecute the offender.

By adding these offenses to the definition of "specified unlawful activity," Congress makes it possible to prosecute any person who conducts a financial transaction in the United States involving the proceeds of such offense with the requisite specific intent (or with no such intent if, as provided in section 1957, more than $10,000 is involved). Moreover, under section 1956(a)(2)(A), it will be an offense to send any money from any source into or out of the United States with the intent to promote one of the foreign offenses.

Section 316 Anti-Terrorist Forfeiture Protection

This section provides certain procedural protections to owners of property confiscated under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1702 et seq., as assets of suspected international terrorists. The provision allows the owner of such property to interpose the defense that the property is not subject to confiscation under IEEPA and the "innocent owner" defense of 18 U.S.C. § 983(c). Finally, this section also exempts confiscations from the requirements of the Civil Asset Forfeiture Reform Act of 2000 (CAFRA).

Section 317 Long-arm Jurisdiction Over Foreign Money Launderers

Section 1956(b) creates a civil cause of action by the government against any person who commits a money laundering offense. It is an alternative to a criminal prosecution under section 1956(a) that is sometimes used when the offender is a corporation (including a bank) against whom a criminal prosecution is of less importance than a finding of liability and the imposition of a monetary penalty.

One defect in prior section 1956(b) was that it created a cause of action only for violations of section 1956(a). As amended by section 317, section 1956(b) now permits the government to base its case on a violation of section 1957, which in many instances will be easier for the government to prove.

Second, under prior law there was some question whether the government could bring a section 1956(b) lawsuit against a foreign person, including a foreign bank, that committed a money laundering offense but could not be found in the United States. For example, if employees of a Mexican bank conducted financial transactions that constituted a violation of section 1956(a), and the government wanted to file a lawsuit against the Mexican bank under section 1956(b), there was uncertainty whether the bank would be subject to the jurisdiction of a U.S. court if it had no physical presence in the United States. As amended, section 1956(b) now provides that the court has jurisdiction if the money laundering offense occurred in part in the United States, or the foreign bank has a correspondent account in the United States.

Third, section 1956(b) was amended to permit a court to take jurisdiction over an action brought by the government to enforce a forfeiture judgment based on a violation of section 1956. Section 317 provides that if property is ordered forfeited under section 982(a)(1), based on a violation of section 1956, and the government files a lawsuit against a foreign person who has converted that forfeited property to his own use instead of turning it over to the government, the district court will have jurisdiction over the foreign person. What the amendment does is to eliminate any uncertainty over what circumstances will permit a court to exercise long-arm jurisdiction in such cases.

Finally, section 317 amends section 1956(b) to authorize a court to enter a restraining order to ensure "that any bank account or other property held by the defendant in the United States is available to satisfy a judgment under this section." The court is also authorized to appoint, at the request of the Attorney General, a receiver to manage assets in three categories of cases: 1) where assets are subject to a civil penalty under section 1956(b); 2) where assets are subject to any civil or criminal forfeiture under sections 981 or 982; and 3) where assets are subject to a restitution order in a section 1956 or 1957 criminal case. This authority – both to enter restraining orders and to appoint receivers – appears to be limited, however, to cases in which the court is exercising its long-arm authority over a foreign person.

Section 318 Laundering Money Through a Foreign Bank

18 U.S.C. § 1956 prohibits conducting a transaction involving a financial institution if the transaction involves criminally derived property. Similarly, section 1957 creates an offense relating to the deposit, withdrawal, transfer or exchange of criminally derived funds "by, to or through a financial institution." Both statutes employ the definition of "financial institution" found in 31 U.S.C. § 5312. See 18 U.S.C. § 1956(c)(6); 18 U.S.C. § 1957(f).

Under prior law, the definition of "financial institution" did not explicitly include foreign banks. Such banks arguably were within the meaning of "commercial bank" or other terms in the statute, but there was some confusion over whether the government could rely on section 5312 to prosecute an offense under either section 1956 or 1957 involving a transaction through a foreign bank, even if the offense occurred in part in the

United States. Section 318 ends the confusion by explicitly including foreign banks within the definition of "financial institution" in section 1956(c)(6).

Section 319 Forfeiture of Funds in United States Interbank Accounts

It is quite common for foreign criminals to deposit money derived from crimes committed in the United States into foreign bank accounts. This is often done by depositing the money directly into the correspondent account that a foreign bank maintains at another bank in the United States. When the government tries to seize and forfeit the money in the correspondent account, however, the foreign bank, which is considered the owner of the funds in its correspondent account, is able to assert an innocent owner defense under 18 U.S.C. § 983(d). In Section 319, Congress has addressed this problem by creating a new provision codified as 18 U.S.C. § 981(k).

Section 981(k)(1) provides that if funds are deposited into an account in a foreign bank, and that foreign bank has a correspondent account in the United States, "the funds deposited into the [foreign bank] shall be deemed to have been deposited into the correspondent account in the United States," and the government may seize, arrest or restrain the funds in the correspondent account "up to the value of the funds deposited" into the foreign bank. Moreover, section 981(k)(2) provides that when a forfeiture action is brought against those funds, "the government shall not be required to establish that such funds are directly traceable to the funds [that were deposited into the foreign bank], nor shall it be necessary for the government to rely on the application of Section 984." Thus, if a drug dealer deposits funds into a foreign bank that has a correspondent account in the United States, the government can now seize and bring a forfeiture action against an equivalent sum of money in the correspondent account, regardless of whether the money in the correspondent account is traceable to the foreign deposit, and without having to be concerned with the application of the fungible property provisions of 18 U.S.C. § 984.

Section 981(k)(3) and (4) provide that for purposes of the application of the innocent owner defense in section 983(d), the "owner" of the funds is the person who deposited the funds into the foreign bank, not the foreign bank or intermediary institution that may have been involved in the transfer of the funds. As explained in the legislative history, "[u]nder this arrangement, if funds traceable to criminal activity are deposited into a foreign bank, the government may bring a forfeiture action against funds in that bank's correspondent account, and only the initial depositor, and not the intermediary bank, would have standing to contest it." *See* H.Rep. 107-250. The only exception to this rule applies when the government's theory of forfeiture is that the foreign bank was itself the wrongdoer (thus subjecting the money in its correspondent account to civil forfeiture), or when the foreign depositor had already withdrawn his money from the foreign bank before the money in the correspondent account was restrained, seized or arrested.

This provision will greatly facilitate the ability of federal prosecutors to forfeit funds that domestic criminals seek to insulate from forfeiture by depositing them in

foreign banks and then hiding behind the banks' innocent owner defenses, even though the funds are safely maintained in a correspondent account in the United States.

In another part of section 319, Congress has given law enforcement a potent new investigative tool by creating a mechanism for serving a subpoena for bank records on a foreign bank. New 31 U.S.C. § 5318(k)(3) provides that the Attorney General or the Secretary of the Treasury may serve "a summons or subpoena" on any foreign bank that has a correspondent account in the United States, and request records relating to that correspondent account or any "records maintained outside of the United States relating to the deposit of funds into the foreign bank." *See* H.Rep. 107-250 ("Under this provision, a foreign bank that maintains a correspondent account in the United States must have a representative in the United States who will accept service of a subpoena for any records of any transaction with the foreign bank that occurs overseas."). Thus, if the government wished to obtain records maintained by the foreign bank in its offices overseas, it would no longer be necessary to seek those records pursuant to a mutual legal assistance treaty or other procedure that is dependent upon the cooperation of a foreign government. Rather, the government could proceed by serving a summons or subpoena, issued by the Department of Justice or the Department of the Treasury, on the person the foreign bank is required to designate to "accept service of legal process" in the United States.

Section 5318(k)(3) provides a sanction for a foreign bank's failure to comply with the "summons or subpoena." Upon notification by either the Secretary of the Treasury or the Attorney General that a foreign bank has failed to comply with a summons or subpoena issued under the new statute, a U.S. bank that maintains a correspondent account for the foreign bank must close that account or face civil penalties of up to $10,000 per day "until the correspondent relationship is terminated."

Finally, section 319 gives the courts explicit authority to order the repatriation of assets in criminal cases. While numerous courts have directed criminal defendants to repatriate assets to the United States for the purpose of forfeiture as part of a pre-trial restraining order, this provision establishes clear statutory authority for that practice. Section 319 amends 21 U.S.C. § 853(e) to include a new paragraph explicitly authorizing a court to order a defendant to repatriate any property subject to forfeiture to the United States, and to deposit it with the Marshals Service, the Secretary of the Treasury, or in the registry of the court. Moreover, the same section amends the substitute asset provision in 21 U.S.C. § 853(p) to provide that in addition to ordering the forfeiture of substitute assets, the court may order a defendant who has placed his forfeitable property beyond the jurisdiction of the court to "return the property to the jurisdiction of the court so that the property may be seized and forfeited." Section 853(e)(4) also includes a provision giving the court the authority to sanction a defendant who fails to comply with a repatriation order by increasing his sentence under obstruction of justice provisions of the sentencing guidelines or by holding the defendant in contempt of court.

Section 320 Proceeds of Foreign Crimes

Under 18 U.S.C. § 981(a)(1)(C), as amended by CAFRA, any proceeds of any offense listed in the definition of "specified unlawful activity" are subject to civil forfeiture. Thus, Congress automatically created authority to forfeit the proceeds of the expanded list of foreign crimes merely by including them in section 1956(c)(7)(B). However, section 320 also amends 18 U.S.C. § 981(a)(1)(B) to authorize the forfeiture of both the proceeds of, *and any property used to facilitate,* any offense listed in section 1956(c)(7)(B), if the offense would be a felony if committed within the jurisdiction of the United States.

Section 322 Corporation Represented by a Fugitive

One of the key provisions in CAFRA was the reinstatement of the fugitive disentitlement doctrine. As codified at 28 U.S.C. § 2466, the doctrine provides that a person who is a fugitive in a criminal case cannot contest the forfeiture of his property in a related forfeiture case unless he surrenders to face the criminal charges. It has become apparent, however, that this provision contains a loophole: while the fugitive himself may not be able to file a claim, a corporation claiming to be the true owner of the property may do so, even if the corporation is owned by the fugitive, or the fugitive files the claim on the corporation's behalf. While the government could in some cases defeat this ploy by showing that the corporation was not the true owner of the property or that the corporation was the *alter ego* of the defendant, the loophole impaired the effective application of section 2466.

In section 322, Congress closed this gap by providing that the fugitive disentitlement doctrine applies to claims filed by corporations "if any majority shareholder, or individual filing the claim on behalf of the corporation" is otherwise disqualified from contesting the forfeiture by section 2466. As explained in the legislative history, "[t]he amendment clarifies that a natural person who is a fugitive may not circumvent this provision by filing, or having another person file, a claim on behalf of a corporation that the fugitive controls." H.Rep. 107-250.

Section 323 Enforcement of Foreign Judgments

CAFRA gave the federal courts authority to enforce foreign forfeiture judgments. Under 28 U.S.C. § 2467, a judgment of forfeiture of property located in the United States that is issued by a foreign court can be certified by the Attorney General and presented to a federal district court to be registered and enforced. This statute contained two major deficiencies: first, it provided no mechanism for preserving the property while the foreign forfeiture action was pending in the foreign court; and second, it applied only to a narrow range of foreign offenses such as drug trafficking and bank fraud.

Section 323 corrects both of these problems. First, it inserts new language in section 2467(d)(3) authorizing a district court to "preserve the availability of property subject to a foreign forfeiture or confiscation judgment" by issuing a civil forfeiture restraining order pursuant to 18 U.S.C. § 983(j). The order may be issued "at any time before or after" the government receives a final judgment of forfeiture from the foreign

court. The new statute provides that no person may contest the issuance of the restraining order "on any ground that is the subject of parallel litigation involving the same property that is pending in a foreign court." This provision avoids the "two bites at the apple" problem that often arises when the United States asks a foreign country to restrain property in that jurisdiction that is subject to forfeiture in a case pending in the United States. Almost invariably, the foreign court that restrains the property will allow potential claimants to object to the restraining order on grounds (such as an innocent owner defense) that could also be raised in the forfeiture proceeding underway in the U.S. This gives the foreign claimant the advantage of being able to attack the forfeiture twice on the same grounds: if he is unsuccessful in persuading the foreign court to vacate the restraining order, he may file a claim in the United States and assert the same defense all over again. (While the amendment to section 2467 can do nothing to prevent foreign courts from continuing to give their citizens two bites at the apple, the change to the federal statute will provide an example for other countries to follow in reforming their own laws.)

Second, to rectify the narrow application of section 2467, Congress amended section 2467(a)(2)(A) to provide that federal courts may enforce a foreign forfeiture order based on "any violation of foreign law that would constitute a violation of an offense for which property could be forfeited under Federal law if the offense were committed in the United States."

Section 371 Bulk Cash Smuggling Into or Out of the United States

In *United States v. Bajakajian*, 524 U.S. 321 (1998), the Supreme Court held that forfeiture of 100 percent of the unreported currency in a CMIR case would be "grossly disproportional to the gravity of the offense," unless the currency was involved in some other criminal activity. In so holding, the Court ruled that the unreported currency is not the *corpus delicti* of the crime. This contrasts, the Court said, with the various anti-smuggling statutes which authorize the forfeiture of 100 percent of the items concealed from the Customs Service or imported in violation of the Customs laws.

Section 371 makes currency smuggling a criminal offense, thus elevating the seriousness of smuggling currency into or out of the United States to the same level as the smuggling of firearms, jewels or counterfeit merchandise. As codified at 31 U.S.C. § 5332(a), the new statute makes it an offense for any person, with the intent to evade a currency reporting requirement under section 5316, to conceal more than $10,000 in currency in any fashion, and to transport, or attempt to transport, such currency into or out of the United States. Section 5332(b) provides for criminal forfeiture of the property involved in the offense, including a personal money judgment if the directly forfeitable property cannot be found and the defendant does not have sufficient substitute assets to satisfy the forfeiture judgment. Section 5332(c) authorizes civil forfeiture for the same offense.

In anticipation of legal attacks suggesting that the new statute is nothing more than a recodification of the existing penalties for violating the CMIR requirement, and

that forfeiture of 100 percent of the smuggled currency would still violate the Eighth Amendment, Congress made findings emphasizing the seriousness of currency smuggling and the importance of authorizing confiscation of the smuggled money. In particular, the "findings" state that the intentional transportation of currency into or out of the United States "in a manner designed to circumvent the mandatory reporting [requirements] is the equivalent of, and creates the same harm as, smuggling goods." Moreover, the findings state that "only the confiscation of smuggled bulk cash can effectively break the cycle of criminal activity of which the laundering of bulk cash is a critical part." The findings conclude that "in cases where the only criminal violation under current law is a reporting offense, the law does not adequately provide for the confiscation of smuggled currency." "In contrast," Congress found, "if the smuggling of bulk cash were itself an offense, the cash could be confiscated as the *corpus delicti* of the smuggling offense."

The House Report on this provision specifies that "[t]he civil forfeiture provision would apply to conduct occurring before the effective date of the act."

Section 372 Forfeiture in Currency Reporting Cases

Section 372 contains a seemingly minor amendment that strikes the references to 31 U.S.C. sections 5313, 5316 and 5324 from sections 981(a)(1)(A) and 982(a)(1), respectively, and places the authority to forfeit the property involved in those offenses in 31 U.S.C. § 5317(c). Sections 5313, 5316 and 5324 are the provisions requiring the filing of CTR and CMIR reports, and prohibiting the structuring of transactions to evade the reporting requirements.

Sections 981(a)(1)(A) and 982(a)(1) do not provide for the forfeiture of property involved in a conspiracy to commit any of the enumerated currency reporting offenses. Thus, under the prior law, the government could forfeit property involved in a structuring offense under 31 U.S.C. sections 5324(a)(3), but not property involved only in a conspiracy to commit that offense in violation of the general conspiracy statute, 18 U.S.C. section 371. In the revised version of section 5317(c), however, Congress has provided for the forfeiture of all property, real or personal, involved in a violation of sections 5313, 5316 or 5324, "or any conspiracy to commit such offense."

Section 373 Illegal Money Transmitting Businesses

When it was enacted in 1992, 18 U.S.C. § 1960 made it a federal offense to conduct a money transmitting business without a State license. While in the past this statute has been of limited use to federal law enforcement, section 373's amendments to section 1960 are likely to make the statute a much more effective tool against money laundering.

Under the prior law, the government had to prove that the defendant knew that his money transmitting business was "intentionally operated without an appropriate [State] money transmitting license" or that it did not comply with the registration requirements of 31 U.S.C. § 5330. Arguably, this required the government to prove that the defendant

knew of the State licensing requirements or federal registration requirements and knew that his business did not comply with them; it may also have required proof that the defendant knew that operating a business in such circumstances was illegal. Section 373 eliminated this ambiguity by clearly converting section 1960 into a "general intent" crime, making it illegal to conduct any unlicenced money transmitting business, "whether or not the defendant knew that the operation was required to be licensed" or that operation without a license was a criminal offense. Section 373 also makes it an offense for anyone to conduct a money transmitting business that fails to comply with the provisions of section 5330 (or the regulations that the Department of the Treasury is to promulgate within the next few months). *See* H.Rep. 107-250.

Most importantly, section 373 expands the scope of section 1960 to include any business, licensed or unlicenced, that involves the movement of funds that the defendant knows were derived from a criminal offense, or are intended to be used "to promote or support unlawful activity." Thus, under this new provision, a person operating a money transmitting business could be prosecuted for conducting transactions that the defendant knows involve drug proceeds, or that he knows involve funds that someone is planning to use to commit an unlawful act. Moreover, as explained in the House Report, "[i]t would not be necessary for the government to show that the business was a storefront or other formal business open to walk-in trade. To the contrary, it would be sufficient to show that the defendant offered his services as a money transmitter to another."

It is already an offense under sections 1956 and 1957, of course, for any person to conduct a financial transaction involving criminally derived property. But section 1957 has a $10,000 threshold requirement, and section 1956 requires proof of specific intent either to promote another offense or to conceal or disguise the criminal proceeds. New section 1960 contains neither of these requirements if the property is criminal proceeds, or alternatively, if there is proof that the purpose of the financial transaction was to commit another offense, it does not require proof that the transmitted funds were tainted by an prior misconduct. Thus, in cases where the defendant is a money transmitting business, section 1960 may prove more potent than either section 1956 or 1957 as a tool of the prosecution.

Finally, the changes to section 1960 include an amendment to 18 U.S.C. § 981(a)(1)(A) authorizing civil forfeiture of all property involved in the section 1960 violation.

Section 503 DNA Identification of Terrorists and Other Violent Offenders

Under prior law, the statutory provisions governing the collection of DNA samples from convicted federal offenders (42 U.S.C. § 14135a(d)) have been restrictive and, in particular, have not included persons convicted for the crimes that are most likely to be committed by terrorists. DNA samples could not be collected even from persons federally convicted of terrorist murders in many circumstances.

Section 503 addressed that deficiency, and generally strengthened the collection of DNA samples from federal offenders, by extending sample collection to all federal offenders convicted of the types of offenses that are likely to be committed by terrorists (as set forth in 18 U.S.C. § 2332b(g)(5)(B)) or any crime of violence (as defined in 18 U.S.C. §16).

Section 801 Terrorist Attacks and Other Acts of Violence Against Mass Transportation Systems

Section 801 created a new offense codified at 18 U.S.C. § 1993, prohibiting various violent offenses against mass transportation systems, vehicles, facilities, or passengers. The provision prohibits disabling or wrecking a mass transportation vehicle; placing a biological agent or destructive substance or device in a mass transportation vehicle with intent to endanger safety or with reckless disregard for human life; setting fire to or placing a biological agent or destructive substance or device in a mass transportation facility knowing or having reason to know that the activity is likely to disable or wreck a mass transportation vehicle; disabling mass transportation signaling systems; interfering with personnel with intent to endanger safety or with reckless disregard for human life; use of a dangerous weapon with intent to cause death or serious bodily injury to a person on the property of a mass transportation provider; conveying false information about any such offense; and attempt and conspiracy. The provision carries a maximum sentence of 20 years imprisonment, or life imprisonment if the crime results in death.

Section 802 Definition of Domestic Terrorism

Section 802 added to 18 U.S.C. § 2331 a new definition of "domestic terrorism," corresponding to the existing definition of "international terrorism." The term is defined to mean activities occurring primarily within the territorial jurisdiction of the United States involving acts dangerous to human life that are a violation of the criminal laws of the United States or any state and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnaping. The provision also makes a minor conforming change in the definition of "international terrorism."

The definition is used in other provisions of the Act, including the provision allowing nationwide service of search warrants in cases of international or domestic terrorism.

Section 803 Prohibition Against Harboring Terrorists

Section 803 created a new offense codified at 18 U.S.C. § 2339 that prohibits harboring or concealing persons who have committed or are about to commit a variety of terrorist offenses, including destruction of aircraft or aircraft facilities, use of nuclear materials or chemical or biological weapons, use of weapons of mass destruction, arson

or bombing of government property, destruction of energy facilities, sabotage of nuclear facilities, or aircraft piracy. The harboring offense of prior law prohibited only the harboring of spies (see 18 U.S.C. §792); there was no comparable terrorism provision, though the harboring of terrorists creates a risk to national security readily comparable to that posed by harboring spies.

Section 804 Jurisdiction Over Crimes Committed at U.S. Facilities Abroad

Section 804 explicitly extended the special maritime and territorial jurisdiction of the United States to U.S. diplomatic and consular premises and related private residences overseas for offenses committed by or against a U.S. national. When offenses are committed by or against a U.S. national abroad at such U.S. facilities, the country in which the offense occurs may have little interest in prosecuting the case. Unless the United States is able to prosecute such offenders, these crimes may go unpunished. Section 804 clarified inconsistent prior caselaw to establish that the United States may prosecute offenses committed in its missions abroad, by or against its nationals. The provision explicitly exempts offenses committed by members or employees of the U.S. armed forces and persons accompanying the armed forces, who are covered under a provision of existing law, 18 U.S.C. § 3261(a).

Section 805 Material Support for Terrorism

18 U.S.C. § 2339A prohibits providing material support or resources to terrorists. The prior definition of "material support or resources" was generally not broad enough to encompass expert advice and assistance – for example, advice provided by a civil engineer on destroying a building, or advice by a biochemist on making a biological agent more lethal. Section 805 amends 18 U.S.C.§ 2339A to include expert advice and assistance, making the offense applicable to experts who provide advice or assistance knowing or intending that it is to be used in preparing for or carrying out terrorism crimes. Section 805 also eliminates language in § 2339A restricting its application to material support provided within the United States, and adds to the list of underlying terrorism crimes for which provision of material support is barred. Other provisions in the section provide that material support offenses can be prosecuted in any district in which the underlying offense was committed, and make it clear that prohibited material support includes all types of monetary instruments.

Section 806 Assets of Terrorist Organizations

Prior law did not specifically provide authority for the confiscation of terrorist assets. Instead, forfeiture was authorized only in narrow circumstances for the proceeds of murder, arson, and some terrorism offenses, or for laundering the proceeds of such offenses. However, most terrorism offenses do not yield "proceeds," and available forfeiture laws required detailed tracing that is quite difficult for accounts coming through the banks of countries used by many terrorists.

Section 806 increases the government's ability to strike at terrorist organizations' economic base by permitting the forfeiture of their property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense. This is similar in concept to the forfeiture now available under RICO. In parity with the drug forfeiture laws, the section also authorizes the forfeiture of property used or intended to be used to facilitate a terrorist act, regardless of its source.

Section 806 amends 18 U.S.C. § 981(a)(1) to include a new subparagraph (G) which makes the following property subject to civil forfeiture:

> "(G) All assets, foreign or domestic--
>
> > "(i) of any individual, entity or organization engaged in planning or perpetrating any act of domestic terrorism or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;
> >
> > "(ii) acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic terrorism or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property; or
> >
> > "(iii) derived from, involved in, or used or intended to be used to commit any act of domestic terrorism or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property.".

Prosecutors are encouraged to check with AFMLS before commencing any civil forfeiture action based on section 981(a)(1)(G) so that we may coordinate application of the new law.

Section 807 Technical Clarification Relating to Provision of Material Support to Terrorism

The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX of Public Law 106-387, creates exceptions in the nation's Trade Sanctions Programs for food and agricultural products. Section 807 makes clear that the Trade Sanctions Reform and Export Enhancement Act of 2000 does not limit 18 U.S.C. §§ 2339A or 2339B. In other words, the exceptions to trade sanctions for these items does not prevent criminal liability for the provision of these items to support terrorist activity or to foreign terrorist organizations as described in 2339A and 2339B. This is not a change from existing law, but rather serves to foreclose any possible misunderstanding or argument that the Act in some manner trumps or limits the prohibition on providing material support or resources to terrorism.

Section 808 Definition of Federal Crime of Terrorism

Section 808 added several offenses, including a number of aircraft violence crimes and certain computer crimes, to the list of predicate offenses in the definition of "Federal crime of terrorism" that appears in 18 U.S.C. § 2332b(g)(5). That term is defined as any of a comprehensive list of offenses likely to be committed by terrorists

(set forth in § 2332b(g)(5)(B)) if calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct. The list of predicate crimes in § 2332b(g)(5)(B) is used elsewhere in the Act to define the scope of other provisions, including a longer statute of limitations (section 809), lengthened periods of supervised release (section 812), and additional crimes that are now RICO predicates (section 813).

Because of Congressional concerns about overbreadth, this section removes some crimes from prior § 2332b(g)(5)(B) (primarily offenses involving assault and less grave property crimes). To fully preserve the Attorney General's primary investigatory authority over these offenses, section 808 includes a conforming amendment to § 2332b(f) which explicitly adds these offenses to that provision.

Section 809 No Statute of Limitations for Certain Terrorism Offenses

Most non-capital federal offenses are subject to a five-year statute of limitations; under prior law, many terrorism offenses were subject to an eight-year statute of limitations under 18 U.S.C. § 3286. Section 809 expands the list of offenses subject to the eight-year limitation period to include all offenses listed in § 2332b(g)(5)(B), unless otherwise subject to a longer limitation period. In addition, section 809 provides that any offense listed in § 2332b(g)(5)(B) may be prosecuted without limitation of time if the offense resulted in, or created a foreseeable risk of, death or serious bodily injury to a person other than the defendant. This will make it possible to prosecute the perpetrators of such terrorist acts whenever they are identified and apprehended.

The section expressly provides that it is applicable to offenses committed before the date of enactment of the statute, as well as those committed thereafter. This retroactivity provision ensures that the section's limitation period reforms will apply, for example, to the prosecution of crimes committed in connection with the September 11, 2001 terrorist attacks. The constitutionality of such retroactive applications of changes in statutes of limitations is well settled. *See, e.g.*, *United States v. Grimes*, 142 F.3d 1342, 1350-51 (11th Cir. 1998); *People v. Frazer*, 982 P.2d 180 (Cal. 1999).

Section 810 Alternative Maximum Penalties for Terrorism Offenses

Section 810 amended existing statutes prescribing punishment levels for crimes likely to be committed by terrorists that previously were subject to inadequate maximum penalties. This section provides for enhanced maximum penalties for arson offenses under 18 U.S.C. § 81, destruction of an energy facility under § 1366, material support to terrorists under § 2339A, material support to designated foreign terrorist organizations under § 2339B, destruction of national-defense materials under § 2155(a), sabotage of nuclear facilities or fuel under 42 U.S.C. § 2284, carrying weapons aboard aircraft with reckless disregard for human life under 49 U.S.C. § 46505(c), and damaging or destroying an interstate gas or hazardous liquid pipeline facility under 49 U.S.C. § 60123(b).

Section 811 Penalties for Terrorist Conspiracies

While many terrorism offenses contain specific provisions punishing conspiracies with the same maximum penalties as substantive offenses, under prior law, some did not. If no specific conspiracy provisions existed, the alternative was proceeding under the general conspiracy provision (18 U.S.C. § 371), which carries a maximum penalty of five years even if the object of the conspiracy is a serious crime carrying a far higher maximum penalty. Section 811 amended several criminal statutes to provide adequate conspiracy penalties by authorizing maximum penalties equal to the completed offense. Section 811 created enhanced conspiracy penalties for arson under 18 U.S.C. § 81, killings in federal facilities under § 930(c), injuring or destroying communications lines or systems under § 1362, injuring or destroying buildings or property within the special maritime and territorial jurisdiction of the United States under § 1363, wrecking trains under § 1992, material support to terrorists under § 2339A, torture under § 2340A, sabotage of nuclear facilities or fuel under 42 U.S.C. § 2284, interference with flight crew members and attendants under 49 U.S.C. § 46504, carrying weapons aboard aircraft under 49 U.S.C. § 46505, and damaging or destroying an interstate gas or hazardous liquid pipeline facility under 49 U.S.C. § 60123(b).

Section 812 Post-Release Supervision of Terrorists

Prior federal law (18 U.S.C. § 3583(b)) generally capped the maximum period of post-imprisonment supervision for released felons at 3 or 5 years. Thus, for a released but unreformed terrorist, there was no means of tracking the person or imposing conditions to prevent renewed involvement in terrorist activities beyond a period of a few years. The drug laws (21 U.S.C. § 841) mandate longer supervision periods for persons convicted of certain drug trafficking crimes, and specify no upper limit on the duration of supervision, but there was nothing comparable for terrorism offenses.

Section 812 added a new subsection to 18 U.S.C. § 3583 to authorize longer supervision periods, including potentially lifetime supervision, for persons convicted of certain terrorism crimes. This permits appropriate tracking and oversight following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments. The covered class of crimes is the crimes listed in 18 U.S.C. § 2332b(g)(5)(B), where the commission of the offense resulted in, or created a foreseeable risk of, death or serious injury to another person.

Section 813 Inclusion of Acts of Terrorism as Racketeering Activity

Under prior law, the list of predicate federal offenses for RICO, appearing in 18 U.S.C. § 1961(1), did not include the offenses which are most likely to be committed by terrorists. Section 813 added the crimes listed in § 2332b(g)(5)(B) to the list of RICO predicates, which will make it possible to use RICO more readily in the prosecution of terrorist organizations.

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.

A. **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).

A. **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).

A. **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.

A. **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.

A. **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).

A. **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.

Section 817 Expansion of the Biological Weapons Statute

Section 817 expanded the coverage of existing restrictions on the possession and use of biological agents and toxins. Prior law prohibited the possession, development, acquisition, etc., of biological agents or toxins "for use as a weapon." 18 U.S.C. § 175. Section 817 amended the definition of "for use as a weapon" to include all situations in which it can be proven that the defendant had any purpose other than a prophylactic, protective, bona fide research, or other peaceful purpose. This enhances the government's ability to prosecute suspected terrorists in possession of biological agents or toxins, and conforms the scope of the criminal offense in 18 U.S.C. § 175 more closely to the related forfeiture provision in 18 U.S.C. § 176.

Moreover, the section added a subsection to 18 U.S.C. § 175 which defines an additional offense of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose. Finally, this section also enacts a new statute, 18 U.S.C. § 175b, which generally makes it an offense for certain restricted persons (including felons, persons indicted for felonies, fugitives, drug users, illegal aliens, mentally impaired persons, aliens from certain terrorist states, and persons dishonorably discharged from the U.S. armed services) to possess a biological agent or toxin listed as a "select agent" by the Secretary of Health and Human Services.

Section 1004 Venue in Money Laundering Cases

In *United States v. Cabrales*, 524 U.S. 1 (1998), the Supreme Court held that a money laundering prosecution may be brought in any district where the financial or monetary transaction takes place, but not in the district where the specified unlawful activity took place, if the financial or monetary transaction occurred wholly in another district. The court suggested, however, that the situation might be different if the defendant had transported the funds from the district where the underlying crime occurred to the district where the financial or monetary transaction was conducted. In that case, the court said, the money laundering offense might be considered a continuing offense. Several courts of appeals have ruled that venue is appropriate in the district where the specified unlawful activity occurred in that situation. *See United States v. Angotti*, 105 F.3d 539 (9th Cir. 1997); *United States v. Abuhouran*, 1996 WL 451368 (E.D. Pa. 1996); *United States v. Beddow*, 957 F.2d 1330 (6th Cir. 1992).

Section 1004 codifies the suggestion made in *Cabrales*, making it clear that a substantive money laundering prosecution may be brought in the district where the underlying specified unlawful activity took place if the defendant participated in the movement of the criminal proceeds from that district to the district where the financial or monetary transaction occurred. It also makes clear that the transfer of funds from one district to another, such as a wire transfer of drug proceeds is a single, continuing offense, so that any defendant who conducts any part of the transfer can be prosecuted in any district in which any part of the transfer takes place. This addresses an interpretation of the current statute in *United States v. Stewart*, 256 F.3d 231 (4th Cir. 2001), which held that a defendant who received drug proceeds that were transferred by wire from Virginia to California could be prosecuted only in California, because the wire transfer comprised

two separate transactions: a deposit in Virginia and a withdrawal in California. Under the amendment, the defendant in that case could be prosecuted in either Virginia or California because the wire transfer would constitute a single, continuing offense in which the defendant had participated.

Finally, the amendment codifies the present rule that venue for attempts and conspiracies is not limited to the district where the completed offense would have occurred, but will lie in any district where an overt act was committed.

Section 1006 Inadmissibility of Aliens Engaged in Money Laundering

Section 1006 provides for inadmissibility of any individual whom a consular officer has reason to believe has or is engaged in certain money laundering offenses, or any criminal activity in a foreign country that would constitute such an offense if committed in the United States, regardless of whether a judgment of conviction has been entered or avoided due to flight, corruption, etc. This section treats money launderers under the same standard applicable to drug traffickers and will make our ability to exclude aliens involved in such activities less dependent upon our ability to draw inferences about a person's intent to do something illicit in the United States. Money laundering offenses are, in general, related to underlying crimes involving moral turpitude that are already grounds for exclusion under the Immigration and Nationality Act.

Section 1011 Crimes Against Charitable Americans

Section 1011, entitled the "Crimes Against Charitable Americans Act of 2001" responds to fraudulent charity scams that arose in the wake of the September 11 terrorist attack. Section 1011 has three principal provisions. First, it amends the Telemarketing and Consumer Fraud and Abuse Protection Act (15 U.S.C. § 6101 et seq.) by adding three new substantive provisions that expand the authority of the Federal Trade Commission (FTC) over telemarketing fraud and abuse. Second, it amends 18 U.S.C. § 917, which prohibits falsely impersonating a member or agent of the American National Red Cross for the purpose of soliciting, collecting, or receiving money or material. It increases the maximum term of imprisonment from one to five years, making section 917 a felony (and thereby increasing the maximum fine to $250,000).

Third, section 1011 amends the definition of "telemarketing" in the Senior Citizens Against Marketing Scams Act of 1994, 18 U.S.C. § 2325, to include a plan, program, promotion, or campaign that is conducted to induce a charitable contribution, donation, or gift of money or any other thing of value, by use of interstate telephone calls. *See* 18 U.S.C. § 2325(1). This makes clear that participants in a scheme that fraudulently solicits charitable contributions or donations, even if they do not require the prospective victim to purchase other goods or services, may be subject to enhanced penalties for telemarketing fraud under 18 U.S.C. § 2326 and mandatory restitution under 18 U.S.C. § 2327.