International Penal Law Association
Report on Information Society, Section 4
United States Report
January 8, 2013*

Bruce ZAGARIS*

I. JURISDICTIONAL ISSUES

A. The Manner in Which the U.S. Locates the Place of the Commission of a Crime in Cyberspace[1]

For the U.S. to assert jurisdiction over the commission of a crime in cyberspace, the manner in which the U.S. locates the place of the commission of the crime is not essential. As discussed below, the U.S. has and uses several theories of extraterritorial jurisdiction that enable it to criminalize the commission of crime in cyberspace.

B. U.S. Law Does Not Require the Location of the Place Where Information and Evidence Are Held

Unless evidence exists of a contrary intent, U.S. laws are presumed not to have extraterritorial application. *See United States v. Cotton*, 471 F.2d 744, 750 (9th Cir. 1973). The prosecution can overcome the presumption against extraterritoriality by showing "clear evidence of congressional intent to apply a statute beyond our borders." *United States v. Gatlin*, 216 F.3d 207, 211 (2d Cir. 2000) (internal quotations omitted).

Congress has the authority to enforce its laws beyond the territorial boundaries of the United States. When a defendant challenges whether Congress has in fact exercised that authority in a specific case, a court must apply statutory construction rules to ascertain the intent of Congress. *Equal Employment Opportunity Comm. v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991).

In 2001, in enacting the USA PATRIOT Act, Congress revised 18 U.S.C. §§ 1029 and 1030 to provide explicitly for extraterritorial jurisdiction in certain cases, including cybercrime. The USA PATRIOT Act added the following language to Sec. 1029:

> (h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—
>
> (1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and
>
> (2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom 18 U.S.C. § 1029(h).

Congress also amended Section 1030(e)(2)(B) to expressly include a computer that "is used in interstate or foreign commerce, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). Even before the 2001 amendment, at least one court held that the plain language of 18 U.S.C. § 1030 was a clear expression of congressional intent to apply that section extraterritorially. *See United States v. Ivanov*, 175 F.Supp. 2d 367, 374-75 (D. Conn. 2001).

Extraterritorial jurisdiction can exist not only based on express Congressional intent, but also based on intended and actual detrimental effects within the United States. "The intent to cause effects within the United States…makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope." *United States v. Muench*, 694 F.2d 28,

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Partner. Berliner, Corcoran, & Rowe LLP. 1101 17th St. NW. Washington D.C. 20036. (202)293-2371 (phone). (202)293-9035 (fax). bzagaris@bcr-dc.com

[1] The discussion in this section relies closely on Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, PROSECUTING COMPUTER CRIMES MANUAL, especially 113-15 (accessed last Jan. 3, 2012) http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

33 (2d Cir. 1982). "It has long been a commonplace of criminal liability that a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit." *United States v. Steinberg*, 62 F.2d 77, 78 (2d Cir. 1932).

Other sources of extraterritorial jurisdiction may include 18 U.S.C. § 7, which defines the special maritime and territorial jurisdiction of the United States, and 18 U.S.C. §§ 3261-3267, which govern criminal offenses committed outside of the United States members of the military and persons employed by or accompanying them.

C. Cyber Crime Does Not Need a Determination of the Locus Delicti in the U.S. Criminal Justice System

Several statutes give jurisdiction to U.S. prosecutors over certain acts of cyber crime without a determination of the *locus delicti*. However, some statutes require showing that the computers involved must have been used in or affect interstate or foreign commerce and computers used by the federal government and financial institutions. Some statutory provisions of the Computer Fraud and Abuse Act (CFAA), enacted by Congress in 1986, criminalizes accessing and other acts concerning a "protected computer", a statutory term of art in 18 U.S.C. § 1030(e)(2). Essentially, "protected computer" covers computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions.

Regardless of where the act is committed, a defendant commits a crime by improperly accessing or obtaining information from trespassing, etc. a "protected computer", that is, computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions.

Several courts have held that using the Internet from a computer is sufficient to meet the element that a computer "is used in or affecting interstate or foreign commerce or communication." *See, e.g., United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("[T]he latter two elements of the section 1030(a)(2)(C) crime [obtaining information from a protected computer] will always be met when an individual using a computer contacts or communicates with an Internet website."). *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) ("No additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated.") (internal citations omitted); *Paradigm Alliance, Inc. v. Celeritas Technologies, LLC*, 248 F.R.D. 598, 602 (D. Kan. 208) ("As a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement.")

In terms of the jurisdictional rules applicable to cyber crime, those involving obtaining national security information and trespassing in a government computer, both part of the CFAA, seem based on the protective principle.

For many of the CFAA provisions, the basis for legislative jurisdiction is both the national principle (e.g., that the perpetrator is a U.S. national or resident), the protective principle, insofar as national security or government computers are involved, and territorial principle, insofar as the perpetrator's act has an effect on the U.S. or has been committed in the U.S.

D. U.S. Case Law Provides Rules on the Prevention or Settlement of Conflicts of Jurisdiction

When U.S. jurisdiction may conflict with the jurisdiction of another country, even if one of the bases for jurisdiction is present, both U.S. and international law preclude a state from applying its law to conduct linked to another state or states when such exercise is unreasonable. The determination of whether the exercise of jurisdiction is unreasonable is evaluated in light of a number of relevant factors, including:

1. the extent to which the activity (a) occurs within the regulating state, or (b) has a substantial, direct, and foreseeable effect upon or in the regulating state;
2. the links, such as nationality, residence, or economic activity, between the regulating state and the personal principally responsible for the activity to be regulated, or between that state and those whom the law or regulation is intended to protect;
3. the character of the activity to be regulated, the significance of regulation to the regulating state, the extent to which other states regulate such activities, and the extent to which the goals of such regulations are generally accepted;
4. the existence of justified expectations that might be protected or hurt by the regulation in question;
5. the significance of regulation to the international political, legal, or economic system;
6. the extent to which another state may have an interest in regulating the activity; and
7. the potential of conflict with regulation by other states.

Under established U.S. law and an emerging principle of international law, exercising jurisdiction on one of the bases normally permitted is still unlawful if it is unreasonable. A wide international consensus exists that the links of territoriality or nationality are necessary, but that not in all cases sufficient, conditions for the exercise of jurisdiction. As a general proposition legislatures and administrative agencies in the U.S. and abroad have not exercised jurisdiction where it would be unreasonable to do so. Courts

have usually interpreted general language in a statute as not intended to exercise or authorize the exercise of jurisdiction in circumstances where application of the statute would be unreasonable. How do these factors apply to hypothetical 2 above?
According to the Restatement, when regulatory statutes that may result in both civil and criminal liability – such as U.S. antitrust or securities laws – apply, the presence of substantial foreign elements will ordinarily weigh against applying criminal law. In such cases, legislative intent to subject conduct outside the state's territory to its criminal law should be found only on the basis of express statement or clear implication.
A U.S. statute should be construed to apply to a person or activity only if not unreasonable, and to the extent consistent with the extraterritorial jurisdiction principles mentioned above, unless such construction is impossible. Similarly, if one construction of a U.S. statute would conflict with the law of another state that has a clearly greater interest, or would subject a person to conflicting commitments, while another construction would avoid such a conflict, the latter is preferable. This rule applies to courts and to executive branch officials and regulatory bodies interpreting authority conferred to them by legislation. In addition, the President may rely on this rule while considering a bill submitted for his approval. If construction of a statute that fulfills the intent of Congress within the limits of international law is not possible, the statute is nevertheless valid, but its application may cause the U.S. to conflict with its international legal responsibilities.
The application of the principle of reasonableness to the exercise of criminal jurisdiction with respect to acts committed in another state can be viewed as especially intrusive. For example, the House of Lords reacted angrily to U.S. involvement in Westinghouse Corporation efforts to take the testimony of British witnesses, in an alleged conspiracy to fix the price of uranium. U.S. enforcement agencies generally try to exercise restraint in applying criminal jurisdiction over activity with substantial foreign elements unless they have strong justification. Examples of U.S. exercise of criminal jurisdiction include, under the special "protective principle," efforts to punish immigration fraud and currency counterfeiting.

E. U.S. Cyber Crime Laws Do Not Apply Under the Universal Principle of Jurisdiction

Cyber crime laws in the United States require jurisdictional principle other than just universal jurisdiction. In other words, the U.S. criminal justice system does apply to cyber crime universally. The principle of universal jurisdiction enables a state to exercise jurisdiction to prescribe for a class of offenses known as *delicta juris gentium* or certain crimes under international law. These acts constitute crimes under international law that the community of nations recognizes as warranting universal concern. Such crimes by their very nature threaten to undermine the foundations of the enlightened international community. The U.S. does not apply cyber crimes under the universal principle because it does not believe that such crimes as *per se delicta juris gentium*. If cyber crime was to be applied on a universal basis, it should do so on the basis of a treaty.

II. SUBSTANTIVE CRIMINAL LAW AND SANCTIONS

A. U.S. Cyber Crime Offenses with a Transnational Dimension and Whose Definitions Contain Jurisdictional Elements

Insofar as the definition of "protected computer" in CFAA, 18 U.S.C. § 1030(e)(2) covers computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions, these cyber crime offenses have a transnational dimension.
Insofar as the CFAA and the USA PATRIOT Act provisions mentioned above require acts "within the jurisdiction of the United States", computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions, they contain jurisdictional elements.
18 U.S.C. § 1030(b) provides that attempts to commit the crimes covered in section 1030 are also criminal acts. In 2008, the Identity Theft Enforcement and Restitution Act amended Section 1030(b) to create a new conspiracy offense. Insofar as the substantive crimes in Section 1030 require showing, e.g., that a protected computer "is used in or affecting interstate or foreign commerce or communication," the prosecution would need to show whose jurisdiction elements in order to achieve a conviction.

B. The U.S. Government Believes It Can Regulate Cyber Crime on Its Own

The United States legislative and executive branches do believe they can regulate cyber crimes on their own, since, as mentioned above for many of the cyber crimes, such as the CFAA provisions, the basis for legislative jurisdiction is both the national principle (e.g., that the perpetrator is a U.S. national or resident); the protective principle, insofar as national security or government computers are involved; and the territorial principle, insofar as the perpetrator's act has an effect on the U.S. or has been committed in the U.S. Subjective territoriality requires an element of the case to occur within the asserting state. Objective

territoriality exists when the effect or result of the criminal conduct impacts on the asserting state, but the other elements of the offense occur wholly beyond the territorial boundaries.[2]

Traditionally, the United States has at least theoretically denied the ability of a state to assert criminal jurisdiction outside of its territory against a non-national. However, it believes that in certain circumstances a crime may be committed within the territory of a state and hence be justifiable by its criminal courts, even though the actor is physically outside the territory. Moreover, the U.S. asserts jurisdiction when an act is committed physically outside its territory but injures, harms or affects its citizens or interests located within its territory. In such cases the basis for jurisdiction is often referred to as "objective territorial jurisdiction," mentioned above – also called the effects doctrine.[3]

In recent years the U.S. government and U.S. courts have tended to expand jurisdiction over extraterritorial crime in a way that is inconsistent with fundamental principles of international law. Some U.S. court decisions have broadened the objective and subjective territoriality theories beyond any actual effect upon or connection with U.S. territory. For instance, the territorial theory has been applied to thwart extraterritorial narcotics or other conspiracies, as mentioned above, even when no overt act, element, or any effect has occurred there.[4] According to Professor Blakesley, the courts have not distinguished between the protective and objective territoriality principles. The cases and the Restatement (Third)[5] expand the objective territorial principle, providing in section 402(1)(c) that jurisdiction over an extraterritorial crime will be obtained when the crime "has or is intended to have substantial effect within [U.S] territory."[6]

C. The U.S. Government Increasingly Asserts Jurisdiction over Conspiracies and All Forms of Participation of Cyber Crimes

According to Professor Blakesley, the application of objective territoriality in this manner is incorrect. In some cases other theories would have been appropriate. Jurisdiction over thwarted extraterritorial conspiracies is proper, but not on the basis of objective territoriality or subjective territoriality unless the co-conspirators worked in the U.S. or the goods involved entered the U.S.

Professor Blakesley points out that this trend in U.S. courts began with the Supreme Court's incorrect statement, in *Ford v. U.S.*, 273 U.S. 593 (1927), that objective territoriality applied to circumstances in which no territorial effects had occurred. In making this statement, the court misused objective territoriality in circumstances where subjective territoriality would have applied. The British subjects that were convicted of conspiracy to violate U.S. liquor laws were onboard a British vessel on the high seas. The conspiracy itself had its situs within U.S. territory. Conspirators were within and outside of U.S. borders and four overt acts occurred in the U.S.[7]

By definition, a fully thwarted extraterritorial conspiracy has no effect within the territory; rather, it is an inchoate offense and has no effect until the substantive offense to which the parties were conspiring is accomplished. The goal of criminalizing conspiracy is to prevent the effects from occurring by attaching a sanction to undesirable collaboration early in its development. While conspiracy laws attempt to prevent potential effects, the objective territorial theory is not the correct mechanism for this purpose. It strains credulity and the objective territoriality theory to say that the harm has impacted on the intended state the moment the agreement is made outside the territory. In spite of this, U.S. courts have subsequently used the erroneous *Ford* dicta and its confused analysis as authority for the proposition that objective territorial jurisdiction applies to extraterritorial conspiracies in which no element nor any harmful effects have been caused.[8]

Many difficult territorial cases involve intended but unrealized effect. When the intent to commit a proscribed act – for example, securities fraud or export control violations – is clear and shown by some activity, and the effect to be produced by the activity is substantial and foreseeable, the fact that a plan or conspiracy was stopped does not deprive the target state of jurisdiction to make its law applicable.[9] The territorial theories are not sufficient for jurisdiction over wholly extraterritorial offenses such as

---

[2] Blakesley, *Extraterritorial Jurisdiction*, INTERNATIONAL CRIMINAL LAW: PROCEDURAL AND ENFORCEMENT MECHANISMS (M. Cherif Bassiouni, ed.) 33, 47 (2d. 1999).
[3] RESTATEMENT (3RD), § 402, Comment (d).
[4] *See, e.g.*, Blakesley, *Extraterritorial Jurisdiction, supra*, at 82, fn. 263 and cases cited therein.
[5] RESTATEMENT (3RD), §§ 402(1)(c), 403.
[6] Blakesley, *Extraterritorial Jurisdiction*, *id.*, citing RESTATEMENT (3RD), §§ 402(1)(c), 403. Reporter's 8, following § 403, incorrectly relies on some of the cases discussed therein, e.g., those on the territoriality theories, to promote the notion that objective territorial jurisdiction obtains when there exists simply an intent to have an impact on U.S. territory.
[7] *Ford v. United States*, 273 U.S. 593, 630 (1927).
[8] Blakesley, *Extraterritorial Jurisdiction*, *supra*, at 83-84.
[9] *See* RESTATEMENT (3RD), § 402, Comment d.

narcotics trafficking or money laundering. When the offense occurs totally abroad and no effect actually occurs within the territory, territoriality cannot apply.[10] European jurisprudence does not provide jurisdiction over thwarted extraterritorial attempts or conspiracy.[11]

The United States Code does provide for criminal responsibility for international corporations and providers, insofar as they commit a crime against protected computers or violate U.S. cyber crimes.

The protective principle gives a state the right to exert jurisdiction over a certain class of limited offenses which are committed outside its territory by non-nationals. This claim can be invoked to assert jurisdiction when the offenses are directed against the security of the state or against important state interests or functions.[12]

Representative offenses include: espionage, counterfeiting of the state's seal or currency, the falsification of official documents, perjury before consular officials and conspiracies to violate immigration and customs law. Although the U.S. does not often invoke the protective principle, it has been used to establish jurisdiction over non-nationals who make false statements on visa applications at U.S. consulates.[13] Some U.S. courts have asserted the protective principle with the objective territoriality principle simultaneously to support criminal jurisdiction.[14]

D. Criminal Responsibility for International Corporations/Providers

The protective principle also applies to crimes against U.S. national security, such as crimes against computers belonging to U.S. agencies.

III. COOPERATION IN CRIMINAL MATTERS

A. The Extent to which the Specificities of Information Technology May Change the Nature of Mutual Assistance

Insofar as the U.S. is the requested state, the specificities of information technology may impose limitations on the ability of the U.S. to obtain evidence. For instance, as discussed below, constitutional and legal limits may limit the use of Pen/Trap devices or the interception of wireless communications.

The United States, like other countries, takes the position that it can use its own legal mechanisms to request data from any cloud server, located anywhere around the world, so long as the cloud service provider is subject to US jurisdiction — that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.[15]

B. Interception of (Wireless) Telecommunications

The U.S. does provide for the interception of communications. Real-time electronic surveillance in federal criminal investigations is controlled primarily by two statutes. The first is the Federal Wiretap Act, 18 U.S.C. §§ 2510-2522, which was passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereafter referred to as "Title III"). The second statute is the Pen Registers and Trap and Trace Devices chapter of Title 18 ("the Pen/Trap statute"), 18 U.S.C. §§ 3121-3127, which was enacted as part of the Electronic Communications Privacy Act of 1986. A person who fails to comply with these statutes may be civilly and criminally liable. In the case of Title III, the court may suppress the evidence obtained in violation of the statutes.

C. Content vs. Addressing Information

In general, the Pen/Trap statute regulates the collection of addressing and other non-content information for wire and electronic communications. Title III regulates the collection of actual content of wire and electronic communications.

---

[10] *See* Blakesley, *Extraterritorial Jurisdiction*, INTERNATIONAL CRIMINAL LAW: PROCEDURAL AND ENFORCEMENT MECHANISM, at 53.

[11] *Id. C.f., Liangsiriprasert v. United States Government*, [1990] All E.R. 866 (English court based jurisdiction on a conspiracy entered into abroad with no overt act in the U.K.).

[12] RESTATEMENT (3RD), § 402(3) and § 402(3), Comment (f); *Harvard Research in International Law, the Draft Convention With Respect to Crime*, arts. 7, 8, 29 AM. J. INT'L L. 435 (Supp. 1935); M. WHITEMAN, *supra*, at 95-100.

[13] 18 U.S.C. § 1546. *See, e.g., United States v. Pizzarusso*, 388 F.2d 8 (2d Cir. 1968), *cert. denied*, 392 U.S. 936 (1968); *United States v. Rodriguez*, 182 F. Supp. 479 (S.D. Cal. 1960); *United States v. Archer*, 51 F. Supp. 708 (C.D. Cal. 1943).

[14] *See, e.g., Rocha v. United States*, 288 F.2d 545 (9th Cir. 1961), *cert. denied*, 366 U.S. 948 (1961). *See also* Blakesley, *supra*, at 3.

[15] Council of Europe, *Transborder access and jurisdiction: What are the options?*
Report of the Transborder Group, Cybercrime Convention Committee (T-CY), Ad-hoc sub-group on jurisdiction and transborder access to data, Adopted by the T-CY on 6 December 2012, at 48. http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf.

Title III and the Pen/Trap statute govern access to different types of information. Title III allows the government to obtain the contents of wire and electronic communications in transmission. In contrast, the Pen/Trap statute concerns the real-time collection of addressing and other non-content information concerning those communications.[16]

The difference between addressing information and content is clear for telephone calls. The addressing information is the phone numbers of the originating and receiving telephones, while the content of the communications is the actual conversation between the parties to the call.

The distinction between addressing information and content also applies to Internet communications. When computers on the Internet communicate with each other, they classify messages into discrete chunks known as packets and then send each packet to its intended destination. Every packet has addressing information in the header of the packet (much like the "to" and "from" addresses on an envelope), followed by the payload of the packet, which has the contents (much like a letter inside an envelope).

The Pen/Trap statute allows law enforcement to obtain the addressing information of Internet communications much as it would the addressing information for traditional phone calls. However, collecting the entire packet ordinarily implicates Title III. The primary difference between an Internet Pen/Trap device and an Internet Title III intercept device is that the former is designed to capture and retain only addressing information, while the latter is designed to capture and retain the entire packet.

The same distinction applies to Internet email. Every Internet email message has a set of headers that contain addressing and routing information that the mail program generates, followed by the actual contents of the message of the sender. The addressing and routing information includes the email address of the sender and recipient, as well as information about when and where the message was sent on its way (roughly analogous to the postmark on a letter).[17] The Pen/Trap statute allows law enforcement to obtain the header information of Internet emails (except for the subject line, which can contain content) using a court order, just like it allows law enforcement to obtain addressing information for phone calls and individual Internet packets using court order. Conversely, the interception of email contents, including the subject line, requires compliance with the strict requirements of Title III.

D. The Pen-Trap Statute, 18 U.S.C. §§ 3121-3127

The Pen/Trap statute allows a government attorney to apply to a court for an order authorizing the installation of a pen register and/or trap and trace device, if "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 2122(b)(2). A pen register records outgoing addressing information (such as a number dialed from a monitored telephone), and a trap and trace device records addressing information (such as caller ID information). The Pen/Trap statute applies to a wide range of communication technologies, including computer network communications.[18]

1. Definition of Pen Register and Trap and Trace Device

The Pen/Trap statute defines pen register and trap and trace devices broadly. A "pen register" is:

A device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided; however, that such information shall not include the contents of any communication…[19]

The definition of pen register further excludes devices or processes used for billing or cost accounting. See 18 U.S.C. § 3127(3).

The breadth of these definitions arises from the scope of their components. First, "an instrument or facility from which a wire or electronic communication is transmitted" encompasses a wide variety of communications technologies, including a non-mobile telephone, a cellular telephone, an Internet user account, an email account, or an IP address. Second, the definitions'; inclusion of all "dialing, routing, addressing, [and/or] signaling information" encompasses almost all non-content information in a communication. Third, since the definitions of a pen register and a trap and trace device include both a "device" and a "process," the statute covers software as well as physical devices.

[16] *See* 18 U.S.C. § 2511(2)(h)(i) (stating that it is not a violation of title III to use a pen register of trap and trace device); *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 453-54 (D.C. Cir. 2000) (contrasting pen registers and title III intercept devices); *Brown v. Waddell*, 50 F.3d 285, 289-94 (4th Cir. 1995).

[17] *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (email to/from addresses and IP addresses constitute addressing information).

[18] *See in re Application of United States*, 416 F. Supp. 2d 13, 15 (D.D.C. 2006).

[19] 18 U.S.C. § 2127(3).

2. Pen/Trap Orders: Application, Issuance, Service, and Reporting

In order to obtain a pen/trap order, applicants must identify themselves, identify the law enforcement agency conducting the investigation, and then certify their belief that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency. See 18 U.S.C. § 3122(b)(1)-(2). The issuing court must have jurisdiction over the offense being investigated. See 18 U.S.C. § 3122(a); 18 U.S.C. § 3127(2)(1). If the application has these elements, the statute requires the court to authorize the installation and use of pen/trap device anywhere in the U.S. See 18 U.S.C. § 3123(a)(1). The court will not conduct an "independent judicial inquiry into the veracity of the attested facts."[20]

A federal pen/trap order can have effect outside the district of the issuing court. In the case of a federal applicant, the order "appl[ies] to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." 18 U.S.C. § 3123(a)(1).

The government must also use "technology reasonably available to it" to avoid recording or decoding the contents of any wire or electronic communications. 18 U.S.C. § 3121(c). When there exists no way to avoid the inadvertent collection of content through the use of reasonably available technology, Justice Department policy requires that the government may not use any inadvertently collected content in its investigation. However a few courts have gone beyond the statute's requirement that the government use technology reasonably available to it to avoid collecting content.

A pen/trap order may authorize the installation and use of a pen/trap device for up to sixty days and may be extended for additional sixty-day periods. See 18 U.S.C. § 3123(c). The order should direct the provider not to disclose the existence of the pen-trap or the investigation "to any…person, unless or until otherwise ordered by the court," 18 U.S.C. § 3123(d)(2), and may order providers of wire or electronic communications service, landlords, custodians, or other persons to furnish all "information, facilities, and technical assistance" necessary to install pen/trap devices unobtrusively and with a minimum of interference with services. 18 U.S.C. § 3124(a), (b).

The Pen/Trap statute requires record keeping and reporting when law enforcement officers install their own pen/trap device on a packet-switched data network of a provider of electronic communications service to the public. See 18 U.S.C. § 3123(1)(3). In such cases, the agency must maintain a record that identifies: (1) the identity of the officers who installed the device; (2) that the device was installed, uninstalled, and accessed to obtain information; (3) the configuration of the device at the time of installation and any subsequent modifications thereof; and (4) the information collected by the device. See 18 U.S.C. § 3123(a)(3)(A). This record must be provided to the court within thirty days after termination of the Pen/Trap order (including any extensions thereof). See 18 U.S.C.§ 3123(a)(3)(A).

The Pen/Trap statute also grants providers of electronic or wire communication service broad authority to use pen/trap devices on their own networks without a court order. 18 U.S.C. § 3121(b).

3. Emergency Pen/Traps

The Pen/Trap statute authorizes the installation and use of a pen/trap without a court order in emergency circumstances involving: (1) immediate danger of death or serious bodily injury to any person; (2) conspiratorial activities characteristic of organized crime; (3) an immediate threat to a national security interest; or (4) an ongoing attack on a protected computer. See 18 U.S.C. § 3125(a)(1). The installation and use of an emergency pen/trap requires approval at least at the Deputy Assistant Attorney General level, or by the principal prosecuting attorney of any state or subdivision thereof who is acting pursuant to a state statute. See 18 U.S.C. § 3125(a). In order to authorize an emergency pen/trap, the relevant official must reasonably determine that: (1) a specified emergency situation requires the installation and use of the pen/trap device before an order authorizing such installation and use can, with due diligence, be obtained, and (2) there are grounds upon which a pen/trap order could be entered to authorize the installation and use. See 18 U.S.C. § 3125(a).

A court order authorizing the installation and use of the emergency pen/trap device must be sought within 48 hours after its installation and use. See U.S.C. § 3125(a), (c). In the absence of such an order, the use of the emergency pen/trap device must immediately end when the earliest of these events occurs: (i) the information sought is obtained, (ii) the application for the order is denied, or (iii) 48 hours have passed since the installation of the pen/trap device. 18 U.S.C.§ 3125(b).

4. Pen/Trap Statute and Cell-Site Information

Cell-site data identifies the antenna tower and, in some cases, the 120-degree face of the tower to which a cell phone is connected at the start and end of each call made or received. At best, this data reveals the neighborhood in which a cell phone

[20] *In re Application of United States*, 846 F.Supp. 1555, 1559 (M.D. Fla. 1994); *See also United States v. Fregos*o, 60 F.3d 1314, 1320 (8th Cir. 1995) ("The judicial role in approving use of trap and trace devices is ministerial in nature").

user is located at the time a call starts and at the time it ends. It does not provide continuous tracking and is not a virtual map of a cell phone user's movement. Notwithstanding its relative lack of precision, cell-site information is an important investigatory mechanism that can help law enforcement determine where to establish physical surveillance and locate kidnapping victims, fugitives, and targets of criminal investigations.

In most districts, investigators can obtain prospective cell-site information through an application that satisfies both the Pen/Trap statute and 18 U.S.C. § 2703(d). The rationale beyond this "hybrid" use of the Pen/Trap statute and § 2703(d) is as follows: cell-site data is "dialing, routing, addressing, or signaling information." Hence, 18 U.S.C. § 3121(a) requires the government to obtain a pen/trap order to acquire this information. However, the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") precludes the government from relying "solely" on the authority of the Pen/Trap statute to obtain cell-site data for a cell phone subscriber. 47 U.S.C. § 1002(a). Hence, some additional authority is required to obtain prospective cell-site information. Section 2703(d) provides this authority because it authorizes the government to use a court order to obtain all non-content information concerning a customer or subscriber of an electronic communication service.

When they seek a hybrid order for prospective cell-site information, prosecutors must satisfy the requirements of both the Pen/Trap statute and 18 U.S.C. § 2703(d). This application should furnish: (i) a government attorney's affirmation "that the information likely to be obtained is relevant to an ongoing criminal investigation," 18 U.S.C. § 3122, and (ii) a further showing by the government attorney or "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Hybrid orders otherwise generally follow the procedures for pen/trap orders.

5. The Wiretap Statute ("Title III")

1. The General Prohibition

Title III governs real-time electronic surveillance of the contents of communications. If law enforcement officials want to wiretap a suspect's phone, monitor a hacker breaking into a computer system, or accept the fruits of wiretapping by a private citizen who has discovered evidence of a crime, they first must consider the implications of Title III.

Title III assumes that every private communication can be modeled as an exchange between two participating parties, such as a telephone call between A and B. The statute forbids using an electronic, mechanical, or other device to intercept private wire, oral, or electronic communications between the parties unless one of several statutory exceptions applies. See 18 U.S.C. §§ 2510(4), 2511(1). The prohibition is quite broad and unlike some privacy laws that regulate only certain cases or specific places, Title III expansively prohibits eavesdropping (subject to certain exceptions and interstate requirements) essentially everywhere, by anyone, in the U.S. Whether investigators want to conduct surveillance at a home, at a workplace, in government offices, in prison, or on the Internet, they must almost invariably ensure that the monitoring complies with Title III's prohibitions.

Law enforcement officials and prosecutors must pose the following questions to ensure compliance with Title III:

1) Is the communication to be monitored one of the protected communications defined in 18 U.S.C. § 2510?
2) Will the proposed surveillance lead to an "interception" of the communications?
3) If the answer to the first two questions is "yes," does a statutory exception apply that allows the interception?

2. Key Phrases

Title III broadly forbids the "interception" of "oral communications," "wire communications," and "electronic communications." These phrases are defined by the statute. See 18 U.S.C. §§ 2510(1), (2), (4), (12).

In general, telephone conversations are wire communications. The most important requirement is that the content of the communication must include the human voice. If a communication does not contain a human voice, either alone or in a group conversation, then it is not a wire communication. The additional requirement that wire communications must be sent "in whole or in part…by the aid of wire, cable, or other like connection."

Most Internet communications (including email) are electronic communications. "Electronic communication" is a broad, catch-all category. As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in party by wire).

The structure and language of the Stored Communications Act (SCA) and Title III require that the term "intercept" be applied only to communications acquired contemporaneously with their transmission. Title III defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The statutory definition of "intercept" does not expressly require that the "acquisition" of the communication be contemporaneous with the transmission of the communication. However, a contemporaneity requirement is necessary to maintain the proper relationship between Title III and the SCA's restrictions on access to stored communications. Otherwise, for example, a Title III order could be required to obtain unretrieved email from a service provider.

3. Exceptions to Title III's Prohibitions

Title III broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. See 18 U.S.C. § 2511(1). In general, this prohibition bars third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.

The breadth of Title III's prohibition means that the legality of most surveillance techniques under Title III depends upon the applicability of a statutory exception. Title III has dozens of exceptions that may or may not apply in hundreds of different situations. In cases involving computer crimes or computer evidence, however, seven exceptions are especially pertinent as follows.

a. Interception Authorized by a Title III Order, 18 U.S.C. § 2518

Title III allows law enforcement to intercept wire and electronic communications pursuant to a court order under 18 U.S.C. § 2518 (a "Title III order"). Law enforcement officials must obtain high-level Justice Department approval for federal Title III applications, by statute in the case of wire communications, see 18 U.S.C. § 2516(1), and by Justice Department policy in the case of electronic communications (except for numeric pagers). When authorized by the Justice Department and signed by a U.S. district court or court of appeals judge, a Title III order allows law enforcement to intercept communications for up to thirty days. See 18 U.S.C. § 2518(5).

Title III imposes several formidable requirements that must be fulfilled before investigators can obtain a Title III order. See 18 U.S.C. §§ 2516-2518. The application for an order must show probable cause to believe that the interception will reveal evidence of a predicate felony office listed in § 2516. See § 2518(3)(a)(b). For federal officials, the predicate felony offense must be one of the crimes specifically enumerated in § 2516(2). The application for a Title III order must also: (1) show that normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed or to be too dangerous, see § 2518(1)(c); and (2) show that the surveillance will be conducted in a way that minimizes the interception of communications that do not provide evidence of a crime. See § 2518(5).

b. Consent of a Party to the Communication, 18 U.S.C. § 2511(2)(c)-(d)

The consent exceptions under paragraphs 2511(2)(c) and (d) are perhaps the most frequently used exceptions to Title III's general prohibition on intercepting communications. The first consent exception applies to those acting under color of law:

It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

The second consent exception applies more generally:

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

In general, both of these provisions authorize the interception of communications when one of the parties to the communication consents to the interception. For instance, if an undercover government agent or informant records a telephone conversation between his/herself and a suspect, his/her consent to the recording authorizes the interception.[21] Similarly, if a private person records his/her own telephone conversations with others, his/her consent authorizes the interception unless the commission of a criminal or tortious act was at least a determinative factor in his/her motivation for intercepting the communication.[22]

Consent under subsections 2511(c) and (d) may be express or implied.[23] The key to establishing implied consent in most cases is showing that the consenting party received actual notice of the monitoring and used the monitored system anyway.

i. Bannering and Consent

Monitoring use of a computer network does not violate Title III after users view an appropriate network banner informing them that use of the network constitutes consent to monitoring. A banner is a posted notice informing users as they log on to a network that their use may be monitored, and that subsequent use of the system constitutes consent to the monitoring.

ii. Who Is a "Party to the Communication" in a Network Intrusion?

Sections 2511(2)(c) and (d) allow any "person" who is a "party to the communication" to consent to monitoring of that communication. In the case of wire communications, a "party to the communication" is usually easy to identify. For instance, either conversant in a two-way telephone conversation is a party to the communication.

---

[21] *See e.g., Obron Atlantic Corp. v. Barr*, 990 F.2d 861, 863-64 (6th Cir. 1993) (relying on § 2511(2)(d).

[22] *See United States v. Cassiere*, 4 F.3d 1006, 1021 (1st Cir. 1993) (interpreting § 2511(2)(d).

[23] *See United States v. Amend*, 831 F.2d 373, 378 (2d Cir. 1987).

c. The Provider Exception

Employees or agents of communications service providers may intercept and disclose communications to protect the providers' rights or property. For example, system administrators or computer networks generally may monitor hackers intruding into their networks and then disclose the fruits of monitoring to law enforcement without violating Title III. This privilege belongs to the provider alone, however, and cannot be exercised by law enforcement. After the provider has communicated with law enforcement, the computer trespasser exception may provide surer basis for monitoring by law enforcement.

The "rights or property of the provider" clause of § 2511(2)(a)(1) grants providers the right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service."[24] For instance, employees of a cellular phone company may intercept communications from an illegally "cloned" cell phone in the course of locating its source.[25]

Hence, providers investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under § 2511(2)(a)(i), but should try to tailor their monitoring and disclosure to that which is reasonably related to the purpose of the monitoring.

Agents and prosecutors should refrain from using the provider exception to satisfy law enforcement needs that lack a substantial nexus with the protection of the provider's rights and property. While the exception allows providers to intercept and disclose communications to law enforcement to protect their rights or property, it does not allow law enforcement officers to direct or ask system administrators to monitor for law enforcement purposes.

Law enforcement involvement in provider monitoring of government networks creates special problems. Because the lines of authority often blur, law enforcement agents should exercise special care.

d. The Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i)

Title III permits victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. In particular, the computer trespasser exception provides:

It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if:

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communication on the protected computer;
(II) the person acting under color of law is lawfully engaged in an investigation;
(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C.§ 2511(2)(i).

18 U.S.C. § 2510(21) defines a "computer trespasser" to include any person who accesses a "protected computer" without authorization, provided the person is not "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."

The exception authorizes law enforcement or a private party acting at the direction of law enforcement to intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before the interception can occur, the four requirements found in § 2511(2)(i)(I)-(IV) must be met.

e. The Extension Telephone Exception, 18 U.S.C. § 2510(5)(a)

As a result of Title III's "extension telephone" exception, the statute is not violated by the use of:

Any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

18 U.S.C. § 2510(5)(a). Congress intended this exception to have a fairly narrow application: the exception was designed to allow businesses to monitor by way of an "extension telephone" the performance of their employees who spoke on the phone to customers. The "extension telephone" exception clarifies that when a phone company furnishes an employer with an extension

[24] *United States v. Villanueva*, 32 F.Supp. 2d 635, 638 (S.D.N.Y. 1998).
[25] *See United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997).

telephone for a legitimate work-related purpose, the employer's monitoring of employees using the extension phone for legitimate work-related purposes does not violate Title III.[26]

f. The 'Inadvertently Obtained Criminal Evidence' Exception, 18 U.S.C. § 2511(3)(b)(iv)

Section 2511(3)(b) lists several narrow contexts in which a provider of electronic communication service to the public can divulge the contents of communications. The most important of these exceptions allows a public provider to divulge the contents of any communications that

Were inadvertently obtained by the service provider and which appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

18 U.S.C. § 2511(3)(b)(iv).

g. The 'Accessible to the Public' Exception, 18 U.S.C. § 2511(2)(g)(i)

Section 2511(2)(g)(i) allows "any person" to intercept an electronic communication made through a system "that is configured so that…[the] communication is readily accessible to the general public." Congress intended this language to allow the interception of an electronic communication that has been posted to a public bulletin board, a public chat room, or a Usenet newsgroup.

6. Remedies for Violations of Title II and the Pen/Trap Statute

Law enforcement officials and prosecutors must comply with Title III and the Pen/Trap statute when they plan electronic surveillance. Violations can result in criminal penalties, civil liability, and (in the case of certain Title III violations) suppression of the evidence obtained. See 18 U.S.C. § 2511(4) (criminal penalties for Title III violations); 18 U.S.C. §2520 (civil action for Title III violations); 18 U.S.C. § 3121(d) (criminal penalties for Pen/Trap statute violations); 18 U.S.C. § 2707(a), (g) (civil action for certain Pen/Trap statute violations); 18 U.S.C. § 2518(10)(a) (suppression for certain Title III violations). However, as a practical matter, courts may conclude that the electronic surveillance statutes were violated even after agents and prosecutors have acted in good faith and with full regard for the law. For instance, a private citizen may wiretap his/her neighbor and later turn over the evidence to the police, or agents may intercept communications using a court order that the agents later learn is defective. In addition, a court may construe an ambiguous portion of Title III differently than did the investigators, leading the court to find that a violation of Title III occurred. Accordingly, prosecutors and agents must understand not only what conduct the surveillance statutes prohibit, but also what the ramifications might be if a court finds that the statutes have been violated.

1. Suppression Remedies

Title III provides for statutory suppression of wrongfully intercepted oral and wire communications, but not electronic communications. The Pen/Trap statute does not provide a statutory suppression remedy. Constitutional violations may also result in suppression of the evidence wrongfully obtained.

2. Defenses to Civil and Criminal Actions

Agents and prosecutors are generally protected from liability under Title III for reasonable decisions made in good faith in the course of their official duties.

7. U.S. Law Provisions for Mutual Legal Assistance Concerning Interception of Telecommunication

1. *U.S. Law Provisions for Mutual Assistance on Interception of Telecommunications*

The U.S. is a member of the Council of Europe Cybercrime Convention. Art. 34 permits parties to request assistance in the interception of content data. However, it is narrowly drawn. There is no general obligation to provide this form of cooperation. Instead, assistance is available "only to the extent" already allowed by applicable mutual legal assistance treaties and domestic law. In the U.S., such law, as mentioned above, is subject to close judicial supervision. In no case can a foreign authority obtain information on terms that are less restrictive than for U.S. law enforcement. Currently, no authority exists to intercept communications based solely on the request of a foreign government.

The U.S. can only accommodate such a request if the interception of the communications were independently authorized as part of a related or parallel investigation in the U.S., and disclosing the contents of the intercepted communications were otherwise appropriate.[27] A search warrant does not comprise enough authority to intercept the content of communications in transmission, as that collection is governed by the wiretap and interception statutes discussed above. Although a search warrant can be used to obtain stored data, it must involve a crime recognized under U.S. law.[28]

---

[26] *See Briggs v. Am. Air Filter Co*., 630 F.2d 414, 418 (5th Cir. 1980) (reviewing legislative history of Title III); *Watkins v. L.M. Berry & Co*., 704 F.2d 577, 582 (11th Cir. 1983) (applying exception to permit monitoring of sales representatives); *James v. Newspaper Agency Corp*., 591 F.2d 579, 581 (10th Cir. 1979) (applying exception to permit monitoring of newspaper employees' conversations with customers).

[27] *See* 18 U.S.C. § 2517(7).

[28] U.S. Senate Committee on Foreign Relations, Council of Europe Convention on Cybercrime (Treaty Doc. 108-11), 109th Congr., 1st Sess, Exec. Rept. 109-6, Nov. 8, 2005, at 4.

At least one U.S. MLAT, namely Article 12 of the German Treaty[29] provides:

Each party may at the request of the other party, within its possibilities and under the conditions prescribed by its domestic law,

1. take the necessary steps for the surveillance of telecommunications,
2. permit the operation in its territory of criminal investigations by law enforcement officials of the other party acting under covert or false identity, and
3. permit controlled deliveries in connection with criminal investigations.

This article is to implement more detailed articles in the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters[30] and the United Nations Conventions Against Transnational Organized Crime and Corruption. The U.S. government is trying to include similar provisions in its future bilateral treaties on mutual assistance in criminal matters, thereby significantly broadening the scope of treaty sanctioned transnational investigations by its law enforcement agencies.[31]

2. *U.S. Participation in International Conventions on the Interception of Communications*

As mentioned, the U.S. is a member of the Council of Europe Cybercrime Convention. It ratified the Convention on September 29, 2006. The Convention became effective in the U.S. on January 1, 2007.[32]

a. The Extent to Which General Grounds for Refusal Apply Concerning Internet Searches and Other Means to Look Into Computers and Networks Located Elsewhere

U.S. legislative history indicates that the grounds for refusal for the U.S. as a requested state contained in article 27(4) of the Cybercrime Convention are analogous to those contained in U.S. bilateral MLATs. Assistance is to be provided in accordance with the provisions of mutual legal assistance treaties between the parties where they exist. Where no such treaties exist between parties, Article 27 of the Convention provides a procedural mechanism for cooperation to be applied between them, including the grounds for refusal of such requests (in addition to any grounds provided under the law of the requested party).[33]

The grounds for refusal contained in Article 27(4) of the Cybercrime Convention are analogous to those contained in U.S. bilateral MLATs. Among the most important of the grounds whereby the U.S. as the requested state can deny assistance are: prejudice to sovereignty, security, or other essential public interest; requested procedure prohibited by the law of the requested country; excludable offenses; non-compliance with the treaty; refusal to disclose non-public government documents; refusals to transfer person in custody; lack of reasonable grounds or suspicion; non bis in idem; effect on human rights; political offense or offense related to political offense; and military offense.[34]

The executive branch officials confirmed to the Senate Foreign Relations Committee that the defense of "prejudice to sovereignty, security or other essential public interest" authorizes the U.S. to deny a request where providing the assistance would impinge on U.S. Constitutional protections, such as free speech, and that the executive branch intends to deny assistance in such situations. In addition, executive branch officials committed that "[T]he Department of Justice will carefully review each request, regardless of the country from which it comes, to ensure that compliance with it would not impinge on U.S. fundamental principles and policy, and that U.S. implementation of foreign requests would not be inconsistent with Constitutional protections."[35]

b. Whether the U.S. Double Criminality Requirement for Cooperation Is Justified in Situations in Which the Perpetrator Caused Effects from a State in Which the Conduct Was Allowed into a State Where the Conduct is Criminalized

The lack of a dual criminal requirement in conventions, such as the Cybercrime Convention, is not a per se barrier to the U.S. government rendering mutual assistance. In the last few decades, the U.S. has concluded approximately 50 bilateral mutual legal assistance treaties that do not require dual criminality.

The U.S. believes that its MLATs and the Cybercrime Convention provide enough protection of U.S. constitutional interests. For instance, Art. 27(4) of the Cybercrime Convention are analogous to those contained in U.S. bilateral MLATs. A requested party can refuse any request concerning a political offense or that is likely to prejudice its sovereignty, security, *ordre public,* or other

[29] Entered into force February 1, 2010.

[30] The text of the Second Additional protocol, the official explanatory report, a list of the signatories and parties, and the text of their reservations and declarations are available on the Council of Europe treaty website: http://conventions.coe.int.

[31] Michael Abbell, OBTAINING EVIDENCE ABROAD IN CRIMINAL CASES 2010, §4-4, 181 (2010).

[32] *See* the treaty website at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG (accessed Dec. 12, 2012).

[33] U.S. Senate Foreign Relations Committee, Council of Europe Convention on Cybercrime, 109th Cong., 1st Sess., Exec. Rept. 109-6 at 5 (Nov. 8, 2005).

[34] For more discussion on reasons for denying a request for assistance, *see* Michael Abbell, OBTAINING EVIDENCE ABROAD IN CRIMINAL CASES §4.5 (pp. 181-87) 2010.

[35] U.S. Senate Foreign Relations Committee, Council of Europe Convention on Cybercrime, *supra*, at 5.

essential interests. In response to questions from the Senate Foreign Relations Committee in connection with the ratification of the Cybercrime Convention, U.S. executive branch officials confirmed that these provisions in Art. 27 authorize the U.S. to deny a request where providing the assistance would impinge on U.S. constitutional protections, such as free speech. The U.S. executive branch said it intends to deny assistance in such situations.[36]

3. *Whether U.S. National Law Permits Extraterritorial Investigations? If so, under Which Conditions?*

The U. S., like other countries, takes the position that it can use its own legal mechanisms to request data from any cloud server located anywhere around the world so long as the cloud service provider is subject to US jurisdiction — that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.[37]

a. U.S. Extraterritorial Investigations

The U.S. has at least nine different methods of coercion to obtain evidence located abroad, to obtain testimony from witnesses located abroad, and to secure the transfer of private assets to the U.S. These methods include: (1) compelling testimony of U.S. nationals or residents located abroad through subpoenas issued by federal courts and notwithstanding potential violations of the laws of other countries, especially civil law countries; (2) compelling production of documents located abroad when a U.S. court has personal jurisdiction over the alleged wrongdoer, the documents, or other tangible evidence is in the possession, custody, or control of the alleged wrongdoer, or a related entity, and the production of the evidence is not protected by an evidentiary privilege; (3) compelling the production of documents located abroad from a third party that is not a target of the investigation or a defendant in the prosecution, including documents of foreign banks or corporations or of foreign branches of U.S. banks or corporations with which the target or defendant conducted business; (4) compelling through a subpoena a foreign witness in the U.S., including persons transiting the U.S., to testify; (5) compelling the production of documents from foreign entities by a subpoena *duces tecum* of an officer or custodian over whom the U.S. has personal jurisdiction; (6) compelling "consents" to disclose third-party records as means to overcome bank secrecy; (7) compelling targets of U.S. criminal investigations and defendants not to seek action abroad to block prosecutors' efforts to obtain evidence; (8) compelling repatriation of assets to pay a fine or taxes or for purposes of forfeiture; and (9) imposing a tax levy on a bank in the U.S. for funds of a taxpayer located in a foreign branch.

The person whose testimony or assistance is sought often challenges the use of coercive methods to obtain evidence abroad, as do foreign courts. These challenges raise a host of legal issues, including constitutional questions – including the right against self-incrimination, due process, improper search and seizures – jurisdiction, conflicts of law, and foreign sovereign compulsion. Often the more difficult coercive techniques involve third parties abroad and subpoenas directing witness testimony from foreign persons or the production of documents from foreign entities. The coercive techniques often work when federal courts serve them on persons in the U.S. over whom the court has established jurisdiction, especially if documents or other tangible evidence are believed to be within their possession, custody, or control – even if located abroad.

b. Extraterritorial Investigations for Foreign Authorities

In general, the U.S. will not conduct extraterritorial investigations to give mutual assistance to foreign governments. For instance, since the U.S. implements the Cybercrime Convention, consistent with existing procedures for mutual legal assistance, the U.S. does not and will not use tools authorized under Foreign Intelligence Surveillance Act procedures or administrative subpoenas to meet its treaty obligations. Rather, the U.S. uses longstanding statutory and mutual legal assistance treaty and agreement procedures consistently with the judicial oversight provided under those treaties and laws, in full compliance with the rights guaranteed under the U.S. Constitution. For instance, U.S. execution of foreign government requests for collection of disclosure of electronic evidence would require judicial oversight.[38] Yet, U.S. service providers may receive judicial orders from other countries to disclose such information. Direct application of foreign laws, including privacy frameworks, have far-reaching implications for service providers everywhere. Expanded trans-border access would likely make business even more complicated.

In connection with foreign judicial orders, the U.S. does not accommodate national law enforcement authorities or judicial orders, requesting information from third parties and other persons in the absence of MLAT requests. In this connection, service providers and other businesses with websites that can be used by persons in other countries, and other third parties that hold

---

[36] *Id*. at 5.

[37] Council of Europe, *Discussion paper Transborder access and jurisdiction: What are the options*? Report of the Transborder Group Adopted by the T-CY on 6 December 2012, Cybercrime Convention Committee (T-CY) Ad-hoc sub-group on jurisdiction and transborder access to data, Report of the Transborder Group
Adopted by the T-CY on 6 December 2012, http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf (accessed Dec. 17, 2012).

[38] *Id*. at 5-6.

data for or about a person, are already struggling to comply with disparate and sometimes conflicting laws of different states. For example, it is usually a criminal offense in the United States for a commercial service provider to disclose to anyone (including a foreign government) the contents of an electronic communication.[39]

4. *Is Self Service (Obtaining Evidence in Another State Without Asking Permission) Permitted? What Conditions Should Be Fulfilled in Order to Allow Self Service? How Does the U.S. Differentiate for Public and Protected Information? What Is the (Both Active and Passive Practice) in the U.S.?*

In the case of *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), the U.S. Supreme Court upheld the use of evidence seized in Mexico, even though the search did not occur pursuant to a warrant and appeared not to conform to either U.S. or Mexico legal requirements concerning search and seizure. Because the defendant was not a U.S. citizen, the court held that the Fourth Amendment and the Bill of Rights do not apply to foreigners, but only U.S. citizens.

To the extent the U.S. conducts wiretaps and some of the conversations occur in another country, the U.S. law enforcement agents may be said to engage in self-service. There have been a number of high profile law enforcement cases, such as that of Christopher "Dudus" Coke. The Jamaican Prime Minister at the time, Bruce Golding, publicly said the Jamaican government would not honor the U.S. extradition request because it was based on illegally obtained evidence, namely U.S. wiretaps on Jamaican territory. However, Coke eventually surrendered and waived extradition. His counsel moved to suppress the evidence from the illegal wiretaps. After the U.S. court denied his motion, he pled guilty.[40]

In 2003, both the High Court and subsequently the Eastern Caribbean Supreme Court upheld the extradition. The defendants appealed to the UK Privy Council. In the meantime, the two individuals— Noel Heath and Glenroy Matthew—have been named Specially Designated Narcotics Traffickers under the Foreign Narcotics Kingpin Designation Act. One of the major legal issues in their case was whether the court could use evidence from U.S. wiretaps on St. Kitts territory in support of the extradition requests. However, the U.S. had permission from St. Kitts to conduct wiretaps in St. Kitts.[41]

5. *If the U.S. Has Self-Service Legislation, Does Such Legislation Also Apply to Searches to be Performed on the Publicly Accessible Web, or In Computers Located Outside the U.S.?*

It appears, as discussed in the preceding section, that most U.S. self-service is done through practice, rather than by legislation.

6. *Is the U.S. a Party to Passenger Name Record (PNR) (Financial Transactions, DNA-Exchange, Visa Matters or Similar Agreements? Specify and State How the Exchange of Data Is Implemented into National Law. Does the U.S. Have an On-Call Unit that Is Staffed on a 24/7 Basis to Exchange Data with Respect to Information for Criminal Investigation?*

The U.S. shares information on travelers with a handful of countries to better secure, manage, and facilitate the international movement of people. The U.S. and EU members have concluded information-sharing agreements concerning human mobility in the context of strengthening security against "dangerous individuals" and facilitating travel for low risk individuals.

Governments obtain and analyze data on travelers for two main purposes: (1) for traditional security purposes, such as countering terrorism and combating organized crime; and (2) for human mobility-related purposes, such as managing travel and immigration.

The U.S. and some of its partners process information on travelers, including information contained in a visa application, the biographical page of a passport, the biometric chip of an electronic passport, the biometric digital facial picture, and fingerprints submitted to immigration authorities upon arrival at a port of entry, the details included in flight reservations, credit card numbers, frequent flyer miles, and meal preferences.[42]

a. Passenger Name Records

United States (U.S.) law requires airlines operating flights to or from the United States to provide the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) with certain passenger data (referred to as Passenger Name Record (PNR) data) that allows CBP to facilitate safe and efficient travel. This practice has been widely accepted around the world and is increasingly replicated by foreign border authorities, although some commentators in Europe have questioned the privacy impact of this requirement.

---

[39] Council of Europe, *Discussion paper Transborder access and jurisdiction: What are the options?* Report of the Transborder Group Adopted by the T-CY on 6 December 2012, United States Code, Title 18, Section 2701, available at http://uscode.house.gov/download/title_18.shtml, *supra*, at 13.

[40] Chris McGreal, *Christopher 'Dudus' Coke tells US court: 'I'm pleading guilty because I am'*, THE GUARDIAN, Sept. 1, 2012 http://www.guardian.co.uk/world/2011/sep/01/christopher-dudus-coke-us-court.

[41] *See, e.g., Noel Zambo Heath sold to the U.S. Injustice System for Rice and Peas*, http://groups.yahoo.com/group/amlaselassie/message/1, Feb. 13, 2007.

[42] Hiroyuki Tanaka, Rocco Bellanova, Susan Ginsberg, Paul deHert, *Transnatlantic Information Sharing: At a Crossroads,* Migration Policy Institute (Jan. 201) at 9 (http://www.migrationpolicy.org/pubs/infosharing-Jan2010.pdf).

The European Union has determined that U.S. laws, in conjunction with DHS/CBP policies regarding the protection of Personally Identifiable Information (PII) and the U.S. – EU PNR Agreement signed in July 2007, provide an adequate basis upon which to permit transfers of PNR data to the U.S. consistent with applicable EU law.[43]

The purpose of collecting PNR information in advance of a passenger's arrival or departure is to enable CBP to make accurate, comprehensive decisions regarding which passengers require additional inspection at the port of entry based on law enforcement information and other intelligence. Collecting this information in advance provides the traveler two advantages. First, it affords CBP adequate time to research possible matches against derogatory records to eliminate false positives. Second, it expedites travel by allowing CBP to conduct mandatory checks prior to a flight's arrival in the U.S., rather than making the passenger, and everyone else on the flight, stand in line while the CBP manually conduct the review after the passenger arrives.

CBP uses PNR strictly for the purposes of preventing and combating: terrorism and related crimes; other serious crimes, including organized crime, that are transnational in nature; and flight from warrants or custody for crimes described above.[44]

PNR is also used whenever necessary for the protection of the vital interests of a data subject or other persons, in any criminal judicial proceedings, and as otherwise required by law.

By legal statute, 49 U.S. Code § 44909(c)(3) and its implementing (interim) regulations, 19 C.F.R. § 122.49d, each air carrier operating passenger flights in foreign air transportation to or from the U.S. must provide CBP with electronic access to PNR data to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.

CBP and DHS officials responsible for identifying illicit travel and preventing and combating terrorism, transnational crime, and related crimes will have access to PNR data derived from flights between the U.S. and the EU. This PNR data may be transferred to other domestic and foreign government authorities with counter-terrorism, law enforcement, or public security functions in support of counterterrorism, transnational crime, and public security related cases they are examining or investigating, specifically related to the purposes identified above in response to FAQ 1.

PNR data may also be provided to other relevant government authorities, when necessary to protect the vital interests of the passenger who is the subject of the PNR data or of other persons, in particular as regards to significant health risks, or as otherwise required by law.[45]

PNR data is only exchanged with other foreign government authorities after consideration of the recipient's intended use(s) and ability to protect the information.[46]

PNR data derived from flights between the U.S. and the EU will be kept by CBP for a period of seven years in an active file and eight years in an inactive file, which requires additional approvals for access. Additionally, PNR information that is linked to a specific enforcement record will be maintained by CBP until the enforcement record is archived.[47]

The Department of Homeland Security's Chief Privacy Officer is statutorily obligated to ensure that personally identifiable information is handled in a manner that complies with relevant law. He or she is independent of any directorate within DHS and will exercise oversight over the program to ensure strict compliance by CBP and to verify that proper safeguards are in place.[48]

DHS allows persons, including foreign nationals, to seek administrative access under the Privacy Act to their individual PNR data maintained in ATS-P.[49]

In cases where CBP denies access to PNR data pursuant to an exemption under the Freedom of Information Act (FOIA), such a determination can be administratively appealed to the Chief Privacy Officer of DHS, who is responsible for both privacy protection and disclosure policy for DHS. A final agency decision may be judicially challenged under U.S. law.

Passengers can request that corrections be made to their PNR. The PNR is usually information that the passenger (or his or her representative) supplied. Before requesting corrections be made to the passenger's PNR, the passenger should ask for a copy of

---

[43] For additional information on this arrangement, *see* the agreement and exchange of letters between the DHS Secretary and the EU at http://www.dhs.gov/xinfoshare/programs/editorial_0724.shtm. For a comprehensive explanation of the manner in which DHS/CBP generally handles PNR data, please refer to the Automated Targeting System (ATS) Systems of Records Notice (SORN) at http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-15197.htm and the Privacy Impact Assessment (PIA) for ATS at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf.

[44] Department of Homeland Security, Frequently Asked Questions, U.S. Customs and Border Protection Receipt of Passenger Name Record (PNR) Data Flights between the European Union and the United States, pnr_faq.doc (accessed Dec. 17, 2012).

[45] *Id., FAQs 2 and 6.*

[46] *Id.,* FAQ 7.

[47] *Id*., FAQ 8.

[48] *Id*., FAQ 10.

[49] *Id.* FAQ 11, citing Section 7.0 of the ATS PIA at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf).

the record through the FOIA process to determine what information is actually in his/her PNR record(s). If the passenger believes the record contains an error, s/he should send a letter describing his/her concern to FOIA Request co/ CBP. [50]

b. Financial Transactions

At the end of 2009, the European Union passed a controversial measure, with Germany, Austria, Greece, and Hungary abstaining, which allows American justice authorities to access data from SWIFT - the Society for Worldwide Interbank Financial Telecommunications, a cooperative of banks and other financial institutions that facilitates trillions of dollars in daily international transactions. Its members include almost 8,000 financial institutions in more than 200 countries. The agreement falls under the Terrorist Finance Tracking Program (TFTP), an initiative created by the U.S. Department of Treasury following the events of September 11, 2001.

Since 2001, the SWIFT network had been used for several years by the Treasury Department to identify, locate, and track down people suspected of terrorism, as well as their financial backers. SWIFT had provided the Treasury with targeted data to trace the movements of terrorism-related funds, including identifying information about the originator and/or recipient of a transaction.

The first five years of SWIFT operations were conducted in secret, but were revealed by the press in June 2006[51], after which the European Parliament called for the establishment of a framework that would protect privacy rights. The outline of the SWIFT agreement was designed to ensure appropriate data protection and prevent the data being used for purposes other than counter-terrorism.

Some European states had worried about the possibility that personal information could be passed on from the U.S. to third parties, though the agreement states that the U.S. will not be allowed to share European data with third countries, and transactions between EU countries will not be monitored.

The new agreement limits U.S. authorities' information requests to people with links to terrorist activity. U.S. authorities also must justify their requests with the U.S. Treasury, and must structure them to be as specific as possible. However, if a pinpointed request is not possible, SWIFT would provide “all relevant” data - which could include names, addresses, and personal identification numbers.

In July 2010, the European Parliament also voted to adopt the SWIFT agreement, after rejecting an earlier rendition of the agreement in February 2010. “After rejecting the previous agreement, MEPs demanded that European citizens should be guaranteed the same judicial redress procedures as those applied to data held on the territory of the European Union, and in particular payment of compensation in cases of illegal processing of personal data. They pointed out that the U.S. Privacy Act, which protects U.S. citizens against such misuse, does not protect European citizens who might become victims of such misuse on American soil. The new proposal says this time that U.S. law must provide a right of redress, regardless of nationality.”[52]

The text was adopted with 484 votes in favor and 109 against, with the agreement entering into force at the beginning of August 2010 and valid for five years. From there, the agreement automatically renews itself, one year at a time. In order for the agreement to be terminated, one of the participating parties must pursue an initiative to stop it. However, even if the agreement were to terminate, all transferred data will remain at the disposal of U.S. authorities and subject to a retention period of five years.

The supporters of the current version claim that the new text was significantly improved by gaining a number of important concessions from the US, including the limitation of bulk data being transferred to the U.S. or the role of Europol in overseeing the transfer process. However, the data protection European bodies - EDPS and the Article 29 Working Party – have said that the agreement, despite its modifications does not meet the European privacy standards.

In actuality, SWIFT can't currently limit data searches to specific individuals or single transactions. In practice, SWIFT must transfer data about all transactions from a certain country or a certain bank on a certain date.

c. DNA-Exchange

The U.S. exchanges DNA samples. Most U.S. MLATs have a provision under Article 1 (Scope of Assistance) that states the signatories shall provide mutual assistance that includes “any other form of assistance not prohibited by the laws of the Requested State.”

The U.S. exchanges DNA samples under this provision and expects its MLAT partners to exchange DNA material unless the law of the Requested State expressly forbids such exchanges.

---

[50] *Id.*, FAQ 12. For further information regarding the procedures for making such a request, *see* 19 C.F.R., Part 103 (www.dhs.gov/foia).

[51] Parliament Examines Swift II Agreement, Justice and Home Affairs, European Parliament, Jul. 2, 2010, http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20100205BKG68527&language=EN.

[52] *Id.*

d. Visa Matters

The U.S. government does share visa information with a few countries by agreement. For instance, on December 13, 2012, the U.S. ambassador to Canada, David Jacobson, and the Canadian minister of citizenship, immigration and multiculturalism, Jason Kenney, signed a U.S.-Canada visa and immigration information-sharing agreement.

This agreement authorizes Canada and the U.S. to share information from third country nationals who apply for a visa or permit to travel to either country. The goal is to better protect the safety and security of Americans and Canadians and facilitate legitimate travel and business.

Increased information sharing will support better decision-making by both countries to confirm applicants' identities, and identify risks and inadmissible persons at the earliest opportunity. It will increase safety and security, as both countries work to identify terrorists, violent criminals, and others who pose a risk before they reach the borders.

All officers working on immigration and refugee protection will be equipped with more information to make decisions. The agreement will better protect the safety and security of Americans and Canadians alike and further facilitate legitimate travel.

The agreement authorizes development of arrangements under which the United States may send an automated request for data to Canada, such as when a third country national applies to the United States for a visa or claims asylum.

Such a request would contain limited information, such as name and date of birth in the case of biographic sharing, or an anonymous fingerprint in the case of biometric sharing. If the identity matches that of a previous application, immigration information may be shared, such as whether the person has previously been refused a visa or removed from the other country.

The same process would apply in reverse when a third country national applies to Canada for a visa or claims asylum. Biographic immigration information sharing is set to begin in 2013, and biometric sharing in 2014.

Under the agreement, information will not be shared regarding U.S. or Canadian citizens or permanent residents. Any information shared on travelers and asylum seekers will be handled responsibly and, as with other information sharing agreements, exchanged in accordance with relevant U.S. and Canadian laws.[53]

e. The U.S. Has an On-Call Unit That Is Staffed on a 24/7 Basis to Exchange Data With Respect to Information for Criminal Investigation

Pursuant to Article 35, paragraph 1 of the Cybercrime Convention, the Computer Crime and Intellectual Property Section (CCIP), U.S. Department of Justice, Criminal Division, Washington, D.C. 20530, is designated as the point of contact available on a 24-hour, seven-day-a week basis to ensure the provision of immediate assistance under the Convention.

The CCIP is a section of the Criminal Division of the U.S. Department of Justice that has 40 lawyers with responsibilities for combating cybercrime and theft of intellectual property, and with expertise in obtaining electronic evidence. Many CCIPS lawyers also have expertise in international assistance. CCIPS has "duty attorneys" available 24-hours a day, 7 days a week to respond to urgent requests for assistance.

7. *To What Extent Will Data Referred to in the Answer to the Previous Question Be Exchanged for Criminal Investigation and On Which Legal Basis? To What Extent Does the Person Involved Have the Possibility to Prevent/Correct/Delete Information? To What Extent Can This Information Be used As Evidence? Does the Law of Your Country Allow for a Notice and Take-Down of a Website Containing Illegal Information? Is there a Practice? Does the Seat of the Provider, Owner of the Site or Any Other Foreign Element Play a Role?*

If the data that is exchanged shows evidence of the types of crimes covered by the agreement, then it can be used as evidence or at least serve as the basis for an additional request.

Persons whose data has been collected have a right to try to correct the information, but their access to the information and ability to make the corrections has been a subject of criticism, negotiation, and changes in some of the applicable procedures.

Notice and take down is a process operated by online hosts in response to court orders or allegations that content is illegal. Content is removed by the host following notice. Notice and take down is widely operated in relation to copyright infringement, as well as for libel and other illegal content. In the U.S., notice and takedown is mandated as part of limited liability, or safe harbor, provisions for online hosts (e.g., the Digital Millennium Copyright Act 1998). As a condition for limited liability, online hosts must expeditiously remove or disable access to content they host when they are notified of the alleged illegality.

The Online Copyright Infringement Liability Limitation Act, enacted in 1998 as part of the Digital Millennium Copyright Act (DMCA), has safe harbor protection to "online service providers" for "online storage" in Section 512(c). Section 512(c) applies to online service providers that store copyright infringing material. In addition to the two general requirements that online service providers comply with standard technical measures and remove repeat infringers, section 512(c) also requires that the online

[53] U.S. Department of State, U.S.-Canada Visa and Immigration Information-Sharing Agreement, Dec. 14, 2012, http://www.state.gov/r/pa/prs/ps/2012/12/202065.htm; *US and Canada Sign Visa and Immigration Information-Sharing Agreement*, Caribbean NewsNow.com, Dec. 17, 2012.

service providers: 1) do not receive a financial benefit directly attributable to the infringing activity, 2) are not aware of the presence of infringing material or know any facts or circumstances that would make infringing material apparent, and 3) upon receiving notice from copyright owners or their agents, act expeditiously to remove the allegedly copyright infringing material.

The copyright owner may furnish written notification of claimed infringement to an online service provider. Section 521(c) lists a number of requirements the notification must comply with, including: identification of the copyrighted work claimed to have been infringed and information reasonably sufficient to permit the service provider to locate the material; information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number and email address; a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; a statement that the information in the notification is accurate, and under penalty of perjury, and that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.[54]

If the notification complies with the requirements of Section 512, the online service provider must expeditiously remove or disable access to the allegedly infringing material.[55]Thereafter, the online service provider must take reasonable steps to promptly notify the alleged infringer of the action.[56] If there is a counter notification from the alleged infringer, the online service provider must then promptly notify the claiming party of the individual's objection.[57] If the copyright owner does not bring a lawsuit in district court within 14 days, the service provider must restore the material to its location on its network.[58] A counter notice claiming that the material does not infringe copyrights, the service provider must also comply with requirements set out in Section 512, including: the subscriber's name, address, phone number, and physical or electronic signature; identification of the material and its location before removal; a statement under penalty of perjury that the material was removed by mistake or misidentification; subscriber consent to local federal court jurisdiction, or if overseas, to an appropriate judicial body.

In the event a court determines that the copyright owner misrepresented the claim of copyright infringement, the copyright owner is liable for any damages that resulted to the online service provider from the improper removal of the material.[59] The online service provider must also appropriately respond to "repeat infringers", including termination of online accounts. On this basis online service providers may insert clauses into user service agreements which permit them to terminate or disable user accounts following repeat infringement of copyright. Identification of "repeat infringer" may occur through repeated notice and takedown requests, while other online service provider require a determination by a court.

A problem with the Notice and Take-Down provisions is that, under U.S. law, the ISP has a lot of incentive to comply with the initial takedown notice, and very little incentive to comply with any counter notice – or even to tell the Internet user about the takedown in the first place. This is because compliance with the initial notice from the copyright owner gives the ISP immunity against a copyright lawsuit for damages. This immunity is valuable, because ISPs that knowingly facilitate the copyright infringement of Internet users would ordinarily share the users' legal liability. Therefore, complying with a copyright owner's notice aids an ISP to avoid a real threat of liability.[60]

8. *Do You Think an International Enforcement System to Implement Decisions (e.g., Internet Banning Orders or Disqualifications) in the Area of Cyber Crime Is Possible? Why (Not)?*

An international enforcement system to implement decisions, such as Internet Banning Orders or Disqualifications in the area of cyber crime will be successful only if it is done in the context of a treaty that has substantial participation from most of the countries of the world and is implemented by an international organization that has universal or close to universal membership.

The problem at present with the Budapest Convention on Cybercrime is that, as of December 17, 2012, its participants are 35 of the Council of European members, plus Australia, Japan, and the U.S. Major countries that are alleged sources or intermediaries of cybercrime, such as Russia, Canada, the Philippines, the People's Republic of China, and Indonesia are among the non-members. Properly applying international banning and qualification orders effectively requires a treaty with substantial participation and a compliance and enforcement mechanism that can adjudicate disputes. Such an agency does not exist at present.[61] For instance, on November 7, 2012, Egypt's Prosecutor General Abdel Maguid Mahmoud, ordered government ministries to enforce a ban on pornographic websites, based on a three-year old ruling by Egypt's administrative

[54] 17 U.S.C. § 512(c)(3)(A)(i-vi).
[55] 17 U.S.C. § 512(c)(1)(C).
[56] 17 U.S.C. § 512(g)(2)(A).
[57] 17 U.S.C. § 512(g)(2).
[58] 17 U.S.C. § 512(g)(2)(C).
[59] 17 U.S.C. § 512(f).
[60] Prof. James Gibson, Univ. of Richmond, *Notice and Take Down, Here and Abroad*, The Media Institute, Sept. 15, 2012 (http://www.mediainstitute.org/IPI/2011/091511.php).
[61] *See, e.g.*, Dan Robel, *International Cybercrime Treaty: Looking Beyond Ratification*, SANS Institute InfoSec Reading Room 43-44 (2007).

court, which declared that "freedom of expression and public rights should be restricted by maintaining the fundamentals of religion, morality and patriotism" and denounced pornographic content as "venomous and vile."[62] However, the problem of defining throughout the world pornographic content is very difficult.

Another difficulty is the lack of effective attribution and the multinational nature of Internet traffic. This makes it difficult to identify and prosecute cyber criminals.[63] Another element of an effective international enforcement system is the requirement of an effective governance structure for the Internet.[64] The international community has a lot of work to do to develop more effective international enforcement system to implement decisions in the area of cyber crime.

9. *Does the U.S. Allow For Direct Consultation of National or International Databases Containing Information Relevant for Criminal Investigations (Without a Request)?*

In general, the U.S. will require a request if a foreign government wants to directly consult national or international databases controlled by the U.S. government in order to obtain information for admission into court (e.g., for a criminal investigation).

If the foreign government wants the information for intelligence purposes or police-to-police, the U.S. law enforcement agencies will more easily be able to allow direct consultation of national or international databases without a formal request.

10. *Whether the U.S. Participates in Interpol/Europol/Eurojust or Any Other Supranational Office Dealing with the Exchange of Information? Under Which Conditions?*

The U.S. government actively participates in Interpol. Ronald Noble, a former high-level U.S. Department of Treasury official is now the Secretary-General of Interpol. The U.S., although not a member of the European Union, has liaisons and other cooperative arrangements with both Europol and Eurojust. In addition, the U.S. Department of Justice has for over a decade had a senior representative serve as a liaison in Brussels in order to try to strengthen U.S. cooperative ties with EU enforcement efforts, including organs, such as Europol and Eurojust.

IV. HUMAN RIGHTS CONCERNS

Electronic records such as computer network logs, email, word processing files, and image files increasingly provide the government with important and sometimes essential evidence in criminal cases. The United States Constitution, especially the right to be free from illegal searches, applies to criminal investigations using information technology. The law governing electronic evidence in criminal investigations has two primary sources: the Fourth Amendment to the U.S. Constitution, and the statutory privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27. Constitutional and statutory issues overlap sometimes, although most situations present either a constitutional issue under the Fourth Amendment or a statutory issue under these three statutes.[65]

A. Introduction

The Fourth Amendment limits the ability of government agents to search and seize evidence without a warrant. The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Supreme Court has ruled that a "seizure of property occurs when there exists some meaningful interference with an individual's possessory interests in that property."[66] The Court has characterized the interception of intangible communications as a seizure.[67] Additionally, the Court has held that a "search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[68]

---

[62] Eva Galperin, *Egyptian Prosecutor Orders a Ban on Internet Porn*, ELECTRONIC FRONTIER FOUNDATION, Nov. 7, 2012 (https://www.eff.org/deeplinks/2012/11/egyptian-prosecutor-orders-ban-internet-porn).

[63] Jeffrey Hunker, U.*S. International Policy for Cybersecurity: Five Issues That Wont' Go Away*, 4 J. OF NATIONAL SECURITY LAW & POLICY 197, 204-5 (2010).

[64] *Id.* at 199-204.

[65] This section relies heavily on U.S. Department of Justice Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Office of Legal Education Executive Office of United States Attorneys).

[66] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

[67] *See Berger v. New York*, 388 U.S. 41, 59-60 (1967).

[68] *Jacobsen*, 466 U.S. at 113.

If the government's conduct does not violate a person's "reasonable expectation of privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required.[69] Additionally, a warrantless search that violates an individual's reasonable expectation of privacy will still be constitutional if it falls within an established exception to the warrant requirement.[70] Hence, investigators must consider two issues when asking whether a government search of a computer requires a warrant. First, does the search violate a reasonable expectation of privacy? If so, is the search still permissible because it falls within an exception to the warrant requirement?

B. The Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers

1. General Principles

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy.[71] The inquiry includes two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable'."[72]

2. Reasonable Expectation of Privacy in Computers as Storage Devices

To determine whether an individual has a reasonable expectation of privacy in information stored in a computer requires treating the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally forbids law enforcement from accessing and viewing information stored in a computer if it would be forbidden from opening a closed container and examining its contents in the same situation.

The most basic Fourth Amendment issue in computer cases asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers (or other electronic storage devices) under the individual's control. For instance, do individuals have a reasonable expectation of privacy in the contents of their laptop computers, USB drives, or cell phones? If the answer is "yes", then the government ordinarily must obtain a warrant, or fall within an exception to the warrant requirement, before it accesses the information stored inside.

Courts have analogized the expectation of privacy in a computer to the expectation of privacy in closed containers, such as suitcases, footlockers, or briefcases. Since individuals generally have a reasonable expectation of privacy in the contents of closed containers,[73] they also generally retain a reasonable expectation of privacy in data held within electronic storage devices. Accordingly, accessing information stored in a computer ordinarily will implicate the owner's reasonable expectation of privacy in the information.

While courts have generally agreed that electronic storage devices can be analogized to closed containers, they have reached differing conclusions about whether a computer or other storage device should be classified as a single closed container or whether each individual file stored within a computer or storage device should be treated as a separate closed container.

While individuals generally have a reasonable expectation of privacy in computers under their control, special circumstances may eliminate that expectation. For instance, an individual does not have a reasonable expectation of privacy in information that the person has made openly available.[74]

3. Reasonable Expectation of Privacy and Third-Party Possession

Individuals with a reasonable expectation of privacy in stored electronic information under their control may lose Fourth Amendment protections when they relinquish that control to third parties. For instance, an individual may offer a container of electronic information to a third party by bringing a malfunctioning computer to a repair shop or by shipping a floppy diskette in the mail to a friend. Additionally, a user may transmit information to third parties electronically, such as by sending data across the Internet, or a user may leave information on a shared computer network. Law enforcement agents learning of information in the possession of third parties that may show evidence of a crime may want to inspect it. Whether the Fourth Amendment

[69] *See Illinois v. Andreas*, 463 U.S. 765, 771 (1983).
[70] *See Illinois v. Rodriguez*, 497 U.S. 177, 185-86 (1990).
[71] *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[72] *Id.*
[73] *See United States v. Ross*, 456 U.S. 798, 822-23 (1982).
[74] *See Katz v. United States*, 389 U.S> 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

requires them to obtain a warrant before examining the information depends in part upon whether the third-party possession has eliminated the individual's reasonable expectation of privacy.[75]

Government acquisition of an intangible electronic signal in the course of transmission may also have Fourth Amendment implications.[76] However, the lines of the application of the Fourth Amendment in these cases are not clear because Congress addressed the Fourth Amendment concerns identified in *Berger* by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522. Title III sets forth a comprehensive statutory framework that regulates real-time monitoring of wire and electronic communications. Its scope encompasses and even in some ways surpasses the protection offered by the Fourth Amendment.

Ordinarily, if an item has been received by the intended recipient, the sender's reasonable expectation of privacy in the item ends.[77] In general, the Supreme Court has held that the Fourth Amendment is not violated when information is revealed to a third party is disclosed by the third party to the government, regardless of any subjective expectation that the third parties will keep the information confidential.

While an individual normally loses a reasonable expectation of privacy in an item delivered to a recipient, an exception exists to this rule when the individual can reasonably expect to retain control over the item and its contents. When a person leaves a package with a third party for temporary safekeeping, for instance, she usually retains control of the package and hence has a reasonable expectation of privacy in its comments.

In some cases, the sender may initially have a right to control the third party's possession, but may lose that right over time. The general rule is that the sender's Fourth Amendment rights dissipate as the sender's right to control the third party's possession diminishes.

4. Private Searches

The Fourth Amendment does not apply to a search or seizure, even an unreasonable one, affected by a private individual who is not acting as an agent of the government or with the participation or knowledge of any governmental official.[78] As a result, a violation of the Fourth Amendment does not occur when a private individual acts on his own to conduct a search and makes the results available to law enforcement. According to *Jacobsen*, agents who learn of evidence through a private search can reenact the original private search without violating any reasonable expectation of privacy. However, the agents cannot, without a warrant, "exceed the scope of the private search."[79] This standard requires agents to limit their investigation to the scope of the private search when searching without a warrant after a private search has occurred. When agents exceed the scope of the private warrantless search, any evidence uncovered may be vulnerable to a motion to suppress.

Private individuals often find contraband or other incriminating evidence on computers and bring that information to law enforcement, and the private search doctrine applies in such cases. In one common scenario, an individual leaves his computer with a repair technician. The technician discovers images of child pornography on the computer, contacts law enforcement, and shows those images to law enforcement. Courts have found that such searches by repairmen prior to their contract with law enforcement are private searches and do not implicate the Fourth Amendment.

One private search issue that arises in computer cases is whether law enforcement agents must limit themselves to only files examined by the repair technician or whether all data on a particular storage device is within the scope of the initial private search. The Fifth Circuit has taken an expansive approach to this issue.[80] Under this approach means a third-party search of a single file on a computer allows a warrantless search by law enforcement of the computer's entire contents.[81] However, other courts may not follow the Fifth Circuit's approach and instead rule that government searches can view only those files whose

---

[75] Even if an individual has a reasonable expectation of privacy in an item or information held by a third party, the third party may disclose the item or information to the government provided the third party has common authority over the item or information. *See United States v. Young*, 350 F.3d 1302, 1308-09 (11th Cir. 2003).

[76] *See Berger v. New York*, 388 U.S. 41, 58-60 (1967) (applying the Fourth Amendment to a wire communication in the context of a wiretap).

[77] *See United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995) (sender's expectation of privacy in letter "terminates upon delivery").

[78] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (internal quotation marks omitted).

[79] *Id*. at 115. See *also United States v. Miller*, 152 F.3d 813, 815-16 (8th Cir. 1998); *United States v. Donnes*, 47 F.2d 1430, 1434 (10th Cir. 1991). *But see United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) (stating in dicta that *Jacobsen* does not allow law enforcement to reenact a private search of a private home of residence).

[80] *See United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001) (police did not exceed the scope of a private search when they examined more files on privately searched disks than had the private searches).

[81] *Id.*

contents were revealed in the private search.[82] Even if courts follow the more restrictive approach, the information gained from the private search will often provide the probable cause required to obtain a warrant for a further search.[83]

5. Use of Specialized Technology to Obtain Information

The government's use of innovative technology to obtain information about a target can raise Fourth Amendment issues.[84] In *Kyllo*, the Supreme Court held that the warrantless use of a thermal imager to reveal the relative amount of heat released from the various rooms of a suspect's home constituted a search that violated the Fourth Amendment. The Court held that where law enforcement "uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without a physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[85] Whether technology falls within the scope of the *Kyllo* rule depends on at least two factors. First, the use of technology should not implicate *Kyllo* if the technology is in "general public use,"[86] although courts have not defined the standard for determining whether a given technology meets this requirement. Second, the Supreme Court restricted its holding in *Kyllo* to the use of technology that reveals information about the interior of the home.[87]

V. FUTURE DEVELOPMENTS

The use of modern telecommunication to contact accused, victims, and witnesses directly over the border should be encouraged, as long as the techniques do not violate the U.S. Constitution or the Federal Rules of Criminal Procedure and the Federal Rules of Evidence.

Federal rules of civil procedure prefer a policy of open court testimony and live testimony must be taken in court. That said, courts have made allowances "for good cause in compelling circumstances and with appropriate safeguards, the court may permit testimony in open court by contemporaneous transmission from a different location" Rule 43, '2414. In *El-Hadad v. United Arab Emirates*, the district court permitted testimony via teleconference after the plaintiff proved that he had repeatedly been denied a visa to the United States.[88] A defining moment in allowing testimony via telecommunication, in lieu of live testimony, occurred in *Lopez v. NTI*, in which laborers from Honduras, who had brought FLSA action against their employer were allowed to testify through videoconferencing, after it was determined that forcing the Honduran workers, who made less than $7,000 annually, to travel to the United States would impose significant hardship on the laborers.[89] In *Adam v. Carvalho*, the courts affirmed that out-of-state witness testimony by videoconference was allowed, if the witness is sworn in and available for cross-examination.[90] Those who hope to provide testimony remotely must report sufficient cause to do so. In *Gulino v. Board of Educ. Of City School Dist. Of City of New York*, the court rejected the school board's request to allow a witness to testify via videoconference. The court explained that mere inconvenience is not sufficient to permit testimony by phone or video.[91] Increasingly federal courts have appeared to be flexible with regards to evolving technologies, especially those that may make litigation practices in the United Sates more convenient and efficient, yet there still lies a burden to demonstrate that live testimony would pose an unusual hardship on the witness in order to be granted approval for testimony through alternate means.

The provisions of Article 6 (video conferencing) of the U.S.-EU MLAT requires the contracting parties to take such measure as may be required to enable the use of video transmission technology, between each EU Member and the U.S, for taking testimony in a proceeding for which mutual legal assistance is available of a witness or expert located in a requested state, to the extent such assistance is not currently available.[92]

The current prosecution of Megaupload, the digital locker, with transnational organized crime violations, may presage the U.S. approach to future cybercrime prosecutions with transnational elements. On January 19, 2012, the U.S. Department of Justice

---

[82] *See United States v. Barth*, 26 F.Supp. 2d 929, 937 (E.D. Tex 1998) (holding, in a pre-*Runyan* case, that agents who viewed more files than private searcher exceeded the scope of the private search).

[83] After they view evidence of a crime stored on a computer, agents may need to seize the computer temporarily to ensure the integrity and availability of the evidence before they can obtain a warrant to search the contents of the computer. *See, e.g.,United States v. Hall*, 142 F.3d 988, 994-95; *United States v. Grosenheider*, 200 F.3d 321, 330 n. 10 (5th Cir. 2000).

[84] *See Kyllo v. United States*, 533 U.S. 27 (2001).

[85] *Id.* at 40.

[86] *See id*. at 34, 39 n.6.

[87] *See id*. at 40.

[88] *El-Hadad v. United Arab Emirates*, C.A.D.C, 2007, 496 F.3d 658.

[89] *Lopez v. NTI, LLC*, 748 F.Supp.2d 471 (D.Md.2010).

[90] *Adam v. Carvalho,* C.A. 9th, 2005, 138 Fed.Appx.7.

[91] *Gulin v. Board of Educ. Of City School Dist. Of City of New York*, 2002 WL 32068971 (D.C.N.Y.2003) (Second Circuit Rule '0.23) .

[92] Agreement on Mutual Legal Assistance Between the European Union and the United States of America, signed June 25, 2003, entered into force, Feb. 1, 2010.

(DOJ) announced an indictment charging seven individuals and two corporations with operating an international organized criminal enterprise allegedly responsible for enormous worldwide online piracy of various types of copyrighted works, through Megaupload.com and other related sites.[93] The DOJ alleges that the enterprise generated more than $175 million in criminal proceeds and caused more than half a billion dollars in harm to copyright owners.

The DOJ characterized the action as among the largest criminal copyright cases ever brought by the U.S. and directly targets the misuse of a public content storage and distribution site to commit and facilitate intellectual property crime.

The grand jury indictment, returned on January 5, 2012, charges the individuals and two corporations - Megaupload Limited and Vestor Limited - with engaging in a racketeering conspiracy, conspiring to commit copyright infringement, conspiring to commit money laundering, and two substantive counts of criminal copyright infringement.

According to the indictment, Kim Dotcom, aka Kim Schmitz, and Kim Tim Jim Vestor, a resident of both Hong Kong and New Zealand, head the criminal enterprise. Dotcom founded Megaupload Limited and is the director and sole shareholder of Vestor Limited, which has been used to hold his ownership interests in the Mega-affiliated sites. Also charged are: Finn Batato, 38, a citizen and resident of Germany, who is the chief marketing officer; Julius Bencko, 35, a citizen and resident of Slovakia, who is the graphic designer; Sven Echternach, 39, a citizen and resident of Germany, who is the head of business development; Mathias Ortmann, 40, a citizen of Germany and resident of both Germany and Hong Kong, who is the chief technical officer, co-founder, and director; Andrus Nomm, 32, a citizen of Estonia and resident of both Turkey and Estonia, who is a software programmer and head of the development software division; and Bram van der Kolk, aka Barmos, a Dutch citizen and resident of both the Netherlands and New Zealand, who oversees programming and the underlying network structure for the Mega conspiracy websites.

Law enforcement authorities arrested Dotcom, Batato, Ortmann, and van der Kolk in Auckland, New Zealand. The other three individual defendants remain at large.

Law enforcement authorities executed more than 20 search warrants in the U.S. and eight countries, seized approximately $50 million in assets, and targeted sites where Megaupload has servers in Ashburn, Virginia; Washington, D.C.; the Netherlands; and Canada. Additionally, the U.S. District Court in Alexandria, Virginia, ordered the seizure of 18 domain names associated with the alleged Mega conspiracy.

The indictment alleges that for more than five years the conspiracy has operated websites that unlawfully reproduce and distribute infringing copies of copyrighted works, including movies - often before their theatrical release - music, television programs, electronic books, and business and entertainment software on a massive scale. Megaupload is advertised as having more than one billion visits to the site, more than 150 million registered users, 50 million daily visitors and accounting for four percent of the total traffic on the Internet. The estimated harm caused by the conspiracy's criminal conduct to copyright holders is well in excess of $500 million. The conspirators allegedly earned more than $175 million in illegal profits through advertising revenue and selling premium memberships.

According to the indictment, the conspirators conducted their illegal operation using a business model expressly designed to promote uploading of the most popular copyrighted works for many millions of users to download. The indictment alleges that the site was structured to discourage the vast majority of its users from using Megaupload for long-term or personal storage by automatically deleting content that was not regularly downloaded. The conspirators also allegedly had a rewards program that would provide users with financial incentives to upload popular content and drive web traffic to the site, often through user-generated websites known as linking sites. The conspirators allegedly paid users whom they specifically knew uploaded infringing content and publicized their links to users throughout the world.

By actively supporting the use of third-party linking sites to publicize infringing content, the conspirators did not have to publicize such content on the Megaupload site. Rather, the indictment alleges that the conspirators manipulated the perception of content available on their servers by not providing a public search function on the Megaupload site and by not including popular infringing content on the publicly available lists of top content downloaded by its users.

The indictment alleges that the conspirators failed to terminate accounts of users with known copyright infringement, selectively complied with their obligations to remove copyrighted materials from their servers and deliberately misrepresented to copyright holders that they had removed infringing content. For instance, when notified by a rights holder that a file contained infringing content, the indictment alleges that the conspirators would disable only a single link to the file, deliberately and deceptively

[93] This discussion of the Megaulpload prosecution is excerpted from Bruce Zagaris, U*.S. Charges Megaupload, a Digital Locker, with Organized Copyright Crime*, 28 INT'L ENFORCEMENT L. REP. 82-85 (Mar. 2012).

leaving the infringing content in place to make it seamlessly available to millions of users to access through any one of the many duplicate links available for that file.

According to the indictment the defendants conspired to launder money by paying users through the sites' uploader reward program and paying companies to host the infringing content.

The likely defense that will be raised is that the defendants did not charge people for downloading copyrighted content. Instead, they merely served as a "cyberlocker," providing their users with storage space for electronic content. Megaupload contends that their premium members are merely allowed access to more online space and faster and more reliable download and upload connections. The defense is supported by the fact that an individual cannot search for copyrighted content directly on the website. Instead, the customer can only find content stored on the website through third party websites and search engines that are not operated by members of the alleged conspiracy. Additionally, members of the alleged conspiracy have said that they comply with federal laws requiring the removal of copyrighted content after notice is given.

On January 20, 2012, Meagupload's lawyer Ira Rothken said Megaupload is trying to recover its servers and get back online. Rothken said no decision has been made as to whether the four detained defendants would fight extradition. On January 19, 2012, Rothken said "Megaupload believes the government is wrong on the facts, wrong on the law."

In response to the arrests and the seizure of Megaupload, the hacker collective that calls itself Anonymous attacked the Web sites of the DOJ and several major entertainment companies and trade groups.

The case involves many of the most controversial issues of the anti-piracy debate. Megaupload and similar sites, like RapidShare and MediaFire, are promoted as convenient means to transfer large files legitimately. However, media companies say the legitimate uses conceal extensive theft.

The practice of providing digital "lockers" so people can store and share their photos, movies, and songs is very common. Sites such as Facebook, Dropbox, YouTube, and YouSendIt can be used to swap both legitimate and pirated content. However, the DOJ alleges Megaupload took the practice to a new level of criminality.

After the indictment, some Megaupload users complained on Twitter that they had used Megaupload to back up personal files, to share files with clients, and as a collaboration tools.

The indictment occurred during a contest in the U.S. Congress over antipiracy legislation. The technology industry is concerned about the provisions of the Stop Online Piracy Act (SOPA), permitting the DOJ to rapidly close any site that had even a small amount of unauthorized copyrighted material on it. Supporters of the legislation say it was directed only at foreign sites that were primarily about piracy.

Dotcom has a criminal record, including a conviction for breaking into Pentagon computers, resulting in spending three months in a Munich jail in 1994, followed by two year probation. In the mid-1990s, Dotcom was sentenced to a suspended two-year sentence for a swindle using stolen phone card numbers. In 2001, Dotcom was accused in the largest insider-trading case in Germany. He fled to Thailand, but was extradited to Germany and convicted in 2002. He spent five months in pre-trial detention and received a suspended sentence.

The U.S. prosecution is awaiting U.S. efforts to secure effective international enforcement cooperation. The U.S. effort to extradite Mr. Dotcom from New Zealand has become bogged down in a series of controversies.[94]

On September 24, 2012, New Zealand Prime Minister John Key announced that his government is investigating allegations that its Government Communications Security Bureau (GCSB) acted unlawfully in connection with the U.S. prosecution and extradition request for Kim Dotcom. Key expressed his "disappointment that unlawful acts had taken place."

The GCSB illegally bugged Dotcom and an associate, van der Kolk, before their arrest, after police mistakenly told the GCSB they were foreigners, not residents. New Zealand law makes it unlawful for the GCSB to gather intelligence on New Zealand nationals and residents and can only monitor foreign intelligence. Since December 2010, Dotcom has held New Zealand residency.

On September 26, 2012, a New Zealand court in Auckland held a hearing on the search warrants used in the raid on his premises that have been ruled illegal.

[94] This discussion of the international enforcement cooperation controversies is excerpted from Bruce Zagaris, *U.S. Extradition for Dotcom in New Zealand Caught in Controversies*, 28 INT'L ENFORCEMENT L. REP. 450-51 (Dec. 2012).

Judge David Harvey, who initially presided over the extradition, withdrew from the case after he making comments in a speech at a conference, suggesting the U.S. was the "enemy." Since he was an Internet law expert, Judge Harvey initially was considered the perfect choice to preside over the case.

Another problem was that initially, the New Zealand law enforcement obtained the wrong type of restraining order to seize the cash and assets of Dotcom. Thereafter, the court ruled the warrants invalid because they were too broad, making the search and seizure illegal. Yet another problem is that the FBI had taken evidence to the U.S. without the knowledge of the police and the government, and now wants to use it to help extradite Dotcom.

The U.S. has indicted Doctom and others on charges of racketeering, copyright infringement and money laundering in the operation of Megaupload, a cloud storage service that the U.S. Department of Justice took down in January for copyright infringement.

On August 16, 2012, a New Zealand judge upheld a ruling that permits Dotcom to review details of the U.S. case against him ahead of an extradition hearing. While Dotcom requested to examine documents supporting the charges, U.S. prosecutors argued discovery should be narrowly limited. Judge Helen Winklemann ruled that disclosing the documents would help encourage a fair hearing.

Normally, courts do not allow much discovery during an extradition case. However, the charges against the defendants are complex and raise novel issues. In addition, the series of illegalities and the high profile nature of the case make the case quite unique. Because of the number of illegal acts by both governments, the court could exclude evidence or otherwise take action against law enforcement authorities in the extradition proceeding.

The Megaupload prosecution exemplifies many of the conceptual, technical, and legal issues that arise in the efforts to prosecute cybercrime cases with large transnational elements in them. Some of the issues reflect the difficulty that law has in keeping pace with technology, especially internationally, as well as the difficulty of governments keeping pace with entrepreneurs who successfully conceptualize and operate high-tech businesses transnationally, especially because in today's world transnational high-tech business offers a fast lane to success and power. Similar battles are occurring in the Internet game industry in the U.S. and elsewhere.

A towering issue is the lack of a universal international organization over the Internet or a number of areas, such as Internet gaming. Until now, the International Telecommunications Union (ITU) has tried unsuccessfully to develop the architecture and governance of the Internet.[95] Without the proper institutional enforcement architecture, governments, even the superpower, struggle to effectively make, implement, and enforce cybercrime policies and laws.

[95] For background on the ITU, *see* http://www.ihs.com/products/industry-standards/organizations/itu/index.aspx; Charlyn Stanberrys, *Global Regulation of Telecommunications a Good or Bad Idea*?, Politics365, http://politic365.com/2013/01/07/is-global-regulation-of-telecommunications-a-good-or-bad-idea-introducing-the-international-telecommunications-union, accessed Jan. 7, 2012.