Washington and Lee Law Review

Volume 59 | Issue 4

Article 13

Fall 9-1-2002

Script Kiddies Beware: The Long Arm of U.S. Jurisdiction to Prescribe

John Eisinger

Script Kiddies Beware: The Long Arm of U.S. Jurisdiction to Prescribe

John Eisinger*

Table of Contents

[*] Candidate for Juris Doctor, May 2003, Washington and Lee University School of Law. The author wishes to thank his parents and sister for their never-ending support and encouragement, Rebecca Miles for her editorial assistance, and Professor Frederic Kirgis for his advice and guidance.

I. Introduction

On Friday, March 26, 1999, a computer virus shut down computer networks across the United States and around the world.[1] The virus, dubbed "W97M.Melissa.A" by the anti-virus industry and "Melissa" by the media, came in the form of an E-mail attachment written in Visual Basic Script (VBS).[2] When opened, the virus executed a string of commands and E-mailed itself to the first 50 people in the user's Microsoft Outlook address book.[3] The virus set off a chain reaction that flooded the E-mail systems of many large companies and forced them to shut down their Internet gateways and mail systems.[4] Not since university student Robert Morris released the "Internet Worm" in 1988[5] had the Internet been so paralyzed by a program gone awry.[6] Within a week, nearly two dozen copycat versions of Melissa infected computers on the Internet.[7]

On Thursday, May 4, 2000, a computer virus shut down computer networks across the United States and around the world.[8] The virus, dubbed "VBS.Love Letter" by the anti-virus industry and the "iloveyou" virus by the

[1] *See* David Kocieniewski, *Man Is Charged in the Creation of E-Mail Virus*, N.Y. TIMES, Apr. 3, 1999, at A1 (mentioning huge volume of E-mail that forced many firms to shut down computer networks).

[2] *See* Raul K. Elnitiarta, *Security Update: W97M.Melissa.A*, *at* http://securityresponse.ymantec.com/avcenter/venc/data/mailissa.html (March 29, 1999) (documenting technical description of Melissa virus).

[3] *See id.* (explaining how Melissa propagated).

[4] *See* Kocieniewski, *supra* note 1, at A1 (explaining that "[b]y replicating and sending itself so rapidly, the virus clogged and in some cases incapacitated computer networks at about 300 corporations"); Chris Taylor, *How They Caught Him: Tracking the Hacker Who Hatched the Melissa Virus*, TIME, Apr. 12, 1999, at 66 (stating that Melissa virus "caus[ed] shutdowns in more than 300 computer networks").

[5] *See* CLIFF STOLL, THE CUCKOO'S EGG 335-47 (1989) (detailing how worm spread and how it affected computers).

[6] *See* Steven Levy, *Biting Back at the Wily Melissa*, NEWSWEEK, Apr. 12, 1999, at 62 (stating that "[n]ot since the Internet Worm of 1988 has a virus writer been pursued with such fury").

[7] *See* Taylor, *supra* note 4, at 66 (stating that Melissa's "freely available source code soon spawned copycat viruses"); *see also* Elnitiarta, *supra* note 2 (listing several variants which showed up within days of Melissa's release).

[8] *See* Mark Landler, *A Filipino Linked to 'Love Bug' Talks About His License to Hack*, N.Y. TIMES, Oct. 21, 2000, at C1 (explaining effects of iloveyou on computer systems around world).

media, typically came in the form of an E-mail attachment written in VBS.[9] When opened, the virus executed a string of commands that deleted files, infected Internet Relay Chat (IRC), attempted to steal passwords, and E-mailed a copy of the virus to everyone in the user's Microsoft Outlook address book.[10] The virus set off a chain reaction that flooded the E-mail systems of many large companies and forced them to shut down their Internet gateways and mail systems.[11] Within a year, over eighty variants of the iloveyou virus existed.[12]

Although these two virus outbreaks seem quite similar, the legal consequences for the two men who authored and distributed the viruses were very different.[13] Authorities arrested New Jersey resident David Smith, the creator and distributor of Melissa, within a week of Melissa's release and charged him with interruption of public communications, conspiracy, theft of computer service, and wrongful access to computer systems.[14] He faced forty years in prison and $480,000 in fines.[15] Smith pleaded guilty to a violation of the computer fraud statute and admitted causing damages in excess of $80 million.[16]

The Philippine government could not directly charge Manila, Philippines resident Onel de Guzman for his role in creating and distributing the iloveyou virus because the Philippines criminal code did not prohibit computer crimes.[17] Instead, the government charged de Guzman with the traditional

[9] *See* Eric Chien & Brian Ewell, *Security Response: VBS.Love Letter and Variants, at* http://securityresponse.symantec.com/avcenter/venc/data/vbs.loveletter.a.html (last modified May 31, 2001) (documenting technical description of iloveyou virus).

[10] *See id.* (detailing properties of iloveyou virus).

[11] *See* Landler, *supra* note 8, at C1 (claiming iloveyou "paralyzed computers from the Pentagon to the British Parliament" as it moved from Asia to United States and Europe).

[12] *See* Chien & Ewell, *supra* note 9 (listing eighty-two variants of iloveyou virus discovered as of May 2001).

[13] *See infra* notes 14-19 and accompanying text (explaining that distributor of Melissa faced computer crime charges in United States, but distributor of iloveyou did not).

[14] *See* Matt Ackermann, *Prosecuting 'Melissa': Catching David Smith Was the Easy Part. Now What Do Cyberlaw Enforcers Do with Him?* 156 N.J.L.J. 89 (1999) (detailing charges against Smith).

[15] *See id.* (explaining that "Smith could face as much as 40 years in prison and a $480,000 fine if convicted on all charges"). Three years after releasing Melissa, the court sentenced Smith to twenty months in prison, one hundred hours of community service, three years of supervised release, and a $5,000 fine. John Soat, *IT Confidential*, INFO. WEEK, May 6, 2002, at 120.

[16] *See* Robert Moskowitz, *Crime and Punishment*, NETWORK COMPUTING, Feb. 7, 2000, at 37 (stating that "[o]n December 9, 1999, David Smith pleaded guilty to causing more than $80 million worth of damage when he released his Melissa virus on the Internet").

[17] *See* Landler, *supra* note 8, at C1 (stating that "[t]he case against [de Guzman] was

crimes of theft and credit card fraud in connection with the virus.[18] However, in August 2000, the Philippine government dropped all charges due to a lack of evidence of a non-computer crime.[19] The virus caused worldwide damages estimated at $10 billion.[20]

The primary federal computer crime statute, the Computer Abuse Amendments Act of 1994[21] (1994 Act), makes it illegal to damage data on a computer,[22] defraud others,[23] or steal information electronically.[24] However, Smith's virus did very little real damage to files; Melissa only infected documents and occasionally added some text to infected documents.[25] In addition, the Melissa virus did not attempt to defraud people or steal information.[26] Moreover, Smith attempted to limit the spread of Melissa by only sending E-mail to "the first 50 entries out of the address books . . . [and by] only running once per system boot."[27]

Unlike Smith, de Guzman intentionally caused damage and destroyed files.[28] He used his virus in an attempt to defraud people and steal passwords.[29] While Smith evinced surprise at the rapid spread of Melissa,[30] de Guzman used

weakened because at the time, the Philippines did not have laws governing computer espionage").

[18] *See id.* (commenting that "[t]he Philippine authorities filed theft and other charges against Mr. [d]e Guzman").

[19] *See id.* (explaining that Philippine authorities "dropped [the charges] in August because of insufficient evidence").

[20] *See id.* (stating that iloveyou virus caused "an estimated $10 billion in damage").

[21] 18 U.S.C. § 1030 (1994).

[22] *See id.* § 1030(a)(5), (7) (barring unauthorized access that results in damage).

[23] *See id.* § 1030(a)(4), (6) (prohibiting computer fraud).

[24] *See id.* § 1030(a)(1), (2) (criminalizing theft of information).

[25] *See* Elnitiarta, *supra* note 2 (stating that Melissa added text to infected document if user opened document "at the number of minutes past the hour corresponding to the date (*i.e.*, on the 16th of the month, the payload triggers at 16 minutes after every hour)").

[26] *See id.* (explaining process by which Melissa attempted to replicate itself, but making no mention of fraud or theft).

[27] Moskowitz, *supra* note 16, at 37.

[28] *See* Chien & Ewell, *supra* note 9 (stating that iloveyou overwrote some two dozen file formats, including music and image files, and replaced them with virus).

[29] *See id.* (detailing actions of iloveyou, which include trying to "download a password-stealing Trojan horse program from a Web site"); *Computer Virus Charges Sought*, N.Y. TIMES, Sept. 6, 2000, at C5 (claiming that iloveyou stole passwords and sent them to E-mail addresses in Philippines); Landler, *supra* note 8, at C1 (explaining that de Guzman's college thesis described "method for stealing passwords to gain free access to the Internet" and that he possibly released iloveyou to prove thesis).

[30] *See* Moskowitz, *supra* note 16, at 37 (noting Smith's attempts to limit spread of virus and his claim that he did not intend rapid distribution of virus).

the same method for spreading his virus and therefore cannot claim ignorance of the potential worldwide distribution of iloveyou.[31]

Why did Smith face forty years in prison while de Guzman was not even charged with a crime in the United States? It appears that de Guzman went out of his way to create a virus that could rapidly propagate itself around the world and that would damage, defraud, and steal.[32] Why did de Guzman get away without charges in the United States, whereas Smith was charged and convicted for a much less damaging virus? The answer to this question lies in international law concepts that restrict the jurisdiction of states based on the nationality and residence of the person who commits the crime.[33]

This Note examines how the United States can use its jurisdiction to prescribe laws in order to prohibit foreign nationals from releasing viruses that affect domestic computers, even if their actions occur on foreign soil. Part II of this Note outlines the basic tenets of international law, including the sources from which international law derives.[34] Part III discusses various methods by which the United States can exert jurisdiction to prescribe its laws extraterritorially.[35] Those methods include the effects principle,[36] the protective principle,[37] passive personality,[38] and universal jurisdiction.[39] Part IV examines the reasonableness of exerting jurisdiction in computer virus cases[40] and whether or not Congress meant the 1994 Act to apply extraterritorially.[41]

[31] *Compare* Chien & Ewell, *supra* note 9 (explaining that iloveyou sends E-mail to everyone in user's address book, infects files on servers that others access, and also replicates using Internet Relay Chat) *with* Elnitiarta, *supra* note 2 (showing that thirteen months before iloveyou, Melissa spread rapidly by sending to only first fifty users in address book).

[32] *See supra* notes 28-31 and accompanying text (detailing destructive nature of iloveyou virus).

[33] *See infra* notes 70-74 and accompanying text (explaining nationality and territoriality principles).

[34] *See infra* Part II (outlining sources of international law).

[35] *See infra* Part III (noting bases of jurisdiction to prescribe).

[36] *See infra* Part III.A (explaining how effects principle allows states to prescribe laws extraterritorially).

[37] *See infra* Part III.B (detailing state's right to protect state interests from harm).

[38] *See infra* Part III.C (describing state's right to protect its citizens from being targeted based on their nationality).

[39] *See infra* Part III.D (explaining how certain universally condemned crimes create jurisdiction in every state).

[40] *See infra* Part IV.A (justifying United States exercise of jurisdiction in computer virus cases under international comity).

[41] *See infra* Part IV.B (arguing that Congress intended 18 U.S.C. § 1030 (1994) to operate extraterritorially).

This Note concludes that the effects principle allows the United States to prescribe laws against releasing viruses that substantially affect U.S. computers.[42] Furthermore, the protective principle is applicable in cases in which a computer virus specifically targets the U.S. government.[43] However, because passive personality is not as well recognized, it may provide additional justification for jurisdiction, but rarely would justify jurisdiction by itself.[44] Although universal jurisdiction enjoys wide acceptance, it does not cover computer viruses and therefore is not applicable.[45] In addition to having jurisdiction, it is reasonable for the United States to exert its jurisdiction in cases in which a virus substantially affects the United States or targets the United States government, and in which the country of the virus's origin is unable to prosecute.[46] Finally, this Note concludes that Congress intended the 1994 Act to apply extraterritorially.[47]

II. General Principles of International Law

Under international law, a state must have the jurisdiction to prescribe, adjudicate, and enforce its laws before convicting a person of a criminal offense.[48] This Note examines only the jurisdiction to prescribe, which many scholars refer to as the jurisdiction to legislate.[49] It is important to understand the implications of the jurisdiction to prescribe because this principle allows the United States to prescribe laws prohibiting the activities of the perpetrator,[50] but it does not assist the United States in bringing the perpetra-

[42] *See infra* notes 141-49 and accompanying text (explaining how effects principle applies to computer viruses).

[43] *See infra* text accompanying notes 184-94 (noting how computer viruses can invoke protective principle).

[44] *See infra* notes 220-34 and accompanying text (maintaining that passive personality is not well suited for computer viruses).

[45] *See infra* notes 257-60 and accompanying text (concluding that computer viruses do not implicate peremptory norms and thus do not justify universal jurisdiction).

[46] *See infra* notes 307-09 and accompanying text (determining that extraterritorial jurisdiction does not offend international comity in computer virus cases).

[47] *See infra* notes 330-31 and accompanying text (arguing that Congress intended 18 U.S.C. § 1030 (1994) to apply extraterritorially).

[48] *See* Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. TECH. L. REV. 69, 71 (1998) (explaining different types of jurisdiction in international law).

[49] *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 298 (4th ed. 1990) (noting that prescriptive or legislative jurisdiction describes state's authority to make rules and decisions).

[50] *See* 1 SIR ROBERT JENNINGS & SIR ARTHUR WATTS, OPPENHEIM'S INTERNATIONAL LAW 456 (9th ed. 1992) (stating that legislative jurisdiction regulates conduct).

tor into a U.S. court.[51] If the perpetrator's activities occur in another state, the United States will need to convince that state to extradite the perpetrator, or the United States will have to lure or abduct the perpetrator.[52] However, if the United States does not have an internationally recognized basis for jurisdiction, other states will be unwilling to support extradition or a trial in the United States.[53]

International law primarily consists of the practices and opinions of states as evidenced by treaties and custom.[54] Treaties include everything from agreements between two states to conventions with over one hundred signatory nations.[55] Custom is a combination of widespread state practice over time and *opinio juris*.[56] Because no treaty specifies which particular bases of jurisdiction are available to states, this Note deals primarily with customary international law.[57]

Custom requires consistent, widespread state practice over time.[58] Evidence of widespread state practice includes treaties, statutes, court decisions, statements of state representatives, and treatises.[59] However, the amount of weight given to each source depends on the type and scope of the custom.[60]

[51] *See id.* at 463 (requiring physical presence of defendant in order to prosecute).

[52] *See generally* BROWNLIE, *supra* note 49 (noting need to bring accused before tribunal in order to exert adjudicative jurisdiction).

[53] *Cf. infra* note 136 and accompanying text (noting that extradition proceedings in United Kingdom verify foreign state's jurisdiction before allowing extradition).

[54] *See* Statute of the International Court of Justice, June 26, 1945, art. 38 (1), 59 Stat. 1055 (listing sources of international law applied by International Court of Justice, including international conventions, custom, general principles of law, and legal treatises). "Article 38 is generally regarded as a complete statement of the sources of international law." BROWNLIE, *supra* note 49, at 3. Of the four sources, "custom and treaties . . . are the principal and regular sources of international law." JENNINGS & WATTS, *supra* note 50, at 24.

[55] *See* JENNINGS & WATTS, *supra* note 50, at 32 (noting that "all treaties, whether bilateral or multilateral," provide evidence of international law).

[56] *See* BROWNLIE, *supra* note 49, at 5-7 (detailing elements of custom); *infra* note 62 and accompanying text (explaining *opinio juris*).

[57] Treaties are agreements between states or groups of states. *See generally* JENNINGS & WATTS, *supra* note 50, at 32 (discussing international treaties). International law dictates that states that freely consent to be bound by a treaty must live up to their agreement. *See id.* (noting binding nature of treaties). These agreements are the international form of a domestic contract that binds states to each other. *See id.* at 1224 (explaining that treaties are contracts). Normally, a treaty does not bind states that are not parties to the treaty. *See* BROWNLIE, *supra* note 49, at 12 (discussing binding effect of treaties).

[58] *See* BROWNLIE, *supra* note 49, at 5 (explaining elements of international custom).

[59] *See id.* (listing sources of custom).

[60] *See id.* (noting that "the value of these sources varies and much depends on the circumstances").

This Note relies primarily on court decisions, although it also references statutes and treaties.

In addition to widespread state practice, custom requires *opinio juris*.[61] *Opinio juris* is the concept that states act in a way that suggests that they believe themselves to be bound by a customary rule.[62] If a U.S. court rules against the interests of the United States and cites customary international law, the decision is strongly indicative of *opinio juris*.[63] While custom requires a finding of *opinio juris*, the International Court of Justice frequently assumes *opinio juris* when evidence of general practice is present.[64]

A final source of international law is *jus cogens*, or peremptory norms, which override both treaties and custom.[65] Peremptory norms are universally accepted principles that are so central to the functioning of civilized states that countries cannot opt out of them.[66] For example, there is a peremptory norm against slavery,[67] thus evidence of thousands of years of slavery and treaties that support slavery do not allow a state to practice slavery.[68] This Note addresses peremptory norms in subpart III.D, which deals with universal jurisdiction.[69]

III. Jurisdiction to Prescribe

Several different principles under international law allow a state to prescribe laws.[70] The most widely used principles are territoriality[71] and

[61] See *id.* at 7 (noting use of *opinio juris* in determining custom).

[62] *See id.* (explaining concept of *opinio juris*).

[63] It is normally in the best interests of a court to rule in a manner that supports the sovereign that gives the court power. *See* JENNINGS & WATTS, *supra* note 50, at 457 (noting that "courts naturally tend to see the problems which arise primarily from the point of view of the interests of their own state"). Therefore, if a court rules against its sovereign, then the ruling is persuasive evidence that the state believes that it is bound by a customary rule.

[64] *See* BROWNLIE, *supra* note 49, at 7 (discussing approach of International Court of Justice toward custom).

[65] *See id.* at 513 (stating that *jus cogens* "are rules of customary international law which cannot be set aside by treaty or acquiescence").

[66] *See* JENNINGS & WATTS, *supra* note 50, at 7-8 (defining scope of peremptory norms).

[67] *See id.* at 8 (noting that peremptory norm prohibits slavery).

[68] *See supra* note 65 (maintaining that custom and treaties cannot trump peremptory norms).

[69] *See infra* Part III.D (explaining relationship between peremptory norms and universal jurisdiction).

[70] *See infra* notes 71-72, 79-82 and accompanying text (listing different forms of jurisdiction).

[71] *See* JENNINGS & WATTS, *supra* note 50, at 458 (stating that "[t]erritoriality is the primary basis for jurisdiction").

nationality.[72] The principle of territoriality, or more specifically subjective territoriality, grants a state the jurisdiction to prescribe laws that regulate the conduct of persons whose acts occur within that state.[73] The principle of nationality allows a state to prescribe laws that regulate the conduct of the state's citizens regardless of where their actions occur.[74] However, as evidenced by the iloveyou virus, the Internet enables foreign nationals to commit acts in foreign countries that affect computers in the United States in contravention of U.S. laws.[75] Neither the principle of subjective territoriality nor the principle of nationality permitted the United States to exert jurisdiction over Onel de Guzman because he was a citizen of the Philippines[76] and his actions occurred in the Philippines.[77]

However, international law provides several other principles on which a country may base the jurisdiction to prescribe.[78] These principles include the effects principle,[79] the protective principle,[80] passive personality,[81] and universal jurisdiction.[82] This Part examines these principles of extraterritorial

[72] *See id.* at 462-63 (noting divergent views on use of nationality principle).

[73] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1)(a) (1987) (asserting that "a state has jurisdiction to prescribe law with respect to conduct that, wholly or in substantial part, takes place within its territory").

[74] *See id.* at § 402(2)(a) (stating that "a state has jurisdiction to prescribe law with respect to the activities, interests, status, or relations of its nationals outside as well as within its territory").

[75] *See supra* notes 8-12, 20, and accompanying text (outlining damage iloveyou virus caused worldwide).

[76] *See* Landler, *supra* note 8, at C1 (stating that de Guzman is Filipino).

[77] *See id.* (identifying source of virus as Manila, Philippines).

[78] *See infra* notes 79-82 and accompanying text (listing other bases of jurisdiction to prescribe).

[79] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1)(c) (1987) (stating that "a state has jurisdiction to prescribe law with respect to conduct outside its territory that has or is intended to have substantial effect within its territory").

[80] *See id.* § 402(3) (asserting that "a state has jurisdiction to prescribe law with respect to certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests").

[81] *See id.* § 402 cmt. g ("The passive personality principle asserts that a state may apply law – particularly criminal law – to an act committed outside its territory by a person not its national where the victim of the act was its national. The principle has not been generally accepted for ordinary torts or crimes, but it is increasingly accepted as applied to terrorist and other organized attacks on a state's nationals by reason of their nationality.").

[82] *See id.* at § 404 (stating that "a state has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern").

jurisdiction and analyzes how a country can use them to criminalize the actions of foreign virus distributors.[83]

A. The Effects Principle

Many scholars consider the effects principle, which is often referred to as objective territoriality,[84] to be a subset of territoriality.[85] The effects principle allows a state to "prescribe law with respect to conduct outside its territory that has or is intended to have substantial effect within its territory."[86] The classic illustration of this principle is a case in which someone in France shoots someone on the German side of the Franco-German border.[87] Germany can exert jurisdiction in this case because there was a substantial effect in Germany, even though the act took place in France.[88]

1. Legitimacy of the Effects Principle

S.S. Lotus[89] is one of the earliest cases to use the effects principle.[90] In *S.S. Lotus*, the Permanent Court of International Justice (PCIJ) addressed a collision between the French ship *Lotus* and the Turkish vessel *Boz-Kourt*.[91]

[83] *See infra* Parts III.A-C (explaining how effects principle, protective principle and passive personality can aid state in exerting jurisdiction over computer offenses).

[84] *See* Sanjay S. Mody, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365, 375 (2001) (referring to effects principle as objective territoriality).

[85] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 cmt. d (1987) (explaining that effects principle "is an aspect of jurisdiction based on territoriality, although it is sometimes viewed as a distinct category").

[86] *Id.* § 402(1)(c).

[87] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9, at 37 (Sept. 7, 1927) (Loder, J., dissenting).

[88] *See id.* (Loder, J., dissenting) (noting that act and consequences are indistinguishable and that direct relationship justifies applying legal fiction).

[89] (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9 (Sept. 7, 1927).

[90] *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9, at 30-32 (Sept. 7, 1927) (holding that Turkish trial of French citizen for actions committed on French territory did not conflict with international law because effects of action were felt in Turkish territory). In *S.S. Lotus*, the PCIJ reviewed the claims of France and Turkey concerning Turkey's right to exert jurisdiction over a French officer (Lieutenant Demons) who committed negligent acts aboard a French ship. *Id.* at 10-11. The Court determined that the effect of the French officer's negligence aboard the *Lotus*, which the Turkish court found and France did not dispute, resulted in the collision with, and sinking of, the Turkish vessel *Boz-Kourt*, and the subsequent death of eight Turkish nationals. *Id.* at 30-32. The PCIJ concluded that no principle of international law precluded Turkey from instituting criminal proceedings. *Id.* at 31.

[91] *See id.* at 10 (detailing collision between *Lotus* and *Boz-Kourt*).

As a result of the collision, the *Boz-Kourt* sank and eight Turkish nationals drowned.[92] When the *Lotus* arrived in Constantinople, Turkish authorities arrested the captain of the Turkish vessel, Hassan Bey, and the French officer of the watch at the time of the collision, Lieutenant Demons.[93] The prosecutor charged both men with manslaughter.[94] Lieutenant Demons objected to his detention and trial on the ground that Turkey lacked jurisdiction.[95] Both France and Turkey agreed that under international law ships are floating pieces of territory of the country under whose flag they sail.[96]

The PCIJ found that Turkey had jurisdiction to prescribe and enforce its laws on a French citizen whose actions occurred on French territory because the effect of his actions was felt on Turkish territory.[97] In addition, J.B. Moore, the American judge, agreed with all of the majority's conclusions on the use of the effects principle in this case, but dissented because he thought that the Turkish law in question violated international law in other respects.[98] However, Judge Loder's dissent characterized the majority's decision as expanding the scope of the established effects principle from cases involving intentional harm to cases involving only negligence.[99] Thus, Judge Loder implied that if the *Lotus* intentionally rammed the *Boz-Kourt*, Turkey would have jurisdiction, but he thought that the Court should not extend this principle to negligent acts.[100] While the official vote was six to six with the President

[92] *Id.*

[93] *See id.* at 10-11 (detailing facts of case).

[94] *See id.* at 11 (explaining charges against officers).

[95] *See id.* (detailing Lieutenant Demons's objections to his arrest).

[96] *See id.* at 25 (stating that "a ship on the high seas is assimilated to the territory of the state the flag of which it flies").

[97] *See id.* at 30-31 (explaining that Lieutenant Demons's actions aboard *Lotus* caused effects aboard *Boz-Kourt* and exclusive jurisdiction of either state would fail to "satisfy the requirements of justice and effectively . . . protect the interests of the two States," so concurrent jurisdiction was required).

[98] *See id.* at 65 (Moore, J., dissenting) (concurring with "judgment of the Court that there is no rule of international law by virtue of which the penal cognizance of a collision at sea . . . belongs exclusively to the country of the ship by or by means of which the wrong was done").

[99] *See id.* at 37 (Loder, J., dissenting) (maintaining that jurisdiction to prescribe is proper in case in which "the author of the crime intends . . . to inflict injury at a place other than that where he himself is"). However, in this case "officer of the *Lotus* : . . had no intention of injuring anyone, and no such intention is imputed to him." *Id.* (Loder, J., dissenting).

[100] *See id.* (Loder, J., dissenting) (asserting that effects principle is "justified where the act and its effect are indistinguishable . . . for instance a shot fired at a person on the other side of a frontier").

casting a second vote to break the tie,[101] in reality, eight of the twelve judges agreed that the effects principle operates if the intent to harm is present.[102] Additionally, seven of the twelve believed that the effects principle was valid with or without an intent to harm.[103]

In addition to the PCIJ and its successor, the International Court of Justice (ICJ), courts around the world have embraced the effects principle as a valid method for exerting the jurisdiction to prescribe.[104] For instance, in an antitrust case, *Hartford Fire Insurance Co. v. California*,[105] the U.S. Supreme Court recognized the effects principle.[106] Furthermore, the European Commission held that member states have jurisdiction under their competition laws in cases that affect commerce between member nations regardless of the locus of the offense.[107] Similarly, "[m]ost other states of Western Europe, including Austria, Denmark, Finland, France, Greece, Norway, Portugal, Spain, Sweden and Switzerland, as well as Canada and Japan . . . have accepted the effects doctrine as applied to economic effects."[108]

While the preceding cases recognize the effects principle for economic effects, the effects principle has its roots in a criminal case,[109] and numerous

[101] *See id.* at 32 (explaining that President, i.e. Chief Judge, cast second vote, "the votes being equally divided").

[102] *See supra* notes 99-100 and accompanying text (noting Judge Loder's view on validity of effects principle).

[103] *See supra* note 98 and accompanying text (stating that Judge Moore accepted effects principle).

[104] *See infra* notes 105-39 and accompanying text (citing international cases using effects principle).

[105] 509 U.S. 764 (1993).

[106] Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (stating that "it is well established by now that the Sherman Act applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States"). In *Hartford*, the Court heard arguments from domestic and foreign reinsurance companies that the United States had charged with violations of U.S. antitrust laws. *Id.* at 769. The reinsurance companies claimed that "the principle of international comity requires the District Court to refrain from exercising jurisdiction over" foreign insurers. *Id.* The Court disagreed with the defendant reinsurance companies, holding that the foreign defendants "engaged in unlawful conspiracies to affect the market for insurance in the United States and that their conduct in fact produced substantial effect." *Id.* at 796.

[107] *See* Aniline Dyes, 1969 O.J. (L 195) 11, 25 1969 C.M.L.R. D 23, D 33 (1969) (determining that European Commission has jurisdiction over undertakings "whether they are based inside or outside the Common Market . . . that are liable to affect commerce between Member States and which have for their object, or their effect, the result of stopping, restraining or distorting free competition within the Common Market").

[108] RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 cmt. n.3 (1987).

[109] *See supra* notes 97-103 and accompanying text (detailing birth of effects principle in

courts continue to apply it to criminal cases.[110] Examples in the United States include *United States v. Thomas*,[111] a domestic case in which all of the activities and parties were in the United States, and *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*,[112] an international case involving activities in Italy and an Italian defendant.[113] Both cases address electronic activity.[114]

In *Thomas*, the court found proper venue in the Western District of Tennessee, although all of the defendants' activities occurred in California.[115] The defendants in *Thomas* operated a bulletin board in California that allowed users, for a fee, to dial in and download pornographic images or order porno-

S.S. Lotus).

[110] *See infra* notes 111-39 and accompanying text (outlining cases using effects principle in courts around world).

[111] 74 F.3d 701 (6th Cir. 1996).

[112] 939 F. Supp. 1032 (S.D.N.Y. 1996).

[113] *See* United States v. Thomas, 74 F.3d 701 (6th Cir. 1996) (establishing that effects principle is valid for venue determination in pornography case); *see also* Playboy Enters., Inc. v. Chuckleberry Publ'g, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996) (holding that United States has jurisdiction over Italian website to extent that it is viewable in United States).

In *Thomas*, the defendants operated a bulletin board in California that featured pornographic images and movies. *Thomas*, 74 F.3d at 705. A federal grand jury indicted the defendants for numerous federal obscenity and child pornography offenses in the Western District of Tennessee stemming from their operation of the bulletin board and for mailing pornographic video tapes. *Id.* at 705-06. The court determined that venue was proper in Tennessee because, although the defendants conducted their business in California, "the effects of the Defendants' criminal conduct reached the Western District of Tennessee." *Id.* at 710. The court also determined that the charges under 18 U.S.C. §§ 1462 and 1465 (obscenity laws) were proper because the pictures in question were intangible, electronic images and it was the intent of Congress to "legislate comprehensively the interstate distribution of obscene materials." *Id.* at 707-09.

The defendant in *Chuckleberry* published *Playmen* magazine in Italy; fifteen years earlier, the same court had enjoined the defendant from distributing an English language version of the magazine in the United States in contravention of the Playboy Enterprises, Inc. (Playboy) trademark. *Chuckleberry*, 939 F. Supp. at 1033-34. The defendant created an Internet site and began distributing *Playmen* from the Internet site. *Id.* at 1034-35. The defendant contended that the injunction did not contemplate Internet distribution of pictures and magazines and that therefore the court could not expand the injunction to cover Internet distribution of the magazine and images. *Id.* at 1036. The *Chuckleberry* court felt that the fact that the parties could not have contemplated dissemination over the Internet was irrelevant to the purpose behind the injunction. *Id.* at 1037. The court held that "[w]hile this Court has neither the jurisdiction nor the desire to prohibit creation of Internet sites around the globe, it may prohibit access to those sites in *this* country." *Id.* at 1040.

[114] *See Thomas*, 74 F.3d at 704 (describing defendants' computer bulletin board); *Chuckleberry*, 939 F. Supp. at 1034-35 (detailing services on defendant's Internet website).

[115] *See Thomas*, 74 F.3d at 710 (stating that defendant had contact with subscriber in Tennessee and that subscriber had defendant's permission to download images to Tennessee).

graphic videotapes.[116] The court used the effects principle to justify venue by suggesting that Tennessee felt the effects of the defendants' actions and that the defendants also consented to the downloading of the images in Tennessee.[117] Although *Thomas* is a domestic case, its reasoning parallels the effects principle under international law.[118]

The district court in *Chuckleberry* determined that the United States could regulate foreign websites to the extent that users in the United States accessed the sites.[119] In 1981, the plaintiff, Playboy Enterprises, Inc. (Playboy), obtained an injunction against the sale and distribution of the Italian magazine *Playmen* in the United States.[120] Fifteen years later, the defendant in *Chuckleberry*, who published *Playmen*, created a website and charged a membership fee for viewing images from the magazine.[121] Playboy filed suit in New York alleging that the publisher of *Playmen* acted in contempt of the 1981 injunction by distributing *Playmen* magazine over the Internet.[122] The district court agreed with Playboy and ordered the defendant to shut down its website or to ensure that no customers from the United States accessed the site.[123] Although the court did not specifically mention the effects principle, it stated that the United States has the authority to force a foreign business that operates in a foreign country to prohibit customers in the United States from accessing its website.[124] In addition to *Thomas* and *Chuckleberry*, numerous other U.S. cases have involved the effects principle.[125]

[116] *See id.* at 705 (explaining how defendants operated their Amateur Action Computer Bulletin Board System (AABSS)).

[117] *See id.* at 709-10 (noting that "AABBS materials were distributed to an approved AABBS member known to reside in the Western District of Tennessee"). In addition, the court determined that the proper community standard for the *Miller* (Miller v. California, 413 U.S. 15 (1973)) obscenity test was Tennessee. *Id.* at 711.

[118] *See supra* notes 84-88 and accompanying text (explaining effects principle in international law).

[119] *See Chuckleberry*, 939 F. Supp. at 1040 (outlining court's jurisdiction in light of existing injunction).

[120] *See id.* at 1034 (detailing previous injunction against publisher of *Playmen*).

[121] *See id.* at 1034-35 (outlining services available on *Playmen* Internet site).

[122] *See id.* at 1033 (stating cause of action in case).

[123] *See id.* at 1041 (holding that defendant must "either shutdown [sic] its Internet site completely or refrain from accepting any new subscriptions from customers residing in the United States [and] invalidate the user names and passwords to the Internet site previously purchased by United States customers").

[124] *See id.* at 1039-40 (stating that worldwide Internet community's right to freedom of speech does not override court orders and injunctions prohibiting foreign entity from distributing banned material to United States).

[125] *See, e.g.*, United States v. Best, No. 01-4321, 2002 WL 31080306, at *1 (3d Cir. Sept. 18, 2002) (stating that United States had jurisdiction over offense of smuggling aliens into

Other countries have recognized the right of a state to prescribe laws against the activities of aliens who operate in foreign countries if the prescribing state feels the effects of the aliens' activities.[126] The most notable Canadian case is *Libman v. The Queen*[127] because it extensively discusses Canadian and British law dealing with the effects principle.[128] In *Libman*, the Canadian Supreme Court determined that Canada could prosecute a Canadian citizen who acted in Canada for a telemarketing fraud committed against U.S. citizens in the United States.[129] Although this case seems to follow the nationality principle, in fact the Court used the effects principle to justify the decision.[130] The defendant argued that Canada lacked jurisdiction to prescribe because the victims resided in the United States and the money from the scheme was neither sent from nor received in Canada and thus the gravamen of the crime occurred abroad.[131] The Court traced English law on multi-jurisdictional crimes and determined that it was appropriate to find jurisdiction over "activi-

United States, even if actions in pursuit of smuggling are taken abroad); United States v. Vasquez-Velasco, 15 F.3d 833 (9th Cir. 1994) (using effects principle to obtain jurisdiction over suspect accused of murdering two American tourists in Mexico); United States v. Felix-Gutierrez, 940 F.2d 1200 (9th Cir. 1991) (utilizing effects principle in case of murder and kidnapping of DEA agent in Mexico); United States v. Wright-Barker, 784 F.2d 161 (3d Cir. 1986) (holding that United States can prescribe laws that regulate drug smuggling extraterritorially); United States v. bin Laden, 92 F. Supp. 2d 189 (S.D.N.Y. 2000) (holding that defendant's actions in bombing of U.S. embassies fell under U.S. jurisdiction to prescribe).

[126] *See infra* notes 127-39 and accompanying text (noting decisions in Canada and United Kingdom).

[127] [1985] 2 S.C.R. 178.

[128] *See* Libman v. The Queen, [1985] 2 S.C.R. 178 (holding that Canada had jurisdiction over defendant for actions committed in United States). The defendant in *Libman* ran a telemarketing scheme in Canada that defrauded citizens of the United States. *Id.* at 181. The Court discussed the history of decisions in the United Kingdom and Canada pertaining to offenses that were conducted in multiple jurisdictions. *Id.* at 183-207. The Court indicated that a line of English cases pointed to a determination that multiple states could exert jurisdiction over a multinational crime. *Id.* at 187-99. The Court determined that the country in which the perpetrator committed the crime and the country in which the victims felt the effects could both exert the jurisdiction to prescribe an offense. *Id.* at 212-13. The Court adopted the position that Canada can prescribe laws in cases in which there is "'a real and substantial link' between an offence and this country." *Id.* at 213. The Court determined that Canada "has a legitimate interest in prosecuting persons for activities that take place abroad but have unlawful consequences" in Canada. *Id.* at 209. The Court held that, for Canada to exert jurisdiction, "a significant portion of the activities constituting that offence [must take] place in Canada" and there should be a "real and substantial link" between Canada and the offense. *Id.* at 213.

[129] *See id.* at 181-82 (outlining defendant's operation).

[130] *See infra* note 132 and accompanying text (explaining use of effects principle).

[131] *See Libman*, 2 S.C.R. at 182-83 (detailing defense's arguments).

ties that take place abroad but have an unlawful consequence here."[132] Other Canadian courts have followed the "continued offence"[133] reasoning of *Libman* and used the effects principle to allow jurisdiction if Canada feels a substantial impact from actions taken abroad.[134]

The English courts also use the effects principle either to exert jurisdiction over foreigners[135] or to allow foreign jurisdiction over actions that occur in Great Britain.[136] In addition, the purpose of the earlier territorial restrictions on jurisdiction to prescribe that Judge La Forest summarized in *Libman* no longer applies with the same force that it did before communication technologies made international transactions cheap, fast, and reliable.[137] The impact of actions taken abroad affects domestic businesses;[138] thus, a state has an obligation to protect its citizens and businesses from crimes initiated abroad.[139]

[132] *Id.* at 209. The Court determined that because the proceeds of the fraudulent scheme ended up in Canada, Canada felt the effects of the scheme. *Id.* at 211.

[133] *See id.* at 196-99 (explaining that "continuing offence" refers to crime with elements that occur in multiple jurisdictions and that are punishable in all jurisdictions in which substantial portion of crime was committed).

[134] *See, e.g.*, Cook v. The Queen, [1998] 2 S.C.R. 597 (invalidating testimony obtained in United States by Canadian police who failed to properly explain rights to defendant); R. v. Greco, [2001] 159 C.C.C. (3d) 146 (allowing prosecution of Canadian citizen who violated conditions of parole while abroad).

[135] *See* Trade v. Markus, [1976] A.C. 35 (giving English law jurisdiction over "international swindle" because effect of crime was felt in England); R. v. Wall, [1974] 1 W.L.R. 930 (Eng. C.A.) (holding that acts committed abroad that resulted in importation of drugs into England were subject to English law); Director of Public Prosecutions v. Doot, [1973] A.C. 807 (same); R. v. Baxter, [1972] 1 Q.B. 1 (exerting jurisdiction over resident of Northern Ireland for mail fraud affecting English citizens).

[136] *See* Treacy v. Director of Public Prosecutions, [1971] A.C. 537 (stating that appellant could be tried in Germany for blackmail initiated from England); King v. Godfrey, [1923] 1 K.B. 24 (holding that English citizen could be extradited to Switzerland for involvement in crime committed in Switzerland, even though defendant acted in United Kingdom).

[137] *See* Libman v. The Queen, [1985] 2 S.C.R. 178, 208 (noting reasons for development of territoriality). The court explained that:

> the territoriality principle in criminal law was developed by the courts to respond to two practical considerations, first, that a country has generally little direct concern for the actions of malefactors abroad, and secondly, that other States may legitimately take umbrage if a country attempts to regulate matters taking place wholly or substantially within their territories. For these reasons the courts adopted a presumption against the application of laws beyond the realm . . . .

Id.

[138] *See, e.g.*, Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (explaining effects of foreign antitrust violations on domestic insurance market).

[139] *See Libman*, 2 S.C.R. at 209 (determining that state has legitimate interest in protect-

2. Applying the Effects Principle to Computer Viruses

Given the legitimacy of the effects principle in both civil and criminal cases, the principle should cover the release of a computer virus.[140] According to *S.S. Lotus*, intent to harm is not necessary to invoke the effects principle.[141] Therefore, the mere release of a virus that propagates rapidly and causes a large amount of damage is sufficient to allow a damaged country to prescribe the conduct of the distributor.[142] Damages from the Melissa virus exceeded $80 million[143] and estimated damages from iloveyou reached $10 billion.[144] It is hard to argue that these viruses did not have a substantial effect on a country such as the United States, which has the largest presence on the Internet.[145]

Unlike the situation in the *S.S. Lotus*, viruses do not create a physical invasion.[146] However, numerous countries recognize the economic effects of a crime as a valid basis for jurisdiction.[147] Therefore, a computer virus can fall under the effects principle even if neither an intent to harm[148] nor a physical invasion exists.[149]

ing its citizens from crimes committed abroad).

[140] *See infra* notes 141-49 and accompanying text (detailing how effects principle covers computer viruses).

[141] *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9, at 37 (Sept. 7, 1927) (Loder, J., dissenting) (noting that majority's decision effectively disposed of intent-to-harm requirement).

[142] *See supra* notes 105-36 and accompanying text (explaining recognition of effects principle in cases involving damage similar to that caused by computer viruses).

[143] *See* Moskowitz, *supra* note 16, at 37 (detailing damages caused by Melissa).

[144] *See* Landler, *supra* note 8, at C1 (estimating damages from iloveyou virus).

[145] *See* Reno v. ACLU, 521 U.S. 844, 850 (1997) (stating that 60% of Internet hosts are located in United States); Dawn C. Valdivia, *Report on the E-Commerce Activities of the OAS, ICC, ABA, and Uncitral*, 17 ARIZ. J. INT'L & COMP. LAW 109, 110 (2000) (noting that over 55% of all Internet hosts are in United States and Canada).

[146] *Compare* S.S. Lotus, 1927 P.C.I.J at 10 (explaining that actions of French officer resulted in *Lotus* cutting *Boz-Kourt* in half) *with* United States v. Thomas, 74 F.3d 701, 706 (6th Cir. 1996) (noting that computer data is intangible).

[147] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 cmt. n.3 (1987) (noting that Austria, Canada, Denmark, Finland, France, Greece, Japan, Norway, Portugal, Spain, Sweden, and Switzerland have accepted economic effects as valid basis for jurisdiction).

[148] *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9, at 37 (Sept 7, 1927) (Loder, J., dissenting) (noting that majority's decision effectively disposed of intent-to-harm requirement).

[149] *See supra* note 147 and accompanying text (noting that many countries view mere economic effects as sufficient basis for jurisdiction).

B. The Protective Principle

The protective principle, which is similar to the effects principle, allows a state to criminalize conduct directed at the state from outside of the state.[150] The difference between the effects principle and the protective principle is that the protective principle requires that the action target the government of the state itself.[151] Judge Loder described the protective principle in his dissent in *S.S. Lotus* as "the jurisdiction over offences committed by foreigners abroad . . . in so far as they are directed against the state itself or against its security or credit."[152]

1. Legitimacy of the Protective Principle

In 1804, the U.S. Supreme Court decided *Church v. Hubbart*,[153] which contains the origins of the protective principle in the United States.[154] *Church* involved an American ship that Portuguese authorities seized for attempting to trade with the Portuguese colony of Brazil in contravention of Portuguese law.[155] The Court used the protective principle to justify the actions of the Portuguese authorities, stating that Portugal was within its rights to protect its colonies from threats that originated outside of Portugal's territorial waters.[156]

[150] *See infra* text accompanying note 152 (noting protective principle's extraterritorial application).

[151] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(3) (1987) (explaining scope of protective principle).

[152] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9, at 35-36 (Sept. 7, 1927) (Loder, J., dissenting).

[153] 6 U.S. 187 (2 Cranch) (1804).

[154] Church v. Hubbart, 6 U.S. 187 (2 Cranch) (1804) (recognizing Portugal's right to protect its foreign colonies from vessels on high seas). Portuguese authorities boarded and seized the *Aurora*, a ship flying the U.S. flag, off the coast of Brazil for smuggling and attacking a Portuguese vessel. *Id.* at 188-89. The owner of the vessel submitted a claim requesting that the insurance company pay for his losses but the insurance company refused, relying on clauses in the policies exempting losses incurred by illicit trade with the Portuguese. *Id.* at 187. The insurance company produced copies of Portuguese laws and a judgment against the *Aurora* from a local Brazilian court to prove that the Portuguese officials confiscated the ship because of illicit trade with the Portuguese colony. *Id.* at 189-98. The Court stated that it was lawful under international law for Portugal to protect its sovereignty by acting outside of its territory. *Id.* at 220. The Court held that the Portuguese documents presented to the jury were not properly authenticated and thus inadmissible. *Id.* at 227-30.

[155] *See id.* at 198-99 (explaining Portuguese law prohibiting other nations from trading with Portuguese colonies).

[156] *See id.* at 234 (determining that state's "power to secure itself from injury [ ] may certainly be exercised beyond the limits of its territory").

More recently, several circuit courts have applied the protective principle, often in conjunction with other principles of jurisdiction.[157] For instance, the Court of Appeals for the Second Circuit used the protective principle in a case involving false statements on a visa application.[158] Additionally, in a case that involved a conspiracy to import drugs into the United States, the Court of Appeals for the Fifth Circuit used the protective principle to exert its jurisdiction.[159] Furthermore, the Court of Appeals for the Ninth Circuit used the protective principle, in conjunction with the effects principle and passive personality, to maintain jurisdiction over a defendant who assisted with the kidnapping and murder of a Drug Enforcement Agency (DEA) agent.[160] Similarly, the Court of Appeals for the Eleventh Circuit used the protective principle and passive personality in a case concerning a conspiracy to murder a DEA agent.[161]

Another U.S. case, *United States v. bin Laden*,[162] contains a summary of the protective principle.[163] In *bin Laden*, the court explained that the United

[157] *See infra* notes 158-61 (listing circuit court cases using protective principle).

[158] *See* United States v. Pizzarusso, 388 F.2d 8, 10 (2d Cir. 1968) (stating that "the protective principle . . . covers the instant case"). The court went on to state that the protective principle differs from the effects principle in that "there need not be any actual effect in the country . . . ." *Id.* at 11.

[159] *See* Marin v. United States, 352 F.2d 174, 177 (5th Cir. 1965) (determining that U.S. courts have jurisdiction over "a crime committed [by an alien] against the United States at a time when the offender was corporeally out of the jurisdiction of the United States").

[160] *See* United States v. Felix-Gutierrez, 940 F.2d 1200, 1206 (9th Cir. 1991) (explaining that defendant's actions "adversely affected the national interest"). The fact that the DEA agent was a United States citizen contributed to the court's finding that there was a "significant detrimental effect in the United States" and that the DEA agent was attacked because he was a United States citizen. *Id.* The court determined that it did not need to "decide whether any of these facts or principles, standing alone, would be sufficient. Rather, we hold that cumulatively applied they require the conclusion that giving extraterritorial effect" to the statute was proper. *Id.*

[161] *See* United States v. Benitez, 741 F.2d 1312, 1316 (11th Cir. 1984) (stating that "[t]wo of the principles [of jurisdiction] . . . are applicable in this case – the protective principle and the passive personality principle").

[162] 92 F. Supp. 2d 189 (S.D.N.Y. 2000).

[163] *See* United States v. bin Laden, 92 F. Supp. 2d 189, 197 (S.D.N.Y. 2000) (recognizing "the right of the United States to defend itself from harmful conduct regardless of its locus"). The case involved fifteen defendants charged in a conspiracy to bomb the U.S. embassies in Kenya and Tanzania, which resulted in 223 deaths. *Id.* at 192. The court ruled on the extraterritorial jurisdiction of several federal statutes. *Id.* The court held that counts 234, 235, 240, and 241 dealt with statutes that were specifically limited to U.S. territory. *Id.* The court held that 18 U.S.C. § 844(f), (h), and (n) (destroying buildings with explosives or using explosives in commission of felony), 18 U.S.C. § 924(c) (using or carrying firearm during commission of crime of violence), 18 U.S.C. § 930(c) (killing someone in federal facility), 18 U.S.C. § 1114

States has the right to protect itself from harm regardless of where the harm originates.[164] The court examined whether or not certain federal statutes applied extraterritorially.[165] Judge Sand found that the protective principle applied to all but two of the federal statutes in question, regardless of where the crimes occurred.[166]

Further support for the protective principle exists outside of the United States.[167] The leading case in the United Kingdom, *Joyce v. Director of Public Prosecutions*,[168] involved a treasonous act committed during World War II.[169] The defendant in *Joyce* appealed his conviction for treason, resulting from activities committed in Germany during the war.[170] The Court determined that an English court could try an alien for acts committed abroad and directed at the security of the United Kingdom.[171] The Court went so far as to say that "the protective jurisdiction here contended for is well recognized

(killing or attempting to kill officer or employee of United States), and 18 U.S.C. § 2155(a) and (b) (attacking or conspiring to attack national-defense structures of United States) all applied extraterritorially. *Id.* at 198-204.

[164] *See id.* at 197 (explaining protective principle).

[165] *See id.* at 192 (noting need to determine extraterritorial effect of statutes); *see also infra* Part IV.B (analyzing extraterritorial application of 1994 Act).

[166] *See bin Laden*, 92 F.Supp. 2d at 192 (summarizing holding as dismissing only counts specifically limited to U.S. territory).

[167] *See infra* notes 168-77 and accompanying text (detailing cases in courts outside of United States using protective principle).

[168] [1946] A.C. 347 (HL).

[169] *See* Joyce v. Director of Public Prosecutions, [1946] A.C. 347, 348 (H.L.) (outlining charges against defendant). The defendant obtained a British passport and left England in 1939. *Id.* at 348-49. The defendant was later convicted of treason for broadcasting propaganda on behalf of Germany, which was at war with England, while the defendant lived in Germany. *Id.* The defendant appealed his conviction to the House of Lords on the grounds that he owed no allegiance to Great Britain, that protection by the Crown is necessary to prove allegiance, that protection of the Crown must be exercisable, that the renewal of defendant's passport was insufficient to prove protection of the Crown, and that no English court had jurisdiction over aliens acting on foreign soil. *Id.* at 350-51. The Court determined that the defendant owed allegiance to the Crown and that the Crown still protected the defendant. *Id.* at 359. The Court stated that international law does not specifically prohibit a state from exercising its jurisdiction upon aliens who act abroad. *Id.* at 356. The Court held that although a rebuttable presumption exists that English laws do not act extraterritorially, the treason law of 1351 allows English courts to try aliens for acts committed abroad. *Id.* at 336-37.

[170] *See id.* at 348-49 (detailing defendant's actions in obtaining passport, traveling to Germany, and broadcasting propaganda for Germany).

[171] *See id.* at 356 (stating that "there is no principle that no alien is triable in England for offences committed abroad").

in international law."[172] In addition to treason, the House of Lords has subjected an alien living abroad to bankruptcy proceedings in England.[173]

Other European courts also apply the protective principle.[174] For instance, the Supreme Court of Holland upheld the conviction of a Belgian woman for being an accessory while in Belgium to an offense under the Dutch Currency Decree.[175] In Belgium, the Court of Cassation ruled that a Belgian court could try a foreign soldier for actions committed abroad that threatened the safety of Belgium.[176] In addition, treason against France, or its World War II allies, is justiciable in French courts, even if the defendant is a foreign national acting outside of the borders of France.[177]

Numerous other states recognize the protective principle in cases and in statutes.[178] The justification for the protective principle is that most states are ill-equipped to deal with domestic attacks on the sovereignty of foreign states.[179] This justification parallels the growth of computer crime throughout the world, in which many countries have neither laws criminalizing the conduct[180] nor the technological expertise to determine who committed the crime.[181]

[172] *Id.* at 358.

[173] *See* Theophile v. Solicitor-General, [1950] A.C. 186, 195-97 (H.L.) (stating that bankruptcy laws were meant to be enforced extraterritorially).

[174] *See infra* notes 175-77 and accompanying text (noting cases in France, Belgium and Holland that use protective principle).

[175] *See* Public Prosecutor v. L., 18 I.L.R. 206, 206 (HR 1951) (stating that Belgian national could be convicted under Dutch currency law for actions committed in Belgium).

[176] *See* Nusselein v. Belgian State, 17 I.L.R. 135, 135 (Bel. 1950) (holding that Belgian courts have jurisdiction over crimes against Belgium's safety committed by foreign soldiers, whether in Belgium or abroad).

[177] *See Re* van den Plas, 22 I.L.R. 205, 207 (Fr. 1955) (deciding that Belgian national could be tried in France for treason against Belgium, which was wartime ally of France).

[178] *See* Edwin D. Dickinson, RESEARCH IN INTERNATIONAL LAW, UNDER THE AUSPICES OF THE FACULTY OF THE HARVARD LAW SCHOOL, *Jurisdiction with Respect to Crime*, (1932), *reprinted in* 29 AM. J. INT'L LAW 435, 543-61 (Supp. 1935) (detailing national statutes and cases recognizing protective principle).

[179] *See id.* at 552 (stating that protective principle is justified by "inadequacy of most national legislation [in] punishing offenses committed within the territory against the security, integrity and independence of foreign States").

[180] *See* Moskowitz, *supra* note 16, at 37 (stating that Philippines had no computer crime statute prior to 2000).

[181] *See* John Schwartz & David A. Vise, *'Love' Virus Is Traced to Philippines; Authorities Move to Seize Computers Used in Attack*, WASH. POST, May 6, 2000, at A1 (noting how quickly FBI traced iloveyou to Philippines).

2. Applying the Protective Principle to Computer Viruses

Although computer viruses seem to fit relatively easily into the framework of the effects principle,[182] only a very specifically targeted virus would meet the requirements of the protective principle.[183] For the protective principle to operate, the virus must target the instrumentality or the functioning of the state.[184] Thus, although the Melissa and iloveyou viruses affected some governmental computers,[185] they did not specifically target the U.S. government.[186] Therefore, neither virus would have invoked the protective principle.[187]

However, it is possible for the protective principle to encompass at least some computer viruses.[188] For instance, CodeRed, which specifically targeted the White House website,[189] would allow the United States to use the protective principle.[190] 'Although CodeRed did not seriously affect the security of the United States or the ability of the U.S. government to function,[191] it targeted the U.S. government.[192] Therefore, a court could use the protective principle in allowing jurisdiction over the distributor of CodeRed even if the distributor acted while abroad.[193] Thus, the United States can use the protec-

[182] *See supra* notes 140-145 and accompanying text (discussing applicability of effects principle to computer viruses).

[183] *See infra* text accompanying notes 184-94 (noting how viruses can trigger protective principle).

[184] *See supra* notes 150-51 and accompanying text (explaining that protective principle requires crime against security of state or governmental functions).

[185] *See* Landler, *supra* note 8, at C1 (claiming that iloveyou affected Pentagon computers).

[186] *See* Chien & Ewell, *supra* note 9 (explaining how iloveyou operated); Elnitiarta, *supra* note 2 (detailing how Melissa operated).

[187] *See supra* note 151 and accompanying text (requiring that actions target government under protective principle).

[188] *See infra* notes 189-94 and accompanying text (giving example and explaining why CodeRed falls under protective principle).

[189] *See* Eric Chien, *Security Response: CodeRed Worm, at* http://www.symantec.com/avcenter/venc/data/codered.worm.html (last modified Sept. 24, 2002) (stating that "if the date is between the 20th and 28th of the month, the active threads then attempt a Denial of Service attack on . . . 198.137.240.91, which was www.whitehouse.gov").

[190] *See infra* text accompanying notes 191-94 (detailing why CodeRed invokes protective principle).

[191] *See* Chien, *supra* note 189 (noting that IP address 198.137.240.91 "is no longer active").

[192] *See id.* (detailing effects of CodeRed, which consisted mainly of Denial of Service attacks on White House website's IP address).

[193] *See supra* note 151 and accompanying text (explaining that extraterritorial attacks on

tive principle if an instrumentality of the U.S. government is targeted, although very few viruses are likely to meet this requirement.[194]

C. Passive Personality

A third basis for extraterritorial jurisdiction is passive personality.[195] Passive personality is also known as passive nationality[196] because it refers to the nationality of the victim, while active nationality refers to the nationality of the perpetrator.[197] Passive personality protects citizens from crimes committed against them because of their nationality.[198] Similar to the effects and protective principles, passive personality allows a state to prescribe laws against the actions of aliens who act while in foreign countries.[199]

1. Legitimacy of Passive Personality

Passive personality enjoys the least support of any of the bases of jurisdiction to prescribe.[200] Even though the laws of some twenty-seven countries recognized the principle in 1935,[201] courts around the world rarely apply this principle. The United States and the United Kingdom were early critics of passive personality, although they both recognize passive personality in some cases.[202]

U.S. government are covered by protective principle).

[194] *See supra* text accompanying notes 184-93 (noting difficulty of applying protective principle to most computer viruses).

[195] *See supra* notes 71-72, 79-82 and accompanying text (listing different bases of extraterritorial jurisdiction to prescribe).

[196] *See* Menthe, *supra* note 48, at 72 (describing active and passive nationality).

[197] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 cmt. e (1987) (explaining nationality principle).

[198] *See id.* § 402 cmt. g (stating purpose of passive personality).

[199] *See id.* (mentioning that passive personality allows state to "apply law . . . to an act committed outside its territory by a person not its national").

[200] *See* Dickinson, *supra* note 178, at 579 (stating that "[j]urisdiction asserted upon the principle of passive personality without qualifications has been more strongly contested than any other type of competence"); BROWNLIE, *supra* note 49, at 303 (noting that passive personality "is the least justifiable, as a general principle, of the various bases of jurisdiction").

[201] *See* Dickinson, *supra* note 178, at 578 (listing statutes from twenty-seven countries that recognized passive personality). The countries that recognized passive personality in 1935 were: Albania, Brazil, China, Cuba, Czechoslovakia, Estonia, Finland, France, Greece, Guatemala, Italy, Japan, Latvia, Lithuania, Mexico, Monaco, Peru, Poland, Rumania, Russia, San Marino, Sweden, Switzerland, Turkey, Uruguay, Venezuela, and Yugoslavia. *Id.*

[202] *See id.* at 579 (noting strong opposition of United States and United Kingdom to passive personality principle).

While the United States is one of the most aggressive states in its exercise of jurisdiction outside of its own borders,[203] relatively few cases invoke passive personality in the United States.[204] Courts in the United States occasionally bolster their justification for allowing jurisdiction by using passive personality along with other bases of jurisdiction.[205] However, not even the U.S. Restatement of Foreign Relations, which is more accepting of extraterritorial jurisdiction than are many countries,[206] gives passive personality full endorsement.[207]

The *Cutting Case*[208] is the most widely cited case in which a court used passive personality.[209] This case involved an American citizen charged in Mexico for libelous statements about a Mexican citizen.[210] The statements appeared in a U.S. newspaper in 1886.[211] Despite the protests of the United States, Mexico approved the use of passive personality against a foreigner,[212]

[203] *See* BROWNLIE, *supra* note 49, at 308 (noting "strong reaction from a large number of foreign governments" in response to American exercise of extraterritorial jurisdiction).

[204] *See id.* at 308-09 (detailing limited international judicial reaction to United States' policies on exerting extraterritorial jurisdiction).

[205] *See* United States v. Felix-Gutierrez, 940 F.2d 1200, 1206 (9th Cir. 1991) (stating that combination of effects principle, protective principle, and passive personality were sufficient to allow jurisdiction); United States v. Benitez, 741 F.2d 1312, 1316-17 (11th Cir. 1984) (applying protective principle and passive personality in order to justify jurisdiction).

[206] *Compare* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (1987) (stating acceptable bases of jurisdiction) *with* BROWNLIE, *supra* note 49, at 308 (noting hostile reaction of many states to United States exercise of extraterritorial jurisdiction).

[207] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 cmt. g (1987) (noting that passive personality is rarely accepted, except against terrorism).

[208] (1886), *reprinted in* 2 JOHN BASSETT MOORE, INTERNATIONAL LAW DIGEST § 201, at 228 (1906).

[209] *See* The Cutting Case (1886), *reprinted in* 2 JOHN BASSETT MOORE, INTERNATIONAL LAW DIGEST § 201, at 228 (1906) (explaining Mexico's use of passive personality). The *Cutting Case* involved an American, A.K. Cutting, who published statements about a Mexican citizen in a United States paper. *Id.* at 229. Upon Cutting's return to Mexico, Mexican authorities charged him with libel under Article 186 of the Mexican Penal Code, which allowed Mexico to exert jurisdiction over foreigners who commit acts against Mexicans in foreign countries. *Id.* at 230, 232. The United States claimed that this case "disclosed a claim of jurisdiction by Mexico, novel in our history, whereby any offense, committed anywhere by a foreigner . . . [can] be there tried and punished in conformity with Mexican laws." *Id* at 231. However, the Mexican courts sustained jurisdiction over Cutting, and the executive branch of the Mexican government gave its approval. *Id.*

[210] *Id.* at 229.

[211] *Id.*

[212] *See id.* at 231 (stating that "jurisdiction was sustained by the courts of Mexico . . . and approved by the executive branch of that government").

without requiring any showing of effects within Mexico.[213] In addition, the court found no evidence that the defendant singled out the Mexican citizen based on his nationality.[214] This is a rare case, and in the last 125 years no judicial recognition of passive personality in the torts context is evident.

The more commonly accepted use of passive personality involves terrorism.[215] Many states, including the United States, acknowledge the legitimacy of seeking to protect nationals from terrorist activities.[216] However, computer viruses do not rise to the level of terrorism.[217] Although there is no formally accepted definition of terrorism, the release of a computer virus does not instill the same level of fear that the bombing of buildings and the hijacking of airplanes instills.[218] Even if viruses did constitute a terrorist activity, other bases of jurisdiction would encompass the activity.[219]

2. *Applying Passive Personality to Computer Viruses*

Assuming for the moment that passive personality is a valid basis for asserting jurisdiction, it is unlikely to apply to computer viruses.[220] It is very difficult to write a virus that targets victims based on their nationality.[221] However, CodeRed is a computer virus that could be characterized as targeting U.S. nationals.[222] For instance, CodeRed attacked www.whitehouse.gov[223] and defaced websites hosted on computers with a default language of

[213] *See id.* at 229 (noting that "paper was not published in Mexico").

[214] *See id.* (explaining that libelous statement concerned "a citizen of Mexico, with whom Mr. Cutting has been in controversy").

[215] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 cmt. g (1987) (stating that passive personality "has not been generally accepted for ordinary torts or crimes, but it is increasingly accepted as applied to terrorist" activities).

[216] *See id.* (noting growing acceptance of passive personality for acts of terrorism).

[217] *See* Mark Lacter, *Spreading the Virus*, 23 L.A. BUS. J. 46, 46 (Dec. 10, 2001) (stating that "computer viruses are not akin to terrorist attacks").

[218] *Id.*

[219] *See infra* text accompanying notes 229-34 (explaining how passive personality covers same crimes as effects or protective principles).

[220] *See infra* notes 226-28 and accompanying text (detailing difficulty of targeting U.S. nationals with computer virus).

[221] *See infra* notes 226-28 and accompanying text (noting difficulty of creating virus based on nationality of victim).

[222] *See infra* notes 223-25 and accompanying text (determining that CodeRed indirectly targeted U.S. citizens).

[223] *See* Chien, *supra* note 189 (explaining that CodeRed launched Denial of Service attacks against IP address of www.whitehouse.gov).

English.[224] Thus, CodeRed indirectly targeted citizens of the United States because of their nationality.[225] Another way to spread a computer virus to a specific nationality is to write the text in a language used primarily by that country.[226] This strategy is unlikely to target only the United States because English is so prevalent outside of the United States.[227] Finally, a virus could detect the time zone that the computer is set to and activate only if it is a U.S. time zone.[228]

Although it seems possible for a computer virus to target nationals of a specific country, any such attempt will almost certainly fall under the more acceptable forms of jurisdiction, such as the effects or protective principles.[229] For example, for a virus to invoke passive personality but not the effects or protective principles, it would have to target U.S. citizens[230] without any substantial effect in the United States[231] and without affecting U.S. interests abroad or government functions.[232] Such a virus would be very specialized and would not be particularly effective.[233] Therefore, although passive

[224] *Id.*

[225] Attacking the White House website, only activating on web servers with a default language of English, and defacing websites with the text: "Hacked By Chinese!" suggests that the virus targeted U.S. citizens. *Id.* This is reinforced by the fact that the virus was first discovered on Monday, July 16, 2001 (*id.*), three days after the IOC awarded Beijing the 2008 Olympic Summer Games (Ross Siler & Jim Reedy, *Beijing Vote Brings Mixed Reaction; Decision Seen as Positive Step for China*, WASH. POST, July 14, 2001, at D1), which the U.S. Congress opposed. *See* Jere Longman, *Beijing Expected to Receive the 2008 Summer Games When the I.O.C. Votes*, N.Y. TIMES, July 8, 2001, sec. 8 at 1 (noting congressional opposition to Beijing hosting Olympics in 2008).

[226] *See* Chien & Ewell, *supra* note 9 (identifying seven variants of iloveyou virus with E-mail message written in languages other than English, including Spanish, Italian, Lithuanian, and German).

[227] English is the primary language in 104 countries. THE WORLD ALMANAC AND BOOK OF FACTS 2002 447 (2002).

[228] *See* Raul Elnitiarta, *Symantec Security Response: W97M.Melissa.M*, *at* http://securityresponse.symantec.com/avcenter/venc/data/w97m.melissa.m.html (last visited Dec. 16, 2002) (noting that Melissa variant M E-mails information about infected computer, including time zone, to three E-mail addresses).

[229] *See infra* text accompanying notes 230-32 (suggesting that effects and protective principles are better suited for dealing with computer viruses).

[230] *See supra* note 198 and accompanying text (explaining requirement of passive personality that crime targets state's nationals).

[231] *See supra* Part III.A (noting that effects principle requires substantial impact on state's territory).

[232] *See supra* Part III.B (requiring that crime targets state's instrumentality in order to invoke protective principle).

[233] Viruses propagate most effectively by exploiting commonly used languages and

personality may bolster the case for jurisdiction in specific cases, it is unlikely to be the sole basis for extraterritorial jurisdiction over a computer virus.[234]

D. Universal Jurisdiction

The final basis for jurisdiction to prescribe is universal jurisdiction.[235] Although universal jurisdiction has broad support,[236] it is limited to universally recognized crimes.[237] Originally, universal jurisdiction only applied to piracy cases.[238] However, countries now recognize other crimes as being subject to universal jurisdiction.[239] Nonetheless, computer viruses do not rise to the level of a peremptory norm that would justify universal jurisdiction.[240]

1. Legitimacy of Universal Jurisdiction

There is worldwide recognition of universal jurisdiction with respect to piracy.[241] The global community also condemns other crimes under universal

computer programs. If more computers use a particular program or language, then more systems can be infected by exploiting a weakness in that program or language.

[234] *See supra* notes 220-33 and accompanying text (explaining why passive personality is not well suited to computer viruses).

[235] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 404 (1987) (defining universal jurisdiction).

[236] *See infra* notes 241-56 and accompanying text (detailing international support for universal jurisdiction).

[237] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 404 (1987) (explaining types of crimes that invoke universal jurisdiction).

[238] *See* Dickinson, *supra* note 178, at 563 (maintaining that "State has jurisdiction with respect to any crime committed outside its territory by an alien which constitutes piracy by international law").

[239] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 404 (1987) (stating that states have "jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, . . . hijacking . . . , genocide, war crimes, and perhaps certain acts of terrorism"); Patrick L. Donnelly, Note, *Extraterritorial Jurisdiction over Acts of Terrorism Committed Abroad: Omnibus Diplomatic Security and Antiterrorism Act of 1986*, 72 CORNELL L. REV. 599, 603-04 (1987) (describing crimes covered by universal jurisdiction).

[240] *See infra* notes 257-60 and accompanying text (explaining why computer viruses do not justify universal jurisdiction).

[241] *See* Convention on the High Seas, Apr. 29, 1958, art. 14, 13 U.S.T. 2312, 2317, 450 U.N.T.S. 82, 92 ("All States shall co-operate to the fullest possible extent in the repression of piracy . . . ."); *see also* 2 GREEN HAYWOOD HACKWORTH, DIGEST OF INTERNATIONAL LAW, § 203 at 681 (1941) ("It has long been recognized and well settled that persons and vessels engaged in piratical operations . . . may be punished by any nation . . . ."); Dickinson, *supra* note 178, at 563 (noting that "jurisdiction of the State to prosecute and punish for piracy . . . is everywhere recognized"); The Cutting Case (1886), *reprinted in* JOHN BASSETT MOORE,

jurisdiction, as evidenced by both treaties and cases.[242] Numerous international treaties, conventions, and resolutions condemn slavery,[243] war crimes,[244] hijacking,[245] genocide,[246] and torture.[247]

INTERNATIONAL LAW DIGEST § 201, at 951-52 (explaining that piracy "is an offense against the law of nations . . . and [the pirate] is treated as an outlaw, whom any nation may in the interests of all capture and punish").

[242] *See infra* notes 243-55 and accompanying text (outlining treaties and cases that support universal jurisdiction).

[243] *See* Slavery Convention, Sept. 25, 1926, art. 2(b), 46 Stat. 2183, 2191, 60 L.N.T.S. 253, 263 (agreeing that "[t]he High Contracting Parties undertake . . . to bring about . . . the complete abolition of slavery in all its forms"); Protocol amending the Slavery Convention, Dec. 7, 1953, 7 U.S.T. 479, 481-82, 182 U.N.T.S. 51, 52, 54 (adopting Slavery Convention under United Nations); Supplementary Convention on the Abolition of Slavery, the Slave Trade and Institutions and Practices Similar to Slavery, Sept. 7, 1956, 18 U.S.T. 3201, 266 U.N.T.S. 3 (calling on parties to abolish slavery and similar practices); International Covenant on Civil and Political Rights, Dec. 19, 1966, art. 8, 999 U.N.T.S. 171, 175 (stating that "[n]o one shall be held in slavery; slavery and the slave trade in all their forms shall be prohibited"); Universal Declaration of Human Rights, art. 4, G.A. Res. 217A, U.N. GAOR, 3d Sess., Supp. No. 13, U.N. Doc. A/810 (1948) (same); Convention on the High Seas, Apr. 29, 1958, art. 13, 13 U.S.T. 2312, 2316, 450 U.N.T.S. 82, 90 (agreeing that "[e]very State shall adopt effective measures to prevent and punish the transportation of slaves in ships authorized to fly its flag").

[244] *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 (codifying war crimes); Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 (same); Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (same); Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 (same).

[245] *See* Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, art. 11(1), 20 U.S.T. 2941, 2947 (requiring contracting states to "take all appropriate measures to restore control of the [hijacked] aircraft to its lawful commander or to preserve his control of the aircraft"); Convention for the Suppression of Unlawful Seizure of Aircraft, Dec. 16, 1970, art. 7, 22 U.S.T. 1641, 1646, 860 U.N.T.S. 105, 109 (requiring states to prosecute or extradite hijackers found within their territorial boundaries).

[246] *See* Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, art. 1, 78 U.N.T.S. 277, 280 (declaring that "[g]enocide, whether committed in time of peace or in time of war, is a crime under international law which [the Parties] undertake to prevent and punish").

[247] *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 3(1)(a), 6 U.S.T. 3114, 3116, 75 U.N.T.S. 31, 32 (stating that "the following acts shall remain prohibited . . . murder of all kinds, mutilation, cruel treatment and torture"); Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, art. 3(1)(a), 6 U.S.T. 3217, 3222, 75 U.N.T.S. 85, 88 (same); Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, art. 3(1)(a), 6 U.S.T. 3316, 3318, 3320, 75 U.N.T.S. 135, 138 (same); Geneva Convention Relative to the Protection of Civilian

In addition to treaties, numerous cases in national courts suggest that the international community recognizes universal jurisdiction.[248] For example, in the United Kingdom, the House of Lords recognizes universal jurisdiction in cases of torture.[249] Australia recognizes genocide as a crime that justifies universal jurisdiction.[250] The Supreme Court of Canada has held that war crimes and crimes against humanity invoke universal jurisdiction.[251] Finally, the United States uses universal jurisdiction for hijacking,[252] other crimes committed on aircraft,[253] drug trafficking,[254] and terrorism.[255] There is ample

Persons in Time of War, Aug. 12, 1949, art. 3(1)(a), 6 U.S.T. 3516, 3518, 3520, 75 U.N.T.S. 287, 290 (same); International Covenant on Civil and Political Rights, Dec. 19, 1966, art. 7, 999 U.N.T.S. 171, 175 (agreeing that "[n]o one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment"); Universal Declaration of Human Rights, art. 5, G.A. Res. 217A, U.N. GAOR, 3d Sess., Supp. No. 13, U.N. Doc. A/810 (1948) (same); Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, art. 2(1), 1465 U.N.T.S. 85, 114 (stating that "[e]ach State Party shall take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction"); Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, art. 2, G.A.Res. 3452, U.N. GAOR, 30th Sess., Supp. No. 34, U.N. Doc. A/XXX (1975) (stating that "[a]ny act of torture or other cruel, inhumane or degrading treatment or punishment is an offense to human dignity and shall be condemned as a denial of the purposes of the Charter of the United Nations").

[248] *See infra* notes 249-55 and accompanying text (outlining international cases accepting universal jurisdiction).

[249] *See* Regina v. Bow St. Metro. Stipendiary Magistrate, *ex parte* Pinochet Ugarte, (No. 3) [2000] 1 A.C. 147, 160 (H.L. 1999) (recognizing torture as peremptory norm that justifies universal jurisdiction).

[250] *See* Nulyarimma v. Thompson [1999] FCA 1192, 1203 (identifying genocide as peremptory norm that is subject to universal jurisdiction).

[251] *See* Regina v. Finta, [1994] 1 S.C.R. 701, 717 (explaining that "conduct listed under crimes against humanity was of the sort that no modern civilized nation was able to sanction").

[252] *See* United States v. Rezaq, 134 F.3d 1121, 1133 n.6 (D.C. Cir. 1995) (noting that "hijacking crimes are subject to universal jurisdiction"); United States v. Yunis, 924 F.2d 1086, 1092 (D.C. Cir. 1991) (stating that "[a]ircraft hijacking may well be one of the few crimes so clearly condemned under the law of nations that states may assert universal jurisdiction to bring offenders to justice, even when the state has no territorial connection to the hijacking and its citizens are not involved").

[253] *See* United States v. Yousef, 927 F. Supp. 673, 682 (S.D.N.Y. 1996) (determining that blowing up commercial airliner filled with people "is at least as heinous a crime of international concern as hijacking"); United States v. Georgescu, 723 F. Supp. 912, 919 (E.D.N.Y. 1989) (explaining that "[m]any crimes committed aboard aircraft are considered both by the United States and the international community to be 'Offenses against the Law of Nations,'" including sabotage and hijacking).

[254] *See* United States v. Caicedo, 47 F.3d 370, 373 (9th Cir. 1995) (noting that "trafficking in controlled substances aboard vessels is a serious international problem and is universally

evidence that these crimes have risen to the level of peremptory norms and thus invoke universal jurisdiction.[256]

2. *Applying Universal Jurisdiction to Computer Viruses*

While there is worldwide recognition of universal jurisdiction, computer viruses do not rise to the level of a violation of a peremptory norm, so they do not invoke universal jurisdiction.[257] Peremptory norms only apply to heinous crimes that all civilized nations revile.[258] Moreover, computer crimes do not even rise to the level of terrorism, much less to the level of a peremptory norm.[259] Therefore, universal jurisdiction is not applicable to computer crimes.[260]

E. Summary

The United States' exercise of jurisdiction over an alien acting abroad is consistent with international law when the alien releases a virus that has substantial effects within the United States or that targets the U.S. government.[261] The effects principle is widely accepted and applies to computer viruses that cause substantial damage in the United States.[262] In addition, the protective principle is applicable to viruses that specifically target the U.S. government.[263] However, passive personality is less widely accepted than the

condemned" (quoting 46 U.S.C. app. § 1902 (1986))); United States v. Martinez-Hidalgo, 993 F.2d 1052, 1056 (3d Cir. 1993) (noting that "the trafficking of narcotics is condemned universally by law-abiding nations").

[255] *See* United States v. bin Laden, 92 F. Supp. 2d 189, 196 (S.D.N.Y. 2000) (highlighting "certain acts of terrorism" as means of tying case to universal jurisdiction); Flatow v. Islamic Republic of Iran, 999 F. Supp. 1, 14 (D.D.C. 1998) (stating that "international terrorism is subject to universal jurisdiction").

[256] *See supra* notes 65-66 and accompanying text (explaining peremptory norms).

[257] *See infra* notes 258-59 and accompanying text (concluding that releasing computer viruses does not violate peremptory norm).

[258] *See supra* notes 65-68 and accompanying text (noting nature of activity necessary to create peremptory norm).

[259] *See supra* notes 217-18 and accompanying text (arguing that viruses do not rise to level of terrorist activity).

[260] Universal jurisdiction is only applicable to peremptory norms. *See supra* note 237 and accompanying text (explaining limitations on universal jurisdiction).

[261] *See supra* notes 140-45, 188-94 and accompanying text (explaining that effects and protective principles cover computer viruses).

[262] *See supra* notes 140-45 and accompanying text (noting that effects principle applies to computer viruses).

[263] *See supra* text accompanying notes 188-94 (determining that protective principle is

effects and protective principles, and it is unlikely that a virus could effectively target U.S. citizens based on their nationality.[264] Finally, universal jurisdiction does not apply to computer viruses because they are not a peremptory norm.[265]

IV. Applying the Computer Crime Statute Extraterritorially

Although international law allows the United States to prescribe laws that prohibit aliens from releasing viruses,[266] two questions remain unanswered. The first question is whether or not extraterritorial jurisdiction meets the requirement of reasonableness and international comity.[267] The second question is whether or not Congress intended the 1994 Act to function extraterritorially.[268]

A. Reasonableness and Comity

After a court determines that the jurisdiction to prescribe exists, it must determine whether or not the exercise of jurisdiction is reasonable.[269] Even though the Supreme Court at times has chosen to ignore the reasonableness test,[270] as formulated in the Restatement,[271] international comity still requires that a state balance its interests against the interests of other countries.[272] The United States should balance its interests against the country where the virus

applicable to computer viruses).

[264] *See supra* text accompanying notes 229-34 (arguing that passive personality is ill-suited to dealing with computer viruses).

[265] *See supra* text accompanying notes 257-60 (explaining that computer viruses do not invoke universal jurisdiction).

[266] *See supra* note 261 and accompanying text (arguing that United States may exercise jurisdiction over alien who releases viruses affecting country or government).

[267] *See infra* Part IV.A (exploring reasonableness of extraterritorial jurisdiction for computer viruses).

[268] *See infra* Part IV.B (explaining that Congress intended 1994 Act to apply extraterritorially).

[269] *See infra* notes 270-74 and accompanying text (noting reasons why reasonableness and international comity are important).

[270] *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 799 (1993) (determining that international comity was irrelevant to antitrust action).

[271] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(1) (1987) (requiring that exercise of extraterritorial jurisdiction be reasonable).

[272] *See* BROWNLIE, *supra* note 49, at 29-30 (noting that comity is act of politeness toward other nations).

originates[273] and also against other countries that feel a significant effect from the virus.[274]

In many situations in which a state exercises extraterritorial jurisdiction, more than one state has the jurisdiction to prescribe.[275] Comity and reasonableness require states to balance their interests against the interests of other states.[276] Determining whether or not jurisdiction is reasonable requires the court to weigh the interests of the United States against the interests of any other country that could prescribe laws governing the same conduct.[277]

The first step is for the United States to weigh its interests against the interests of the country from which the virus originated.[278] If the originating country does not have laws that prohibit computer viruses, then no conflict between the United States and the originating country will take place.[279] Although a conflict would exist if prosecution was unforeseeable, or if the laws of the originating state and the United States could not both be satisfied, neither of these possibilities exists in the case of a computer virus.[280]

States have a right to protect their citizens from unforeseeable prosecution in foreign states.[281] However, the rapid spread of a computer virus is foreseeable to its creator, especially if the virus propagates quickly by design.[282] Thus, after Melissa and iloveyou, a virus writer cannot claim ignorance of the potential effects and damages caused by computer viruses,

[273] The country in which the virus originates has jurisdiction under the territoriality and possibly nationality principles. *See supra* notes 71-74 and accompanying text (explaining nationality and territoriality principles).

[274] If the United States can base jurisdiction on effects within the United States, then other countries can similarly base jurisdiction on effects within their countries. *See supra* notes 128-37 and accompanying text (discussing use of effects principle by Canada and United Kingdom).

[275] *See* JENNINGS & WATTS, *supra* note 50, at 463 (noting circumstances under which multiple states have jurisdiction).

[276] RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2) (1987) (stating that states must evaluate relevant factors).

[277] *See id.* (listing factors to be weighed in determining reasonableness).

[278] *See supra* note 273 and accompanying text (arguing that United States should balance its interest against those of country where virus originates).

[279] *See infra* notes 280-90 and accompanying text (noting that because there is no conflict of laws or foreseeability issue, there is no comity issue).

[280] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2)(a), (g), and (h) (1987) (stating that conflicting laws and foreseeability are issues when determining reasonableness).

[281] *See* United States v. bin Laden, 92 F. Supp. 2d 189, 218 (S.D.N.Y. 2000) (stating that people have right to fair warning that conduct is proscribed).

[282] *See supra* notes 4, 11 and accompanying text (explaining rapid spread of Melissa and iloveyou viruses).

especially those that exploit security holes in popular computer software.[283] Furthermore, the global nature of the Internet makes the rapid distribution of a virus to the United States foreseeable.[284] Therefore, based on readily available information, script writers are well aware of the potential for causing substantial damage in the United States, regardless of where they release the virus.[285] Moreover, it is not unforeseeable that the United States will try to prosecute the people who release these viruses.[286]

The U.S. prohibition on releasing computer viruses that affect U.S. computers does not conflict with the laws of other states.[287] In order for a conflict to arise, it would be necessary that a person could not obey both the laws of the originating country and the laws of the United States.[288] Therefore, in the case of a computer virus, that would mean that the laws of the originating country would require the perpetrator to release a virus. A law requiring people to release computer viruses is illogical.[289] Thus, no conflict of laws arises from computer viruses.[290]

The second step in determining if an exercise of jurisdiction is reasonable is for the United States to weigh its interests against the interests of other affected countries.[291] There are three ways in which the United States could exert jurisdiction extraterritorially if other countries feel the effects. The United States could exercise jurisdiction if it was specifically targeted, if it was the most substantially affected, or if it exercises concurrent jurisdiction.[292]

[283] *See* Chien & Ewell, *supra* note 9 (noting how iloveyou propagated rapidly by exploiting security flaws); Elnitiarta, *supra* note 2 (detailing how Melissa spread rapidly by exploiting security hole in Microsoft Outlook).

[284] *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 471 (1997) (noting that "[b]its of information . . . flow effortlessly around the globe, rendering the traditional concept of distance meaningless").

[285] *See supra* notes 1-20 (explaining damages caused by Melissa and iloveyou viruses).

[286] *See* Ackermann, *supra* note 14, at 107 (noting rapid capture of David Smith and charges against Smith in connection with release of Melissa).

[287] *See infra* text accompanying notes 288-90 (determining that computer virus laws do not create conflict with laws of other states).

[288] *See* United States v. bin Laden, 92 F. Supp. 2d 189, 197 (S.D.N.Y. 2000) (noting that conflict of laws arises only if laws are incompatible).

[289] A law requiring people to spread computer viruses would be ineffectual in less developed countries due to a lack of computers and would be contrary to the interests of developed nations that rely on computers.

[290] *See supra* notes 288-89 and accompanying text (maintaining that U.S. computer virus laws do not conflict with laws of other states).

[291] *See supra* note 274 and accompanying text (arguing that United States should balance its interests against those of other countries affected by virus).

[292] *See infra* notes 293-306 and accompanying text (detailing methods of exerting

The United States has a right to protect itself[293] and its citizens from harm.[294] Moreover, the United States has a greater interest in preserving U.S. government facilities and protecting U.S. citizens than other countries have; thus, it is reasonable for the United States to prescribe laws for its own protection.[295] Therefore, if a virus targets the U.S. government or U.S. citizens, then it is reasonable for the United States to exert jurisdiction over the person who released the virus even if the virus affects other states.[296]

Similarly, the United States can exert jurisdiction because it incurs a greater cost from computer viruses than does any other country.[297] As the largest user of the Internet and the country most dependent on computers, the United States bears a disproportionate share of the costs associated with computer viruses.[298] Therefore, the huge disparity in Internet users between the United States and any other country justifies the United States in exerting jurisdiction over computer viruses because the United States is disproportionately harmed.[299]

A final method for dealing with international comity is concurrent jurisdiction.[300] It is not unreasonable for multiple jurisdictions to prescribe laws affecting the same conduct.[301] In almost any case that involves extraterritorial jurisdiction, multiple states will have jurisdiction to prosecute.[302] The

extraterritorial jurisdiction in situations in which other states also have jurisdiction).

[293] *See* JENNINGS & WATTS, *supra* note 50, at 416-27 (summarizing states' rights to self-preservation and self defense).

[294] *See supra* notes 198-99 and accompanying text (explaining use of passive personality to protect citizens from harm).

[295] *See* Dickinson, *supra* note 178, at 552 (noting "inadequacy of most national legislation [in] punishing offenses committed within the territory against the security, integrity and independence of foreign States").

[296] *See supra* text accompanying notes 188-94 (arguing that United States has jurisdiction if virus specifically targets United States).

[297] *See infra* note 298 and accompanying text (noting disproportionate harm from computer viruses).

[298] The United States has approximately 50% of all Internet hosts and less than 5% of the world population. *Compare supra* note 145 (noting percentage of Internet hosts located in United States) *with* THE WORLD ALMANAC AND BOOK OF FACTS 2002, at 867 (2002) (stating U.S. population at 278,058,881 and world population at 6,157,000,000).

[299] *See supra* note 298 and accompanying text (explaining disproportionate impact of computer viruses on United States).

[300] *See infra* notes 301-06 and accompanying text (detailing concurrent jurisdiction).

[301] *See infra* notes 302-05 and accompanying text (noting use of concurrent jurisdiction in international law).

[302] By its very name, extraterritorial jurisdiction refers to jurisdiction that is not based on where the action occurred. Because most jurisdiction is territorial, both the state in which the action took place and the state invoking extraterritorial jurisdiction can have jurisdiction to

country acting extraterritorially will have jurisdiction and either the country in which the activity occurred[303] or the country of citizenship of the perpetrator,[304] or both, will have jurisdiction. Moreover, international law allows for concurrent jurisdiction.[305] Thus, the United States and other countries may each exercise jurisdiction over the same offense.[306]

Therefore, it is reasonable for the United States to exert jurisdiction over aliens who release viruses that cause significant damage to the United States.[307] No issue of comity between the United States and the country where the virus originated results if the originating country does not have appropriate computer crime laws.[308] Similarly, if the virus targets or disproportionately affects the United States, no issue of comity between the United States and other affected states results.[309]

B. Applying the 1994 Act Extraterritorially

The United States has the authority to exert jurisdiction over computer viruses extraterritorially,[310] but the question is whether Congress intended for the 1994 Act to apply extraterritorially. Not all laws act extraterritorially.[311]

prescribe. *See supra* notes 71, 73 and accompanying text (explaining territorial jurisdiction).

[303] *See supra* notes 71, 73 and accompanying text (outlining principle of territoriality).

[304] *See supra* notes 72, 74 and accompanying text (stating how nationality principle operates).

[305] *See* S.S. Lotus, (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 9, at 30-31 (Sept. 7, 1927) (explaining that France and Turkey had concurrent jurisdiction over acts of French officer); Libman v. The Queen, [1985] 2 S.C.R. 178, 212 (deciding that although possibility of being tried in multiple jurisdictions exists, "any injustice that might result from this eventuality could be avoided by resort to the pleas of *autrefois acquit* and *autrefois convict*, which have been applied to persons tried in other countries"); United States v. bin Laden, 92 F. Supp. 2d 189, 214 (S.D.N.Y. 2000) (noting that "concurrent jurisdiction is permitted by international law").

[306] *See supra* notes 300-05 and accompanying text (explaining legitimacy of concurrent jurisdiction).

[307] *See supra* notes 287-306 and accompanying text (arguing that it is reasonable for United States to use extraterritorial jurisdiction in computer virus cases).

[308] *See supra* notes 287-90 and accompanying text (stating that there is no conflict of laws issue in computer virus cases).

[309] *See supra* notes 291-306 and accompanying text (determining that United States assertion of extraterritorial jurisdiction in virus cases does not offend international comity in respect to other affected countries if United States is targeted or disproportionately affected).

[310] *See* EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991) (stating that "Congress has the authority to enforce its laws beyond the territorial boundaries of the United States"); *see also supra* Part III (detailing applicability of various bases of jurisdiction to computer viruses); *supra* notes 281-309 (explaining reasonableness of assertion of jurisdiction by United States).

[311] *See* Sale v. Haitian Ctrs. Council, Inc., 509 U.S. 155, 188 (1993) (maintaining that "Acts of Congress normally do not have extraterritorial application").

Therefore, for a law to function outside of the United States, Congress must intend for it to do so.[312]

The 1994 Act does not specifically mention the extraterritorial effect.[313] The general rule when a statute makes no explicit mention of extraterritorial effect is to look at the "text, structure, and legislative history" of the act.[314] However, an exception to this rule for criminal offenses that are as easy to commit abroad as they are to commit within the United States exists.[315] Because of the widespread use of the Internet, computer crimes commonly cross national boundaries.[316] If fraud,[317] racketeering,[318] distribution of narcotics,[319] and theft of U.S. property,[320] all of which normally involve physical elements, have extraterritorial effect, then computer crime laws, which are generally nonphysical and do not rely on the proximity between the perpetrator and the victim, should apply extraterritorially.[321]

Even if computer crimes do not fall within the exception, the 1994 Act still operates extraterritorially because the text of the statute prohibits transmission of data that would advantage a foreign nation.[322] If data residing in the United States is going to advantage a foreign nation, some action will most likely occur outside of the United States.[323] The explicit mention of a foreign nation within the statute is strong evidence of the extraterritorial reach of the

[312] *See* United States v. bin Laden, 92 F. Supp. 2d 189, 193 (S.D.N.Y. 2000) (noting that "[i]t is equally well-established . . . that courts are to presume that Congress has not exercised [extraterritorial] power . . . unless Congress manifests an intent to reach acts performed outside United States territory").

[313] *See* 18 U.S.C. § 1030 (1994) (failing to mention territorial boundaries of statute).

[314] *bin Laden*, 92 F. Supp. 2d at 193.

[315] *See* United States v. Bowman, 260 U.S. 94, 98 (1922) (stating that there is limited exception for "criminal statutes which are, as a class, not logically dependent on their locality").

[316] *See* Landler, *supra* note 8, at C1 (explaining that iloveyou virus rapidly spread worldwide).

[317] *See Bowman*, 260 U.S. at 102 (giving extraterritorial effect to fraud statute).

[318] *See* United States v. Vasquez-Velasco, 15 F.3d 833, 839-41 (9th Cir. 1994) (determining that jurisdiction over violent crimes in aid of racketeering applies extraterritorially).

[319] *See* United States v. Larsen, 952 F.2d 1099, 1101 (9th Cir. 1991) (stating that narcotics law applies extraterritorially).

[320] *See* United States v. Benitez, 741 F.2d 1312, 1317 (11th Cir. 1984) (allowing extraterritorial application to statute criminalizing theft of United States property).

[321] *See supra* note 146 and accompanying text (noting non-physical nature of computer crimes).

[322] *See* 18 U.S.C. § 1030(a)(1) (1994) (criminalizing transmission of data that "could be used . . . to the advantage of any foreign nation").

[323] The data must get from the United States to the foreign government in order to advantage the foreign government, and it is likely that some or all of that activity will occur outside of the United States.

statute. In addition, the statute mentions interstate and foreign communication.[324] If a foreign communication is intercepted in violation of the statute, then it is likely that the underlying criminal activity occurred abroad, which is further evidence that the authors of the 1994 Act intended it to apply extraterritorially. Therefore, the text of the 1994 Act supports an extraterritorial interpretation.[325]

In addition to the text, the history of the statute indicates that it acts extraterritorially.[326] A government survey of businesses showed that over fifty percent of respondents identified foreign competitors as potential computer intruders and twenty-two percent identified foreign governments as potential computer intruders.[327] Furthermore, the news media hyped the danger posed by hackers both inside and outside the United States.[328] Ample evidence exists that the public and Congress had concerns in the early 1990s about computer crimes that originated outside the United States.[329]

In summary, it is as easy to commit a computer crime from outside the United States as from within, thus the 1994 Act is extraterritorial because it prohibits activities that fall within an exception to the normal rules of interpretation.[330] Even if the 1994 Act does not fall within that exception, the text and history of the 1994 Act support the conclusion that Congress meant the 1994 Act to apply extraterritorially.[331] Therefore, Congress must have enacted the 1994 Act with the intent to prosecute both domestic and foreign offenders because computer crimes are so easily perpetrated from abroad.

[324] *See* 18 U.S.C. § 1030(a)(2)(C) (1994) (stating that conduct is illegal if it "involved an interstate or foreign communication"); *id.* § 1030(a)(7) (explaining that transmission through foreign commerce of threat to damage computer violates Act).

[325] *See supra* notes 322-24 and accompanying text (determining that text of statute supports extraterritorial application).

[326] *See infra* notes 327-28 and accompanying text (noting that history of statute supports extraterritorial application).

[327] *See* Hedieh Nasheri & Timothy J. O'Hearn, *Crime and Technology: New Rules in a New World*, 34 CRIM. L. BULL. 520, 524 (1998) (citing survey administered by Computer Security Institute).

[328] *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 107 (1988) (stating that "during the late summer and fall of 1983, the media began to fixate on the prospect of young computer hackers creating international mayhem"); *see generally* STOLL, *supra* note 5 (chronicling activities of German hackers in 1987 who attacked some four hundred military computers).

[329] *See supra* notes 327-28 and accompanying text (detailing historical factors that support extraterritorial application of 1994 Act).

[330] *See supra* note 315 and accompanying text (noting exception to general rule of interpretation).

[331] *See supra* notes 322-29 and accompanying text (explaining that text and history of 1994 Act support extraterritorial application).

V. Conclusion

Computer viruses threaten our increasingly technological society.[332] Traditionally, the United States recognized jurisdiction based solely on the territorial principle.[333] However, expansion of the U.S. view on jurisdiction over the last one hundred years has allowed U.S. laws to reach activities committed by aliens while they are outside of the United States.[334] Moreover, the rest of the world now accepts the view that laws are not strictly territorial.[335] In addition, widespread use of the effects and protective principles validate their use under international law.[336]

The 1994 Act prohibits computer crimes that affect the United States, regardless of the nationality or residence of the perpetrator.[337] Because of the nature of computer viruses and the substantial effect they have on the United States, it is reasonable for the United States to exert jurisdiction over persons who release computer viruses that have a substantial effect in the United States or that target an instrumentality of the U.S. government.[338] However, the United States is limited to cases in which the perpetrator acted from a country without appropriate computer crime laws.[339] Computer criminals can no longer use states without effective computer crime laws as modern-day hideouts to avoid prosecution.

[332] *See* Lacter, *supra* note 217, at 46 (noting damages caused by computer viruses); *supra* notes 16, 20 and accompanying text (estimating damages from Melissa and iloveyou at $80 million and $10 billion respectively).

[333] *See* BROWNLIE, *supra* note 49, at 300 (stating that "English and American decisions . . . suggest that the territorial principle is exclusive").

[334] *See* RESTATEMENT (THIRD) FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (1987) (detailing alternative bases for jurisdiction to prescribe).

[335] *See supra* Part III (outlining international acceptance of various extraterritorial bases of jurisdiction to prescribe).

[336] *See supra* Part III.A-B (noting general acceptance of effects and protective principles).

[337] *See supra* Part IV.B (arguing that 1994 Act applies extraterritorially).

[338] *See supra* Part IV.A (explaining that extraterritorial jurisdiction is reasonable in virus cases).

[339] *See supra* note 279 and accompanying text (noting that there is no conflict of laws in such situations).