

HOT TOPICS ON THE INTERNET
February 28, 2001

TABLE OF CONTENTS

- I. TABLE OF CONTENTS**
- II. PERSONAL JURISDICTION THROUGH THE INTERNET**
- III. E-MAIL, ATTORNEY-CLIENT PRIVILEGE AND THE ETHICAL DUTY OF CONFIDENTIALITY**
- IV. PRIVACY**
- V. ONLINE CONTRACTING**
- VI. VIRGINIA AND FEDERAL COMPUTER CRIMES: SENTENCING ADULTS AND JUVENILES**
- VII. APPENDIX**
 - A. VIRGINIA CODE § 8.01-328.1**
 - B. LEGAL ETHICS IN CYBERSPACE**
 - C. HOW THE INTERNET WORKS**
 - D. GUIDE TO INTERNET RESEARCH**

PERSONAL JURISDICTION THROUGH THE INTERNET

I. INTRODUCTION

The area of law surrounding Internet jurisdiction is presently evolving. No case has reached the Supreme Court, nor has any state supreme court conclusively decided this issue. Therefore, this body of law is severely disjointed. Judges appear to have wide latitude in examining these jurisdictional issues. Likewise, attorneys have the ability to present courts with novel and creative arguments when representing a client, be it a huge Internet conglomerate protecting a trademark or an individual attempting to exercise their First Amendment rights. For the most part, courts appear to fall in one of two camps. The first camp asserts that Internet-related issues are no different than other more traditional subjects, thus they attempt to examine these questions under the previously structured doctrines. Conversely, the second camp argues that the Internet is a unique tool that cannot be effectively captured by out-dated doctrines. This section will examine these two opposing frameworks, and discuss both the actual and potential impact on Virginia law.

II. BACKGROUND

A. THE DUE PROCESS CLAUSE AND LONG-ARM STATUTES

In examining personal jurisdiction, whether in state or federal court, the test is the same. First, the court in the forum must examine that state's long-arm statute. Assuming the requirements of the long-arm statute are met, then the court turns to the Due Process Clause.¹ Due process mandates that jurisdiction may only be appropriately exercised when: (1) the defendant has "minimum contacts" with the forum; and (2) exercising jurisdiction "does not offend traditional notions of fair play and justice."² Under this test, the Due Process Clause precludes a court from exercising jurisdiction over a party unless the party's conduct and connection to the forum is such that it should "reasonably anticipate being haled into court there."³ Therefore, the "constitutional touchstone" has always been "whether the defendant purposefully established minimum contacts in the forum state."⁴

Courts have the ability to assert either general or specific personal jurisdiction. General jurisdiction is proper only when the defendant has engaged in continuous and systematic activity in the forum state.⁵ If general jurisdiction is appropriate, the defendant is amenable to all causes of action, even actions unrelated to the defendant's forum-related contacts. Conversely, specific

¹ In most cases involving jurisdictional questions the Fourteenth Amendment controls. Yet, when a case is in federal court, on federal question grounds, then the Fifth Amendment controls. Regardless, the analyses are the same. The only narrow exception is when a federal statute authorizes "nationwide" jurisdiction. These statutes have been found to comply with the Due Process Clause of the Fifth Amendment, irrespective of the forum state's long-arm statute.

² *International Shoe v. Washington*, 326 U.S. 310, 316 (1945).

³ *World-Wide Volkswagen v. Woodson*, 444 U.S. 286, 297 (1980).

⁴ *Burger King v. Rudzewicz*, 471 U.S. 462, 474 (1985).

⁵ *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 414 (1984).

jurisdiction is warranted only if the cause of action arises from, or relates to, the defendant's "minimum contacts" with the forum state.

B. GENERAL JURISDICTION

General jurisdiction requires that the defendant continuously and systematically pursue general business activities in the forum state.⁶ General jurisdiction does not mandate relatedness to the underlying claim, but it does require the defendant's contacts with the forum state be more extensive than the 'minimum contacts' requirement of specific jurisdiction. The requirements for general jurisdiction are far more stringent than those for specific jurisdiction. While physical presence in the jurisdiction is not a bright-line requirement for general jurisdiction, courts do require that the defendant's contacts approximate physical presence.

C. SPECIFIC JURISDICTION

A three-part test governs the exercise of specific jurisdiction. Under this test, a court may only exercise specific jurisdiction if (1) the defendant purposefully avails himself of the privileges of doing business in the forum, (2) the claim arises out of or results from the defendant's forum related activity and (3) the exercise of jurisdiction is reasonable.⁷ The plaintiff must establish all three requirements.

III. COMPETING FRAMEWORKS

A. "SLIDING SCALE"

The "sliding scale" model is the most widely used test for Internet jurisdiction. Under this "sliding scale" approach first articulated in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, whether jurisdiction can be constitutionally exercised is "directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."⁸ The "sliding scale" consists of three categories of websites: (1) interactive websites that are used to conduct business over the Internet; (2) semi-interactive websites that allow for the exchange of information with a host computer; and (3) passive websites through which it is not possible to exchange information with the host computer.⁹ Under this approach, exercise of personal jurisdiction is always appropriate for interactive websites, but never appropriate for passive websites.¹⁰ Semi-interactive websites, which encompass a large majority of all Internet websites, require a balancing approach that looks at the degree of interactivity and the commercial nature of the site.¹¹

⁶ *Perkins v. Benguet Consol. Mining Co.*, 342 U.S. 437, 448 (1952).

⁷ *Burger King*, 471 U.S. at 463.

⁸ 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

⁹ *Amberson Holdings LLC v. Westside Story Newspaper*, 110 F.Supp.2d 332, 336 (D.N.J. 2000).

¹⁰ *Mink v. AAAA Development, LLC*, 190 F.3d 333, 336 (5th Cir. 1999); *Cybersell, Inc. v. Cybersell Inc.*, 130 F.3d 414, 419 (9th Cir. 1997).

¹¹ *Mink*, 190 F.3d at 336.

B. COMMERCIAL TRANSACTION TEST

Under the “commercial transaction” framework, exercising jurisdiction is only proper when the Internet activity results in commercial activity within the forum. Courts adopting this model state that while the “sliding scale” model is effective in dealing with interactive and passive sites, it is not useful in examining semi-interactive websites. “[A]pplication of the *Zippo Manufacturing* framework provides no clear answer to the jurisdictional question.”¹² From this dissatisfaction has grown a second line of cases that either explicitly or implicitly reject the “sliding scale” interactivity framework.¹³

These cases have eschewed “sliding scale” for what they assert is a more traditional approach in line with Supreme Court precedent and traditional notions of personal jurisdiction. Instead of focusing on the degree of interactivity, these courts have concentrated on “the degree to which the defendant actually used its web site to conduct commercial or other activity with the forum residents.”¹⁴ In sum, these courts assert that the “sliding scale” is not an effective doctrine, because it is out of line with the Supreme Court personal jurisdiction precedent and traditional notions of due process. As a District of South Carolina court stated in *ESAB Group*:

Merely categorizing a web site as interactive or passive is not conclusive of the jurisdictional issue. General in personam jurisdiction must be based on more than the defendant’s mere presence on the Internet even if it is an “Interactive” presence. Rather, the critical issue for the court to analyze is the nature and quality of commercial activity actually conducted by an entity over the Internet in a forum state.¹⁵

This alternate rule, focusing on actual commercial activity rather than interaction, claims to be more consistent with the traditional rule that mere access and interaction do not confer general jurisdiction. By analogy, these courts argue that under traditional general jurisdiction precedent, placing a store or salesperson in a given state does not confer general jurisdiction unless there is sufficient evidence that the store or salesperson “actually generated sufficient sales in the forum state to be considered continuous and systematic” contact.¹⁶ While the number of times a site has been accessed is relevant under this analysis, the most important factor is the number of sales generated through the website in the forum state.¹⁷ These courts claim that this framework, unlike the “sliding scale,” is in line with the Supreme Court’s explicit directive to exercise jurisdiction where there is “deliberative contact” between the resident and the forum state.¹⁸

Several Circuit Courts of Appeal, including the Second, Fifth, Sixth and Ninth, have adopted the “sliding scale” framework. Conversely, the Court of Appeals for the District of Columbia has not, but rather implicitly endorsed the “commercial transactions” framework. The

¹² *Dagesse v. Plant Hotel*, 113 F. Supp. 2d 211, 222 (D.N.H. 2000).

¹³ *See Dagesse*, 113 F. Supp. 2d at 222; *ESAB Group, Inc. v. Centricut, LLC*, 34 F. Supp. 2d 323 (D.S.C. 1999).

¹⁴ *Dagesse*, 113 F. Supp. 2d at 222.

¹⁵ 34 F. Supp. 2d at 330-331.

¹⁶ *Coastal Video Communications Corp. v. Staywell Corp.*, 59 F. Supp. 2d 562, 571-72 (E.D. Va. 1999).

¹⁷ *Id.* at 572.

¹⁸ *Winfield Collection, Ltd. v. McCauley*, 105 F. Supp. 2d 746, 750 (E.D. Mich. 2000).

Fourth Circuit Court of Appeals has not yet addressed this issue. Likewise, no Virginia state court has addressed Internet-related jurisdiction. The only Virginia court to address this new issue is the Eastern District of Virginia. Cases from the Eastern District will be examined in the sections that follow.

IV. INTERNET JURISDICTION IN VIRGINIA

A. THE LONG-ARM STATUTE

The Virginia Long-arm statute, codified in section 8.01-328.1 of the Virginia Code sets forth several bases for exercising jurisdiction for a non-resident defendant. This pertinent sections of this statute can be found in the Appendix to this section. Section 8.01-328.1(A) allows a court to exercise jurisdiction “over a person, who acts directly or by agent, as to a cause of a action arising from the person’s:” (1) transacting of business in the Commonwealth; (2) contracting to supply services or things in the Commonwealth; (3) causing, either by act or omission, a tortious injury in the Commonwealth; (4) causing tortious injury, by act or omission outside the Commonwealth, as long as the person regularly conducts business, or other activities within the Commonwealth; (5) causing injury through breach of warranty; (6) having an interest in, using, or possessing real property in the Commonwealth; (7) contracting to insure person, property or risk within the Commonwealth; (8) matrimonial and child responsibility related obligations within the Commonwealth and (9) having a matrimonial instate residence.

Until July of 2000, these provisions served as the sole basis for review of Virginia personal jurisdiction statutory provisions. However, the statute was amended and section 8.01-328.1(B) was added to the section. Section B states that, “[u]sing a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth. For purposes of this subsection, “use” and “computer network” shall have the same meanings as those contained in section 18.2-152.2.

B. RECENT VIRGINIA CASES

No court has published a decision construing the newly amended provision of the statute. However, prior to the July 2000 amendment, several courts, analyzed this statute in its traditional sense, as well in the context of the Internet.

The Virginia Supreme Court has consistently held that the Virginia Long-Arm Statute extends personal jurisdiction over non-residents “to the extent permissible under the due process clause.”¹⁹ However, it is still possible for a defendant’s contacts to satisfy the due process clause, yet fall outside the scope of one of the provisions of the statute.²⁰ Therefore, in every case involving the Virginia Long-Arm Statute the statutory analysis must precede any constitutional inquiry.

In terms of Internet-related jurisdiction, as noted above, neither the Virginia courts nor the Fourth Circuit Court of Appeals has addressed the issue. However, the Eastern District of

¹⁹ Kolbe v. Chromodern Chair Co., 211 Va. 736, 740 (1971).

²⁰ See TELCO Communications v. An Apple A Day, 977 F. Supp. 404, 405 (E.D. Va. 1997).

Virginia has addressed Internet jurisdiction on several occasions, with varying results. Again, no Virginia court, either state or federal, has addressed section B of the statute subject since its adoption. This amendment will prove crucial to any future analysis.

In several recent cases, Eastern District courts have adopted the “sliding scale” model.²¹ Most recently, Judge Ellis reaffirmed the “sliding scale” model, finding that an Internet gambling website “conducted business” in Virginia by contracting on the Internet with several Virginia residents.²² Conversely, in *Roche*, Judge Lee held that while the “sliding scale” model was the appropriate approach, the defendant’s website was essentially passive and therefore was not sufficient to confer jurisdiction.²³ In *Roche*, the defendant operated a pornographic website. They did not sell products in Virginia, had no employees in the Commonwealth and directed no advertisements or promotional activities at Virginia residents specifically.²⁴ Last, in *Weinstein*, the court applied the “sliding scale” model, but also refused to exercise jurisdiction over the defendant. The defendant’s Internet activity was an advertisement placed on a website called “BoatTrader.com.”²⁵ The court ruled this fell into the “passive” category and therefore found exercising jurisdiction inappropriate.²⁶

As opposed to the cases above, the court in *Coastal Video Communications Corp. v. Staywell Corp.* only partially adopted the “sliding scale” model. While the court found it satisfactory in the context of specific jurisdiction, it found the approach unacceptable in the general jurisdiction context. The court stated that in examining contacts in terms of general jurisdiction, “there must be an examination of the quantity and nature of the Internet-based contacts with the forum, a step that is not adequately reflected in the *Zippo Mfg.* analysis.”²⁷

V. EMERGING ISSUES IN VIRGINIA

This brings the question back to the amended provision of the Virginia Long-Arm Statute. This provision clearly allows for courts to exercise Internet-related jurisdiction much more frequently. Virginia has quickly become the haven to the Internet and computer community, second only to California. Most notably, America On-Line is now headquartered here. Thus, a significant majority of all Internet use in the country is routed through Internet servers within the Commonwealth. By stating that using a “computer network” constitutes an act in the forum, Virginia may have opened the floodgates of jurisdiction.

²¹ See *Roche v. Worldwide Media, Inc.*, 90 F. Supp. 2d 714 (E.D. Va. 2000); *Weinstein v. Todd Marine Enterprises, Inc.*, 115 F. Supp. 2d 668 (E.D. Va. 2000). It should be noted that in 1997, in *TELCO Communications, Inc. v. An Apple A Day*, the Eastern District of Virginia held that merely maintaining an Internet website allows a court to exercise jurisdiction. 977 F. Supp. 404, 405. However, no Virginia court has followed this approach that is more liberal than both the “sliding scale” and “commercial transaction” frameworks. The court followed the lead of the court in *Inset Systems, Inc. v. Instruction Set*, 937 F. Supp. 161 (D. Conn. 1996). Again, this line of reasoning has been largely abandoned because it does not take into account the “purposeful availment” requirement of the Supreme Court’s due process jurisprudence.

²² *Alitalia-Linee Aeree Italiane v. Casinoalitalia.Com*, 2001 WL 62870, --- F. Supp. 2d --- (E.D. Va. Jan. 19, 2001).

²³ 90 F. Supp. 2d at 718.

²⁴ *Id.*

²⁵ 115 F. Supp. 2d at 674.

²⁶ *Id.*

²⁷ *Id.* at 571.

However, this raises an important question: does the amended statute surpass its constitutional limitations? Can simply using a “computer” or “computer network” in Virginia meet the “minimum contacts” test set forth by the Supreme Court? Does it constitute “purposeful availment” or “continuous and systematic business relations?” Last, will it make Virginia the “forum” of choice for those seeking jurisdiction based on Internet activity? These questions are likely to be answered in the months and years ahead, with the results having a significant impact on both business activity and consumer use of the Internet.

***E-MAIL, ATTORNEY-CLIENT PRIVILEGE
AND THE ETHICAL DUTY OF CONFIDENTIALITY***

The attorney-client privilege protects communication between a client and his attorney relating to the attorney's rendering of legal advice when that communication is made with the expectation of confidentiality.²⁸ The attorney-client privilege can be waived through either intentional or negligent disclosure of the privileged communication.²⁹ In addition, attorneys have an ethical duty of confidentiality with regard to client communications. Technological advances in methods of communication require legal professionals to determine whether the new methods are private and confidential enough to establish and maintain the attorney-client privilege and to satisfy the ethical duty of confidentiality.

Email is similar to both regular ("snail") mail and to telephone communications. Like snail mail, email allows precise language and the transmission of "physical" documents, but like telephone communications the information is transmitted through wire lines.³⁰ Each email user has an "address" to which messages are "sent" and are accessible only to the user by use of a password.³¹ When a user decides to send an email to someone, he composes the message like a letter, addresses it and then clicks the "send" button to transmit the message. The user's computer stores the composed email and sends a copy of it, broken into small packets of information, over wire lines to a file server that sends the packets of information over wire lines to the Internet.³² Like other telecommunications transmissions, the packets of information may have to go through several routing servers before it reaches its destination. Each routing server that receives a packet stores the packet and sends a copy on its way. These copies are theoretically available to the system administrator of every file server that makes a copy.³³ Eventually, all of the packets of information are received and put together by the recipient's server, from which the recipient retrieves the message using his computer "mailbox."

A. EMAIL AND THE ATTORNEY-CLIENT PRIVILEGE

The American Bar Association, among others, has encouraged states to recognize that attorney-client email communications have the same privacy and confidentiality expectations as traditional communications means.³⁴ There is no Virginia opinion directly addressing this issue, but it is apparent that, though emails are discoverable, attorney-client email communication is accorded this privilege in Virginia.³⁵ However, the increased possibilities of interception of the

²⁸ Thomas E. Spahn, *VIRGINIA'S ATTORNEY-CLIENT PRIVILEGE AND WORK PRODUCT DOCTRINE*, 4th ed. (1999)

²⁹ *Id.*

³⁰ Sherry L. Talton, *Mapping the Information Superhighway: Electronic Mail and the Inadvertent Disclosure of Confidential Information*, 20 REV. LITIG. 271 (2000).

³¹ *Id.*

³² *Id.*

³³ One commentator has analogized this "store and forward" technology as being similar to "a postcard that might be getting xeroxed in every post office it might pass through." See *Electronic Mail as Private Billboard on the Road: There Isn't Much Protection for Email and People are Finding Out They're Responsible for What They Send*, THE PLAIN DEALER, May 13, 1996, at 5D.

³⁴ ABA Rec. 98A119A (August 4, 1998).

³⁵ See *Gordon v. City of Richmond*, 51 Va. Cir. 183 (2000) (holding that the attorney-client privilege applied to several documents, including emails).

email at various stages of transmission might undermine the privileged status of email communications.

Thus, the major issue is not whether successful communications via email between attorney and client are privileged, but rather, whether a court would find that the privilege is waived in the case of an inadvertent disclosure through an intercepted or misdirected email.³⁶ Some bar associations have indicated that if emails are not encrypted and they are intercepted or misdirected, the privilege should be considered waived.³⁷ Many commentaries suggest that attorneys and clients communicating via email take precautions to guard against a finding of waiver in the case of interception or misdirection. One suggested method is to place the sensitive message in an attached document and use the body of the email message as a cover memo indicating the confidential nature of the attachment, similar to a fax cover page.³⁸ Others include placing a similar notice of confidentiality in the email message and using encryption software to code messages.³⁹ All of these methods can guard against a finding of waiver in the case of intercepted or misdirected email.

In sum, the majority of jurisdictions accord the same privacy to email communications that are accorded to U.S. and commercial mail, landline telephone transmissions, and facsimiles. Because of the increased possibilities of interception or misdirection associated with email, attorneys and clients should take extra protections to guard against inadvertent waiver by misdirection or interception.

B. EMAIL AND THE ETHICAL DUTY OF CONFIDENTIALITY

Although Virginia does not have an ethics opinion regarding email and the ethical duty confidentiality,⁴⁰ the ABA has indicated that routine communication via unencrypted email is not a breach of the duty of confidentiality.⁴¹ Many state bars have adopted the ABA approach, but some have been more cautious.⁴² As is always the case, attorneys should “consult with the client and follow her instructions...as to the mode of transmitting highly sensitive information relating to the client’s representation.”⁴³ It is important that both attorney and client understand the security risks inherent in email communication and take precautions to guard against interception and misdirection. Simple steps like double checking the email address before sending the

³⁶ Thomas F. O’Neil III, *Detours On The Information Superhighway: The Erosion of Evidentiary Privileges In Cyberspace And Beyond*, 1997 STAN. TECH. L. REV. 3. Generally courts have held that emails, although subject to discovery, may be protected by the attorney-client privilege just as letters and other documents. *See Spahn, supra* note 1, at 151.

³⁷ *See Spahn, supra* note 1, at 151-152.

³⁸ *See*, Deborah Elkins and Dawn Chase, *Lawyers’ E-Mail: Are You Protecting Your Clients?*, 15 V.L.W. 459 (Sept. 25, 2000).

³⁹ *Id.*

⁴⁰ *See* Elkins and Chase, *supra* note 11. The Virginia State Bar does not encrypt its email.

⁴¹ Protecting the Confidentiality of Unencrypted Email, ABA Formal Op. 99-413, *available at* www.abanet.org-/cpr/fp99-413.html (stating that the use of unencrypted email does not violate the rules of professional conduct).

⁴² Bar associations following the ABA approach include: Alaska, District of Columbia, Kentucky, Illinois, North Dakota, South Carolina, Vermont. More cautious bar associations include Arizona, Iowa, North Carolina, and Pennsylvania.

⁴³ Protecting the Confidentiality of Unencrypted Email, ABA Formal OP. 99-413, *available at* www.abanet.org-/cpr/fp99-413.html.

message and including notices of confidentiality can help guard against disclosure and can insulate an attorney from malpractice claims. If the attorney and client wish to communicate via email, but are concerned about interception, the use of encryption software is advisable.

PRIVACY

Over the past few decades, use of the Internet and email has become ubiquitous both at home and at work. Coinciding with this rise in popularity has been the concern about the privacy of Internet and email users. Many users treat email as if it is the same as a telephone call or a facsimile transmission. However, email is very different. It is less secure than telephone communication, and courts have held that it is discoverable. Of particular concern has been whether an employer has the right to monitor employee emails, as well as the role of email communication in litigation settings. Two scenarios will help illustrate these concerns.

First, imagine that one day you are sitting at your desk at work when suddenly the police burst in and arrest you. You have no idea what you are being arrested for, and when you ask the arresting officers, they tell you that they have found incriminating evidence on your office computer. You were never aware that anyone had been in your office or had access to your computer files.

Next, imagine that you are the CEO of a leading technology company. Your tireless work has paid off, and your company is highly profitable and continues to put out new products. You use email to communicate with employees, spurring them on to beat the competition to the market. Subsequently, your company is sued for antitrust violations by the United States Department of Justice. Some of the key evidence of your company's anti-competitive behavior is your email messages to employees.

A. PRIVACY OF EMAIL IN THE WORKPLACE

The first scenario above is based loosely on the facts of *United States v. Simons*.⁴⁴ Mr. Simons worked for a division of the CIA. The company who provided Internet service to the division notified Simons' boss that his office computer had been used to visit numerous pornography web sites.⁴⁵ The ensuing investigation involved remotely accessing Simons' computer and copying files from the hard drive.⁴⁶ This turned up several pornographic pictures of minors.⁴⁷ Next, another employee entered Simons' office and removed his hard drive, replacing it with an exact copy.⁴⁸

Simons was indicted on charges of receiving and possessing child pornography. He challenged the warrantless searches on Fourth Amendment grounds, but the trial court and Fourth Circuit disagreed, stating that Simons had no reasonable expectation of privacy in his office computer.⁴⁹ According to the court, the CIA's Internet policy, which gave the agency the right to monitor employee Internet usage as it deemed appropriate, served to reduce Simons' legitimate expectation of privacy.⁵⁰

⁴⁴ 206 F.3d 392 (4th Cir. 2000).

⁴⁵ *Id.* at 396.

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.* at 397.

⁵⁰ *Id.* at 398.

Other courts have found that employees have no legitimate expectation of privacy in email communications sent using the employer's email system.⁵¹ The fact that users of a company's email system must enter a password to access the system has been held to be of little significance.⁵² Using strongly worded language, the Texas Court of Appeals held that email messages stored on a company computer were not the property of the employee, but rather a part of the employer's computer system.⁵³ All of these cases support the broad right of employers to access the email of employees.⁵⁴

B. USE OF EMAIL IN LITIGATION

The second scenario is based loosely on the Justice Department's antitrust case against Microsoft. Microsoft Chairman Bill Gates often communicated with employees through numerous informal email messages, many of which berated competitors and called for Microsoft to dominate the market. Microsoft's email records were subpoenaed, and many were entered into evidence against the company.⁵⁵ The informal manner in which email is often used can add to the inculpatory nature of email communications.⁵⁶

Courts have held that email messages are documents, and are proper targets of discovery.⁵⁷ Furthermore, email messages are not easily destroyed. In one recent case, the court appointed a computer expert to retrieve emails that had been deleted from a defendant's hard drive.⁵⁸ In another case, the court fined the plaintiff \$10,000 for failing to preserve email messages.⁵⁹ Finally, the cost of retrieving the subpoenaed email messages may be placed on the producing party.⁶⁰ The basic lesson to be learned from these cases is that the court will likely treat all email communications just like any other document, and clients should treat them accordingly.

⁵¹ See *Bourke v. Nissan Motor Corp., U.S.A.*, No. B068705 (Cal. Ct. App. July 26, 1993) (holding that employees had no reasonable expectation of privacy because they had signed a waiver stating that email communication must be limited to company business); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (holding that employer's use of employee's emails to his supervisor to terminate the employee was proper even though the employee had been assured that the emails would be confidential).

⁵² See *Restuccia v. Burk Tech., Inc.*, No. 95-2125, (Mass Super. Aug. 13, 1996) (holding that employees had no reasonable expectation of privacy in email communications even though they needed a password to enter the system and the employer did not have a policy restricting email use to business purposes only).

⁵³ *McLaren v. Microsoft Corp.*, no. 05-97-00824-CV (Tex. App. May 28, 1999).

⁵⁴ See generally, Comment, *Workplace E-mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741 (2000).

⁵⁵ See Brett R. Harris, *Counseling Clients over the Internet*, 629 PLI/Pat. 119, 128 (Winter, 2000).

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

⁵⁹ *Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622 (C.D. Utah, 1998), *rev'd in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000).

⁶⁰ *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 W: 360526 (N.D. Ill. 1995) (holding that the retrieval expense, which was estimated at \$50,000 to \$70,000, must be paid by the producing party); see also Harris, *supra note 12*, at 128.

C. EMAIL AND THE ATTORNEY CLIENT PRIVILEGE

Of special interest to attorneys is the treatment of email communications with clients. A recent survey by the ABA Legal Technology Resource Center revealed that 94% of attorneys surveyed use emails in their practices, and 71% of those used email to communicate with clients.⁶¹ Generally, whether or not the attorney-client privilege attaches to a given communication depends upon the protections taken to preserve confidentiality and whether a breach of that confidentiality waives the privilege.⁶² Most courts have held that email communications should be treated just like any other communication between attorneys and clients.⁶³

D. PRIVACY OF HOME INTERNET USAGE

Possibly of even greater significance is whether an Internet Service Provider (“ISP”) can be subpoenaed to provide information about one of its subscribers. This is of great significance in Virginia, as America On-Line (“AOL”), the world’s largest ISP, is headquartered in the Commonwealth. In a recent case initiated in Indiana, AOL was subpoenaed under Virginia Supreme Court Rule 4:9(c), as a “Person Not a Party.”⁶⁴ The case involved allegedly defamatory remarks made by the five defendants about the plaintiffs in AOL “chat rooms.”⁶⁵ AOL was subpoenaed to provide the identity of the five defendants.⁶⁶ AOL made a motion to quash the subpoena, claiming that it violated the First Amendment rights of the defendants.⁶⁷ The court ruled that in such a case, the ISP should only be ordered to produce the subscriber information

- (1) when the court is satisfied by the pleadings or evidence supplied to that court
- (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit is filed and
- (3) the subpoenaed identity information is centrally needed to advance that claim.⁶⁸

⁶¹ Harris, *supra note 55*, at 127.

⁶² *Id.* at 129.

⁶³ *Id.* (listing several cases which have treated email communications between attorneys and clients the same as other forms of communication).

⁶⁴ *In re Subpoena Duces Tecum to America Online, Inc.*, No. 40570, 2000 WL 1210372 (Va. Cir. Ct. January 31, 2000).

⁶⁵ *Id.* at 1.

⁶⁶ *Id.*

⁶⁷ *Id.* at 2.

⁶⁸ *Id.* at 8.

This ruling puts ISP subscribers on notice that their Internet activities are not entitled to anonymity.

ONLINE CONTRACTING

A. CLICKWRAP AGREEMENTS

In our rapidly changing world of e-commerce, websites have begun to require users to enter into “clickwrap agreements.”⁶⁹ Typically, a website operator will provide terms of agreement on a website and require the user to click on a button marked “I AGREE” before that user can proceed further on the operator’s website. It is most common to come across a clickwrap agreement prior to the purchase of a product or service from a website, or the use of a website under a license created by the agreement.

Courts generally uphold clickwrap agreements. For example, in *Hotmail Corp. v. Van\$ Money Pie Inc.*, the Northern District of California upheld Hotmail’s “Terms of Service” with which the defendants were required to agree before receiving an e-mail account from Hotmail.⁷⁰ The “Terms of Service” prohibited the use of Hotmail accounts to facilitate the transmission of spam.⁷¹ Thus, the court enjoined the defendants from using their account to generate spam.

In a similar type of case,⁷² the Sixth Circuit upheld a district court’s exercise of jurisdiction over a defendant because the defendant had lawfully entered into a clickwrap agreement with CompuServe.⁷³

B. E-SIGN, THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

On June 30, 2000, President Clinton signed into law Public Law 106-229, otherwise known as the Electronic Signatures in Global and National Commerce Act.⁷⁴ E-Sign, as it is more commonly known, was enacted to give statutory support to the enforceability of online contracts. It became effective on October 1, 2000.

E-Sign provides that a signature, contract, or related document may not be denied legal validity solely because it is in electronic form.⁷⁵ E-Sign also allows electronic filing systems to satisfy regulatory record-keeping requirements, as long as the record keeping is done accurately

⁶⁹ The phrase “clickwrap agreement” derives from the phrase “shrinkwrap agreement,” which is a term used to describe contractual provisions that are printed on the packaging of a product with a statement that the purchaser, by using the product, agrees to the terms printed on the packaging. The general rule on enforceability of shrinkwrap agreements is that they are enforceable, except where the terms of the agreement are “objectionable on grounds applicable to contracts in general” (e.g., unconscionability). *ProCD Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). Otherwise, shrinkwrap agreements have generally been upheld, except in situations in which the seller attempts to modify via the shrinkwrap agreement previously agreed-upon terms. *See Step-Saver Data Systems Inc. v. Wyse Tech.*, 939 F.2d 91 (3d Cir. 1991).

⁷⁰ 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998).

⁷¹ Spam is “unsolicited junk email.” *United States v. Hay*, 231 F.3d 630, 633 n.3 (9th Cir. 2000).

⁷² There are cases in several jurisdictions that uphold clickwrap agreements. *See, e.g., Caspi v. The Microsoft Network, LLC*, 732 A.2d 528 (N.J. App. Div. 1999); *see also Groff v. America Online, Inc.*, No. PC 97-0331, 1998 WL 307001 (R.I. Super. May 27, 1998).

⁷³ *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996).

⁷⁴ 15 U.S.C. §§ 7001 *et seq.* (2000).

⁷⁵ E-Sign does not apply to wills, codicils, or testamentary trusts. It also does not apply to certain family matters.

and the records are accessible to those with lawful rights of access. E-Sign permits contracts entered into by electronic agents.⁷⁶ Additionally, when required by law to provide information to a consumer, a website operator may provide such information electronically if the consumer has given affirmative consent.

E-Sign does not preempt state law enforcement of similar laws. It allows the enforcement of state law to the extent state law is technologically neutral.

C. UCITA, THE UNIFORM COMPUTERS INFORMATION TRANSACTIONS ACT

On July 29, 1999, the National Conference of Commissioners on Uniform State Laws voted to approve the Uniform Computers Information Transactions Act for states to consider adopting. UCITA was originally drafted as a proposed addition (Article 2B) to the Uniform Commercial Code (UCC).

Under UCITA, clickwrap and shrinkwrap agreements are enforceable if the user/purchaser exhibits “manifest assent” after having an “opportunity to review” the terms of the agreement.⁷⁷ Under UCITA, a user/purchaser may be bound by terms disclosed after the time of payment, if that user exhibits manifest assent prior or during the user’s “initial performance or use of or access to the information.”⁷⁸ UCITA also recognizes contracts entered into through the interaction of electronic agents or the interaction of an individual and an electronic agent.⁷⁹ Virginia has adopted UCITA.

D. UETA, THE UNIFORM ELECTRONIC TRANSACTIONS ACT

The National Conference of Commissioners on Uniform State Laws promulgated the Uniform Electronic Transactions Act on July 30, 2000. UETA provides uniform standards under which electronic signatures and electronic records have legal effect.

UETA prohibits the denial of enforceability to a record or signature solely because it is in electronic form or because an electronic record was used in the formation of a contract.⁸⁰ Like UCITA and the federal E-Sign Act, UETA recognizes contracts formed via electronic agents. UETA also allows for electronic notarization where the law requires that a signature or record be notarized.⁸¹ Electronic signatures of a notary public or any other party to the online contract are attributable to an individual when it can be demonstrated in any manner (including the use of reliable security procedures) that the electronic signature was an act of that individual. UETA applies traditional contract law to errors in an electronic record (i.e., the mistake doctrine) and

⁷⁶ 15 U.S.C. § 7001 An “electronic agent” is a program or means through which a party can negotiate by initiating an action and responding to electronic messages without individual intervention. *See* UCITA § 102.

⁷⁷ UCITA §§ 112, 209.

⁷⁸ UCITA § 211.

⁷⁹ UCITA § 206.

⁸⁰ UETA § 7. UETA does not apply to wills, codicils, or testamentary trusts. UETA also does not apply to any transaction to the extent that UCITA or certain portions of the UCC already govern the transaction.

⁸¹ UETA § 11.

has guidelines for handling errors or changes to an online contract that occur during transmission.⁸² Virginia has adopted UETA legislation.

⁸² UETA § 10.

HACKED OFF ABOUT COMPUTER CRIME: FEDERAL AND STATE COMPUTER CRIME SENTENCING

I. INTRODUCTION

Computer or cybercrime is “one of the fastest evolving areas of criminal behavior and a significant threat to our national and economic security.”⁸³ “Cybercrime is a whole new form of warfare where everyone is a target . . . [O]ne of the most potent weapons available is a laptop computer . . . Never in history has there been a time like this. The technological revolution is marching forward, but I don’t see government matching its past.”⁸⁴ Has Virginia matched the fast moving technological revolution giving rise to cybercrime? This section of the material discusses Virginia’s response to computer crime. It then discusses federal law.

II. IS CYBERCRIME REALLY A PROBLEM?

The Internet has grown tremendously. As of 1999, there were over 100 million Internet users in the United States, a number that is expected to almost double to 177 million users by 2003.⁸⁵ In addition, “business-to-business” electronic commerce is expected to grow to over \$1 trillion by 2003.⁸⁶ The Internet provides benefits in education, research, entertainment and public affairs as well.⁸⁷ Putting a damper on the revolutionary nature of the Internet, is the fact that it provides a new medium for criminal activity. According to a Computer Security Institute survey, financial losses in 1998 from hacker attacks on 241 companies rose thirty-six percent over the prior year to \$136,822,000. Thus, finding effective ways to police, prevent and sentence criminal behavior on the Internet may play a large role in maintaining the financial, commercial and educational benefits the Internet may provide.

Adults are not the only perpetrators of these crimes. Juveniles⁸⁸ can commit serious computer crimes resulting in a large amount of financial injury, distrust in the Internet and the possibility of the loss of, or injury to human life. “[A] survey of about 1,000 kids of high school and college age . . . found . . . that three out of four had engaged and will engage in future computer hacking.”⁸⁹ For example, in 1997, the Federal government brought charges against a minor that used his home computer to find a vulnerable spot in NYNEX’s Next Generation Digital Loop Carrier systems at the Worcester Airport, Rutland, Massachusetts. In March 1997, the minor accessed the loop carrier system connected to the Worcester Airport and disabled it at 9:00 a.m. This resulted in the loss of phone service to the Airport until about 3:30 p.m. and reduced the airport’s radio range from forty to fifteen miles. Later that day, the minor accessed

⁸³ Director Louis J. Freeh, Federal Bureau of Investigation, Remarks before the Senate Committee on the Judiciary; Subcommittee for the Technology, Terrorism, and Government Information, p. 1 (March 28, 2000).

⁸⁴ Caroline Bolte, *Meeting Close-Up: The Dark Side of the Net*, VA. NEWS JRNL. ON-LINE, Vol. 26, No. 2 (March, 2000).

⁸⁵ The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President’s Working Group on Unlawful Conduct on the Internet, p. 10 (March 2000).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ Those under age 18.

⁸⁹ Noack, David Noack, *HACKING – “It ain’t cool...its CRIMINAL”*, (Feb. 18, 2000), available at <http://www.youthwatch.net/hacking-not-cool.html> (quoting Mike Higgins, president and co-founder of Para-Protect, Inc.).

the local carrier loop servicing customers in Rutland and disrupted phone service throughout the area. The minor also broke into a local Worcester pharmacist's computer on four different occasions. On one of those occasions, the minor ordered the pharmacy computer to transmit all prescriptions filled during the preceding week to his computer files. The minor pled guilty and will receive two years' probation. During probation the minor may not use or possess a modem or other means of remotely accessing a computer or computer network directly or indirectly. In addition, he has to forfeit all the computer equipment used to perpetrate the hacks. Finally, the minor must pay restitution to Bell Atlantic and perform 250 hours of community service. The U.S. Attorney prosecuting the case said that "[t]his case reflects our intention to prosecute in federal court anyone, including a teenager, who commits a serious computer crime As with a driver's license, the freedom to explore with a computer and modem comes with the obligation to act responsibly and respect the law."

Like the Worcester teen-hacker, two sixteen-year-old Cloverdale teenagers pled guilty to two federal juvenile delinquency charges. One of the boys, "Makaveli," pled guilty in Federal district court to breaking into the Lawrence Livermore National Laboratory computer system and stealing passwords. The other boy pled guilty to breaking into an Air Force Computer and stealing passwords. Both must perform community service and forgo the use of a home computer with a modem. In addition, each must serve a probationary period, during which neither may hold a computer-industry job, or access a computer without proper supervision. As U.S. Attorney Michael Yamaguchi said: "At the very least, this is very dangerous, in the same way that it is socially harmful to make false calls to 911 or to falsely pull fire alarms."⁹⁰

More recently, a sixteen-year-old from Miami pled guilty in Federal court to two counts of juvenile delinquency and will serve six months in juvenile detention.⁹¹ Going by the name "cOmrade," Jonathan James invaded thirteen computers at the National Aeronautics and Space Administration (NASA).⁹² He downloaded software and stole data, resulting in a three-week shutdown of some NASA computers and more than \$40,000 in labor and replacement costs. James also hacked into computers at the Defense Threat Reduction Agency (DTRA), an agency monitoring nuclear threats to the United States.⁹³ James intercepted more than 3,300 messages and nineteen user names and passwords. Attorney General Janet Reno stated that "[b]reaking into someone else's property, whether it is a robbery or a computer intrusion, is a serious crime We take computer intrusion seriously and are working with our law enforcement partners to aggressively fight this problem." James' attorney, Ted Klein stated that James was a "good smart boy who made a big mistake."⁹⁴

⁹⁰ See Bob Norberg, PRESS DEMOCRAT, March 4, 1998, at A1. The facts of this story came from this article, which also stated that other sites hacked into included the Naval Post Graduate School, Pearl Harbor, the U.S. Marine Corp, the Naval Undersea Warfare Center, the National Oceanic and Atmospheric Administration, NASA, government sites in Taiwan and the United Arab Emirates. *Id.*

⁹¹ See *Juvenile Computer Hacker Sentenced to Six Months in Detention Facility*, (Sept. 21, 2000), available at <http://cybercrime.gov/comrade.htm> See David Stout, *Youth Sentenced in Government Hacking Case*, N.Y. TIMES, Sept. 22, 2000, at A9.

⁹² See *Juvenile Computer Hacker Sentenced to Six Months*, *supra* note 58.

⁹³ *Id.*

⁹⁴ See *Juvenile Computer Hacker Sentenced to Six Months*, *supra* note 58. There are many other stories in the press of hacking minors. For example, Jacey Kyle Johnson, age fourteen, broke into the server at Crystal River High School, but did not change anything. See Bill Varian, *Boy, 14, Charged With Hacking*, ST. PETERSBURG TIMES, Feb. 18, 2000. In Dallas an eighteen-year-old was charged under Texas law for accessing and defacing web pages,

III. VIRGINIA COMPUTER CRIMES ACT

In 1984, the Virginia Computer Crimes Act took effect.⁹⁵ It represented the Virginia General Assembly's choice to prosecute computer crimes by distinct computer-based statutes, as opposed to applying existing criminal statutes to computer crime. The Computer Crimes Act punishes computer fraud, computer trespass, computer invasion of privacy, theft of computer services, personal trespass, harassment, and use of encryption to commit a crime. These offenses encompass crimes against computers as well as the use of a computer to commit a crime.⁹⁶

A. COMPUTER FRAUD

Virginia Code section 18.2-152.3(1) makes it a crime to use a computer⁹⁷ or computer network,⁹⁸ without or in excess of authority,⁹⁹ with the intent 1) to obtain property or services under false pretenses,¹⁰⁰ 2) to embezzle¹⁰¹ or 3) to commit larceny,¹⁰² or 4) to convert another's property.¹⁰³ Success is not required, but rather a violation occurs where there is intent, despite

including those of six Texas government sites. See Holly Becka, *Suspect in hacking surrenders, is jailed: Lawyer says computer incidents in which 18-year-old is charged did not involve theft*, DALLAS MORNING NEWS, Oct. 14, 2000, at 43A. A Riverside California fifteen year-old hacked his way in to Choice 2000, an online Charter School. He wiped out student and school computer records, which was particular harmful given that at Choice 2000, students communicate with teachers and each other from home on computers. See Steve Fetbrandt, *Hacker facing possible charges: Officials say the boy, 15, destroyed the computer records at Choice 2000 On-Line School in Perris*, PRESS-ENTERPRISE, Oct. 14, 2000, at B1.

⁹⁵ Va. Code Ann. § 18.2-152.1 *et seq.* (Michie 2000).

⁹⁶ COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE, § 15.2-1 (1999).

⁹⁷ A computer is "an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on a computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device." § 18.2-152.2.

⁹⁸ A "computer network" is "two or more computers connected by a network." § 18.2-152.2.

⁹⁹ "Without authority," means that a person "(i) ... has no right or permission of the owner to use a computer or he uses a computer in a manner exceeding such right or permission or (ii) he uses a computer, computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider." § 18.2-152.2.

¹⁰⁰ § 18.2-152.3(1).

¹⁰¹ Virginia Code § 18.2-152.8 expands the reach of the embezzlement statute, § 18.2-111. COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE § 15.2-3 (1999). Under this statute, "personal property subject to embezzlement shall include:

1. Computers and computer networks;
2. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
 - a. Tangible or intangible;
 - b. In a format readable by humans or by a computer;
 - c. In transit between computers or within a computer network or between any devices which comprise a computer; or
 - d. Located on any paper or in any device on which it is stored by a computer or by a human; and
3. Computer Services. § 18.2-152.8.

¹⁰² § 18.2-152.3(2).

¹⁰³ § 18.2-152.3(3).

the lack of success.¹⁰⁴ A violation resulting in damage of \$200 or more is a Class 5 felony,¹⁰⁵ punishable by a term of imprisonment between one and ten years, or confinement in jail for a period not to exceed twelve months, or a fine of not more than \$2500, or confinement in jail for a period not to exceed twelve months and a fine not to exceed \$2500.¹⁰⁶ A violation resulting in damage of less than \$200 is a Class 1 misdemeanor,¹⁰⁷ punishable by confinement in jail for not more than twelve months, a fine not to exceed \$2500, or confinement in jail for not more than twelve months and a fine not to exceed \$2500.¹⁰⁸

B. COMPUTER TRESPASS

Virginia Code section 18.2-152.4, computer trespass, makes it a crime to use a computer or computer network, without or in excess of authority to:

- 1) Temporarily or permanently remove, halt or otherwise disable any computer data, programs, or software from a computer or computer network;
- 2) Cause a computer to malfunction,¹⁰⁹ regardless of the length of the malfunction¹¹⁰;
- 3) Change or erase any computer data, programs or software;
- 4) Effect the creation or alteration of a financial instrument or of an electronic fund transfer;
- 5) Cause physical injury to another's property;
- 6) Make or cause to be made an unauthorized copy, in any form, including but not limited to any printed or electronic computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network; or
- 6) Falsify or forge e-mail transmission or other routing information in any manner connected with the transmission of unsolicited bulk e-mail through or into an e-mail service provider or its subscribers.

This statute punishes the effort to gain access and achieve the prohibited results. It does not punish the actual result.¹¹¹ This section also makes it a crime for any person knowingly to sell, give, or otherwise distribute or possess with the intent to sell or distribute software primarily enabling the falsification of e-mail transmission or routing information.¹¹²

¹⁰⁴ COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE, § 15.2-2 (1999).

¹⁰⁵ § 18.2-152.3(3).

¹⁰⁶ Va. Code Ann. § 18.2-10(e) (Michie 2000). *See also* Virginia Model Jury Instructions.

¹⁰⁷ § 18.2-152.3(3).

¹⁰⁸ § 18.2-11(a).

¹⁰⁹ § 18.2-152.4(A)(2).

¹¹⁰ In *Commonwealth v. Honhart* the court dismissed the indictment where the Commonwealth charged the defendant under (A) (2) making it unlawful to use a computer or computer network without authority with intent to cause a malfunction, but the evidence only established that he halted the computer. *Commonwealth v. Honhart*, No. 96656 (Va. Cir. Ct. July 27, 2000).

¹¹¹ COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE § 15.3 (1999).

¹¹² § 18.2-152.4(C). The statute explicitly lays out all types of software that it is unlawful to sell, distribute, or possess: "It shall be unlawful for any person knowingly to sell, give or otherwise distribute software which (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic email transmission information or other routing information; or (iii) is marketed by that person or another acting in concert with that person with that person's

The penalties provided for by the computer trespass statute vary depending upon the amount of damage and the actor's mental state. Any person who violates the statute is guilty of a Class 3 misdemeanor,¹¹³ punishable by a fine not to exceed \$500.¹¹⁴ If a violation results in damage of \$2500 or more caused by the actor's recklessness, the act is a Class 1 misdemeanor,¹¹⁵ punishable by confinement in jail for not more than twelve months, a fine not to exceed \$2500, or confinement in jail for not more than twelve months and a fine not to exceed \$2500.¹¹⁶ Finally, if the act results in damage of \$2500 or more caused by the actor's malice, the act is a Class 6 felony,¹¹⁷ punishable by imprisonment for a term between one and five years, or confinement in jail for no more than twelve months, or a fine of not more than \$2500, or confinement in jail for no more than twelve months and a fine of no more than \$2500.¹¹⁸

Computer Trespass Sentencing – Virginia Code 18.2-152.4

	Mental State	Damage
Class 3 Misdemeanor	None, Negligence	Less than \$2500
Class 1 Misdemeanor	Recklessness	\$2500 or more
Class 6 Felony	Malice	\$2500 or more

C. COMPUTER INVASION OF PRIVACY

To protect the privacy of personal information, Virginia Code section 18.2 -152.5 makes it a crime to use a computer or computer network to intentionally examine, without or in excess of authority, “any employment, salary, credit or any other financial or personal information relating to any other person.”¹¹⁹ Examination requires that the offender know that he or she is without authority to view the displayed information.¹²⁰ A violation of the Computer Invasion of Privacy statute is a Class 3 misdemeanor,¹²¹ punishable by a fine not to exceed \$500.¹²²

knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.” *Id.*

¹¹³ § 18.2-152.4(C).

¹¹⁴ § 18.2-11(c).

¹¹⁵ § 18.2-152.4(C).

¹¹⁶ § 18.2-11(a).

¹¹⁷ § 18.2-152.4(C).

¹¹⁸ § 18.2-10(f).

¹¹⁹ § 18.2-152.5(A).

¹²⁰ The Virginia Court of Appeals upheld a conviction of four counts of computer invasion of privacy. *Plasters v. Commonwealth*, No. 1870-99-3 (Va. App. June 27, 2000). The Commonwealth convicted the defendant for accessing criminal history information while working as a dispatcher for the Covington Police Department. The Court found that defendant knew she was unauthorized because of the computer warning that the information obtained from the system was only to be used from criminal justice purposes. The Court rejected Defendant's argument that she had no knowledge of the specific statute, applying the “ignorance of the law is no excuse” principle. *Id.*

¹²¹ § 18.2-152.5(B).

¹²² § 18.2-11(c). If the access prohibited by §18.2-152.5 was gained with the intent to conceal, copy or alter such data, or do any of the other things condemned by Va. Code § 18.2.-152.4, the additional crime of computer trespass was committed. *COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE*, § 15.4 (1999).

D. THEFT OF COMPUTER SERVICES

Virginia Code section 18.2-152.6 punishes the willful use of a computer or computer network with the intent to obtain computer services, without or in excess of authority.¹²³ This statute punishes use with the intent to obtain services; the violator need not actually receive services.¹²⁴ A violation of this section is a Class 1 misdemeanor, punishable by confinement in jail for not more than twelve months, a fine not to exceed \$2500, or confinement in jail for not more than twelve months and a fine not to exceed \$2500¹²⁵.

E. PERSONAL TRESPASS

Computer trespass carries the harshest penalty of the Computer Crime Act statutes. It aims at actions such as interfering with medical records or air controller's flight data. Virginia Code section 18.2-152.7 punishes use of a computer or computer network, without or in excess of authority, with the intent to cause physical injury to another individual.¹²⁶ This statute punishes use.¹²⁷ If death or malicious wounding results, another charge may result.¹²⁸ If the violator commits the prohibited act maliciously a violation is a Class 3 felony, punishable by a term of imprisonment between five and twenty years and a fine not to exceed \$100,000.¹²⁹ If done unlawfully, a violation of this section is a Class 1 misdemeanor, punishable by confinement in jail for not more than twelve months, a fine not to exceed \$2500, or confinement in jail for not more than twelve months and a fine not to exceed \$2500.¹³⁰

F. HARASSMENT

Virginia Code section 18.2-152.7:1 punishes use of a computer to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or to make any suggestion of an obscene nature, or threaten any illegal or immoral act with the intent to coerce, intimidate, or harass another.¹³¹ A conviction will result in a Class 1 misdemeanor, punishable by confinement in jail for not more than twelve months,¹³² a fine not to exceed \$2500, or confinement in jail for not more than twelve months and a fine not to exceed \$2500.¹³³

G. ENCRYPTION

If a person uses encryption technology to further any criminal activity, computer related or not, he or she may have committed an offense separate from the underlying criminal offense. Virginia Code section 18.2-152.15 punishes the willful use of encryption to further any criminal

¹²³ § 18.2-152.6.

¹²⁴ COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE § 15.4 (1999).

¹²⁵ § 18.2-11(a).

¹²⁶ § 18.2-152.7(A).

¹²⁷ COSTELLO, VIRGINIA CRIMINAL LAW AND PROCEDURE, § 15.6 (1999).

¹²⁸ *Id.*

¹²⁹ § 18.2-10(c). The court shall impose a sentence of imprisonment together with a fine, or imprisonment. However if the defendant is not a natural person, the court shall impose only a fine. § 18.2-10(g).

¹³⁰ § 18.2-11(a).

¹³¹ § 18.2-152.7:1.

¹³² § 18.2-152.7:1.

¹³³ § 18.2-11(a).

activity.¹³⁴ A violation of this statute is a “separate and distinct” offense from the “predicate criminal activity.”¹³⁵ Violation will result in a Class 1 misdemeanor, punishable by confinement in jail for not more than twelve months,¹³⁶ a fine not to exceed \$2500, or confinement in jail for not more than twelve months and a fine not to exceed \$2500.¹³⁷

H. VIRGINIA CRIMINAL SENTENCING GUIDELINES

The Virginia Criminal Sentencing Guidelines do not cover Virginia Computer Crimes Act offenses.¹³⁸

IV. SENTENCING JUVENILES¹³⁹ WHO VIOLATE THE COMPUTER CRIMES ACT

A juvenile charged with violating a computer crime proceeds through the juvenile system like any juvenile facing any other charge. A juvenile enters the system when a police officer, victim, parent, or other agency, for example, reports a delinquent offense to an intake officer at a court services unit. If the case is forwarded to court, the intake officer must determine if the juvenile should be detained or returned to his or her parents. If detained, a hearing in the Juvenile and Domestic Relations General District Court (J&DR court) takes place within 72 hours to determine the necessity of further detention. The juvenile then proceeds to an adjudicatory hearing to determine guilt or innocence. Finally, the juvenile proceeds to disposition, or sentencing.

Computer crimes may present new issues for juvenile courts. Should juveniles receive treatment like any other juvenile? Or, should they receive harsher sentences given the possibly devastating consequences, both economic and physical that could result from cybercrime? For example, the Worcester teen’s act of disabling an airport’s local carrier loop could have resulted in a plane crash and loss of, or injury to life. Perhaps teen cyber-criminals should receive gentler treatment, because of the academic potential and computer knowledge displayed in the commission of crime. Perhaps the juvenile justice system, both state and federal, is adequate to deal with teen cyber-criminals as is. While this section does not tackle these questions, it seeks to provide the background for intelligent discussion on the issues by discussing the options for punishment and rehabilitation of teen cyber-criminals under both Virginia and federal laws.

A. GOAL OF JUVENILE JUSTICE SYSTEM

The Virginia juvenile justice system aims to rehabilitate delinquent juveniles, while protecting their constitutional and other rights and maintaining community safety.¹⁴⁰ Because

¹³⁴ § 18.2-152.15. “‘Encryption’ means the enciphering of intelligible data into unintelligible form or the deciphering of unintelligible data into intelligible form.” *Id.*

¹³⁵ § 18.2-152.15.

¹³⁶ § 18.2-152.7:1.

¹³⁷ § 18.2-11(a).

¹³⁸ Virginia Code § 18.2-152.14 would use the forgery guideline, because the statute refers back to the forgery statute. This paper does not discuss this statute because it appears to broaden an existing criminal statute, rather than create a new computer crime.

¹³⁹ Juveniles are persons under age 18. Va. Code Ann. § 16.1-228 (Michie 2000).

¹⁴⁰ Va. Code Ann. § 16.1-227 (Michie 2000).

the focus is rehabilitation and not punishment, the juvenile court cannot convict a juvenile of any misdemeanor or felony, but may adjudicate a juvenile delinquent.¹⁴¹ A juvenile is delinquent where, prior to his or her eighteenth birthday, the juvenile commits a delinquent act,¹⁴² generally “any act designated a crime under the law of [the] Commonwealth, or an ordinance of any city, county, town or service district, or under federal law.”¹⁴³ Another indication of the rehabilitative nature of the juvenile justice system is that an adjudication of delinquency is a civil, not criminal finding.¹⁴⁴ Thus, the J&DR court should construe its juvenile justice law to protect the community as well as rehabilitate juveniles and reduce the incidence of juvenile crime.¹⁴⁵

B. JUVENILE COURT JURISDICTION

The J&DR court generally has jurisdiction over alleged crimes committed by persons under age eighteen at the time of the alleged crime. The court has “original and exclusive” jurisdiction over all charges against a juvenile that would be a misdemeanor or felony if committed by an adult.¹⁴⁶ The J&DR court may lose jurisdiction upon transfer or certification of the juvenile for trial as an adult.¹⁴⁷ In addition, the J&DR court loses jurisdiction over a juvenile when that juvenile turns 21, and thus cannot sentence a juvenile that age.¹⁴⁸

C. DISPOSITION

The J&DR court has a large number of available options in sentencing a juvenile “that are to be considered in turn, looking at the least intrusive alternative first.”¹⁴⁹ In sentencing juveniles for delinquency involving the Computer Crimes Act, the following options are available:

1. Enter an order under Virginia Code section 16.1-278,¹⁵⁰ ordering a public agency to provide services otherwise mandated by state or federal law.¹⁵¹
2. Allow the juvenile to remain with his or her parents, subject to court imposed conditions and limitations.¹⁵² Should the judge chose this route, the judge may consider banning the use of a computer and mouse, or any other computer-type device, in or our outside the home, by the juvenile. To ensure compliance the judge may charge the parent with monitoring.

¹⁴¹ Jones v. Commonwealth, 185 Va. 335, 342 (1946).

¹⁴² Va. Code Ann. § 16.1-228 (Michie 2000).

¹⁴³ § 16.1-228.

¹⁴⁴ Lewis v. Howard, 374 F. Supp. 446, 447 (W.D. Va. 1974).

¹⁴⁵ § 16.1-227(4).

¹⁴⁶ § 16.1-241(A)(1) (Michie 2000).

¹⁴⁷ Va. Code Ann. § 16.1-229.1 (Michie 2000).

¹⁴⁸ Va. Code Ann. § 16.1-285 (Michie 2000).

¹⁴⁹ VIRGINIA LAW FOUNDATION, JUVENILE LAW AND PRACTICE IN VIRGINIA § 8.1 (1999).

¹⁵⁰ Va. Code Ann. § 16.1-278.8(A)(1) (Michie 2000).

¹⁵¹ VIRGINIA LAW FOUNDATION, *supra* note 117, § 8.1. Virginia Code section 16.1-278.8(A)(1) states that “[t]he judge may order, after notice and opportunity to be heard, any state, county or municipal officer or employee or any governmental agency or other governmental institution to render only such information, assistance, services and cooperation as may be provided for by state or federal law or an ordinance in any city, county or town.”

¹⁵² § 16.1-278.8(A)(2).

3. Order the juvenile's parent to participate in rehabilitative programs and comply with other conditions and limitations for the rehabilitation of the juvenile and parent.¹⁵³
4. Defer disposition for twelve months, with dismissal at the end of that period based on the juvenile's good behavior.
5. Defer disposition and place the juvenile in the temporary custody of the Department of Juvenile Justice to attend boot camp. The court may exercise this option in cases of computer fraud, computer trespass resulting in damage of \$2500 or more, theft of computer services, personal trespass by computer, harassment by computer, or the use of encryption in criminal activity.¹⁵⁴ To qualify, the juvenile must also (1) not have a previous or currently on-going delinquent adjudication, or have a guilty finding in a violent juvenile felony, (2) not have previously attended boot camp, (3) not have a previous commission to and receipt by the Department of Juvenile Justice, (4) be assessed as an appropriate candidate for boot camp.¹⁵⁵ Thus, for the more serious computer crimes a J&DR court may order boot camp.
6. Defer disposition for not more than twelve months, without a guilty determination and with the consent of the juvenile and his or her attorney, for dismissal of the charges after probation and upon terms and conditions.¹⁵⁶
7. Order the parent of the juvenile, with whom the juvenile does not live to participate in programs or treatment, and comply with conditions and limitations for the rehabilitation of the juvenile.¹⁵⁷
8. Place the juvenile on probation subject to conditions and limitations determined by the J&DR court.¹⁵⁸
9. Place the juvenile on probation and order treatment for alcohol or drug abuse or dependence, provided that (i) a substance abuse assessment "reasonably indicates that the commission of the offense was motivated by, or closely related to, the habitual use of alcohol or drugs and indicates that the juvenile is in need of treatment," (ii) the juvenile has not been and is not currently being adjudicated for a violent juvenile felony and (iii) an available facility exists.¹⁵⁹

¹⁵³ § 16.1-278.8(A)(3).

¹⁵⁴ Bot camp is unavailable as a possible disposition in cases of computer trespass where less than \$2500 of damage resulted and no *mens rea* existed. It would also be unavailable in cases of computer invasion of property.

¹⁵⁵ § 16.1-278.8(A)(4a)(ii)-(v).

¹⁵⁶ § 16.1-278.8(A)(5).

¹⁵⁷ § 16.1-278.8(A)(7).

¹⁵⁸ § 16.1-278.8(A)(3).

¹⁵⁹ § 16.1-278.8(A)(7a)(i)-(iii).

10. Impose a fine of no more than \$500 on the juvenile.¹⁶⁰
11. Suspend the motor vehicle and driver's license of the juvenile or impose a curfew as to the hours he or she may operate a motor vehicle.¹⁶¹
12. Require the juvenile to make restitution or reparation to the aggrieved party for actual damages or loss caused by the juvenile's offense.¹⁶²
13. Transfer legal custody to (a) a relative or other person qualified to care for the juvenile, (b) a child welfare agency inside the Commonwealth,¹⁶³ the local board of social services in the county or city in which the court has jurisdiction or the juvenile resides.¹⁶⁴
14. Commit the juvenile to the Department of Juvenile Justice (DJJ).¹⁶⁵ To commit a juvenile to DJJ the juvenile must be eleven years old and meet one of the following condition:
 - (i) the current underlying offense must be a felony;
 - (ii) the current underlying offense must be a Class 1 misdemeanor and the juvenile has a previous delinquent adjudication based on a felony; or
 - (iii) the current underlying offense must be a Class 1 misdemeanor and the juvenile has three previous delinquent adjudications based on Class 1 misdemeanors.¹⁶⁶

Under this section, the J&DR court may commit a juvenile to DJJ for committing malicious computer trespass resulting in damage of \$2500 or more, malicious personal computer trespass, and computer fraud where the juvenile obtained property or services valued at \$200 or more. The J&DR court may also commit a juvenile to DJJ if the juvenile has a previous delinquency adjudication based on a felony, or three previous delinquency adjudications based on Class 1 misdemeanors, and the juvenile commits reckless computer trespass resulting in damage of \$2500 or more, theft of computer services, unlawful computer trespass, harassment by computer, use of encryption in criminal activity, or computer fraud where the juvenile obtained property or services valued at less than \$200

¹⁶⁰ § 16.1-278.8(A)(8).

¹⁶¹ § 16.1-278.8(A)(9).

¹⁶² § 16.1-278.8(A)(10).

¹⁶³ § 16.1-278.8(A)(13)(c). This section states that the "court shall not transfer legal custody of a delinquent juvenile to an agency, organization or facility outside of the Commonwealth without the approval of the Director. *Id.*

¹⁶⁴ § 16.1-278.8(A)(13)(a)-(c).

¹⁶⁵ § 16.1-278.8(A)(14).

¹⁶⁶ § 16.1-278.8(A)(14)(i)-(iii).

15. The court may impose a penalty under Virginia Code section 16.1-284, which allows the court to impose an adult penalty on an adult appearing before the court to answer for a crime committed before that adult turned eighteen.¹⁶⁷ When a juvenile commits a computer crime, but does not appear before the court until he or she reaches age eighteen the court may impose the adult penalties discussed above. However, the court cannot “exceed the punishment for a Class 1 misdemeanor.”¹⁶⁸
16. The court may impose a penalty under Virginia Code section 16.1-284.1, subsections A or B.¹⁶⁹ Under subsection A, the court may order a juvenile, fourteen years of age or older, to confinement in a detention home or other secured facility for no more than thirty days.¹⁷⁰ To do so the court must find that the juvenile committed an offense that if committed by an adult would be punishable by confinement, and (i) that the juvenile has not been adjudicated delinquent within the previous twelve months, (ii) that the juvenile’s and community’s interests require restraint or discipline, (iii) and that other dispositional options will not serve the juvenile’s best interests.¹⁷¹

Under subsection B, the court may order the juvenile committed to DJJ, but suspend this commitment and order the juvenile confined in a detention home or other secure facility for juveniles for a period not to exceed six months. To do so the court must find that the juvenile committed an offense that if committed by an adult would be punishable by confinement correctional facility, and (i) that the juvenile has been adjudicated delinquent within the previous twelve months and has not responded to past treatment efforts, (ii) that the juvenile is amenable to continued treatment, and (iii) that the juvenile’s and community’s interests require restraint or discipline.¹⁷²

These sections appear to apply, where the other factors exist, only to computer fraud, reckless and malicious computer trespass, theft of computer services, personal trespass by computer, harassment by computer and the use of encryption in criminal activity, because each of these is punishable by imprisonment or jail.

17. The court may impose a penalty under Virginia Code section 16.1-285.1. This section allows commitment to DJJ of a juvenile fourteen years of age or older guilty of an offense which would be a felony if committed by an adult.¹⁷³ To order such commitment the court must make two more

¹⁶⁷ § 16.1-284.

¹⁶⁸ § 16.1-284.

¹⁶⁹ This section discusses section 16.1-284.1 as it reads on February 28, 2001. A revision of section 16.1-284.1 will take effect on July 1, 2001.

¹⁷⁰ § 16.1-284.1.

¹⁷¹ § 16.1-284.1(A)(i)-(iii).

¹⁷² § 16.1-284.1(B)(i)-(iii). The court would make these determinations after receipt of a social history compiled within the immediately preceding twelve months. *Id.*

¹⁷³ § 16.1-285.1(A).

findings. First, that the confinement would meet the juvenile's rehabilitative needs and serve the community's best interests. Second, (i) that the juvenile is on parole for an offense which would be a felony if committed by an adult, (ii) that the juvenile was committed, in the immediately preceding twelve months, to the state for an offense which would be a felony if committed by an adult, (iii) that the current felony is punishable by a confinement for more than twenty years if committed by an adult,¹⁷⁴ or (iv) that the juvenile has previously been adjudicated delinquent based on a felony punishable by confinement for more than twenty years if committed by an adult. If the juvenile's case meets the criteria, DJJ would then place the juvenile in a correctional center for a period of time, specified by the court, based on several factors.¹⁷⁵ Based on these characteristics, the court may order such commitment for computer fraud involving \$200 or more of computer services, malicious computer trespass resulting in damage of \$2500 or more, and malicious personal computer trespass.

18. The court may impose a penalty under Virginia Code section 16.1-278.9, the abuse and loss provision of the law.
19. The court may require the juvenile to participate in a gang-activity prevention program if the delinquency is based on certain enumerated offenses.¹⁷⁶ This dispositional option does not apply to any Virginia computer crimes.

D. TRANSFER

Under certain circumstances, a juvenile may be tried as an adult for his or her allegedly criminal acts. Where the ability of the Commonwealth to try the juvenile as an adult rests with the court's discretion this is called transfer. Transfer¹⁷⁷ addresses those offenders who, by virtue of their age or past record or the gravity of the charged offense, or for a combination of these factors, should be exposed to the harsher handling inherent in the adult system.¹⁷⁸ For transfer to occur, the Commonwealth must make a motion for transfer. Transfer cannot take place unless the juvenile is fourteen years of age or older and commits an offense that would be a felony if committed by an adult.¹⁷⁹ Thus, transfer may occur for computer fraud involving \$200 or more of computer services, malicious computer trespass resulting in damage of \$2500 or more, and malicious personal computer trespass.

If the Commonwealth makes a motion to transfer, several conditions must be satisfied before the J&DR court will grant the transfer. The juvenile and his parents must have notice of the motion to transfer. The juvenile court must find probable cause to believe that the juvenile

¹⁷⁴ This subsection would never apply because none of the computer offenses carry a term of more than twenty years.

¹⁷⁵ § 16.1-284.1(B)(1)-(4).

¹⁷⁶ § 16.1-278.8(A)(19).

¹⁷⁷ Certification refers to the automatic transfer of certain statutorily enumerated offenses without a hearing.

¹⁷⁸ VIRGINIA LAW FOUNDATION, *supra* note 117 § 5.1.

¹⁷⁹ § 16.1-269.1(A) (2000).

committed the delinquent act or a lesser included that would be a felony if committed by an adult. The juvenile must be competent to stand trial. Finally, the court must find “by a preponderance of the evidence that the juvenile is not a proper person to remain within the jurisdiction of the juvenile court.” In making this final determination the court shall consider:

1. The juvenile’s age;
2. The seriousness of the offense, including whether the juvenile committed it in an “aggressive, violent, premeditated, or willful manner,” whether the offense was against person or property, “with greater weight being given to offenses against persons, especially if death or bodily injury resulted,” whether the juvenile used a gun in the offense, and the nature of the juvenile’s participation;
3. Whether the juvenile system can maintain jurisdiction over the juvenile to successfully rehabilitate and treat the juvenile;
4. The appropriateness and availability of services and dispositional alternatives in the criminal and juvenile justice systems;
5. The juvenile’s previous criminal history;
6. Whether the juvenile has previously absconded from the legal custody of a juvenile corrections facility;
7. Whether and to what extent the juvenile suffers from mental retardation or mental illness;
8. The juvenile’s school record and education, mental and emotional maturity, and physical condition and physical maturity.¹⁸⁰

Thus, under certain circumstances a J&DR court may transfer a computer crimes case to the circuit court. If this happens and the juvenile receives a guilty verdict, the circuit court judge will sentence the juvenile.¹⁸¹ If found guilty of a “violent juvenile felony” the circuit court must fix the sentence as provided for adults, but the circuit court may suspend the sentence conditioned upon successful completion of “such terms and conditions as may be imposed in a juvenile court upon disposition of a delinquency case.”¹⁸² For all other felonies, the circuit court may sentence according to the laws for sentencing adults, or “in its discretion deal with the juvenile in the manner prescribed . . . for the hearing and disposition of cases in the juvenile court.”¹⁸³ However, if the juvenile is found guilty in circuit court of a misdemeanor the circuit court must “deal with the juvenile in the manner prescribed by law for the disposition of a delinquency case in the juvenile court.”¹⁸⁴

V. FEDERAL LAW: THE COMPUTER FRAUD AND ABUSE ACT

The United States Congress has also chosen to treat computer crimes as distinct crimes, rather than adapt real-space laws to fit computer and Internet arenas. The principal computer crime statute is title 18 of the U.S. Code section 1030, enacted in 1984 as the Counterfeit Access Device and Computer Fraud and Abuse Act. As amended by the National Infrastructure

¹⁸⁰ § 16.1-269.1(A)(j) (2000). A transfer decision is not reversible for failure to consider and of the factors listed in Va. Code Ann. § 16.1-269.1(A). *Id*

¹⁸¹ § 16.1-272 (Michie 2000).

¹⁸² § 16.1-272(A)(1).

¹⁸³ § 16.1-272(A)(2).

¹⁸⁴ § 16.1-272(A)(3).

Protection Act in 1996, section 1030 prohibits the unauthorized access of any “protected computer.”¹⁸⁵ A “protected computer” includes virtually any computer attached to the Internet, even if all the computers are located in one state, because “protected computer” includes those used in interstate communications and commerce.¹⁸⁶

Specifically, section 1030(a)(1) makes it a crime to knowingly access computer files, without or in excess of authorization, and then to transfer classified government information.¹⁸⁷ The statute allows for incarceration not to exceed ten years, twenty if the defendant has a previous conviction under section 1030.¹⁸⁸ The statute also allows for the imposition of a fine.

Section 1030(a)(2) prohibits the intentional access of information from a financial institution, U.S. government, or private sector computer used in interstate commerce, without or in excess of authorization.¹⁸⁹ Section 1030(a)(3) makes it a crime to intentionally access a U.S. agency or department nonpublic computer without authorization.¹⁹⁰ If the government shares use of the accessed computer, the illegal access must affect the government’s use.¹⁹¹ Both sections (a)(2) and (a)(3) are misdemeanors unless done for financial gain, in furtherance of any criminal or tortious act, if the value of the stolen information exceeds \$5,000, or if the defendant has a previous conviction under any subsection of section 1030.¹⁹² If convicted under misdemeanor sections (a)(2) and (a)(3), a person may receive a fine and/or not more than one year in prison.¹⁹³ If convicted of a felony under (a)(2) or (a)(3), a person may receive a fine and/or not more than five years in prison.¹⁹⁴ If a person has a previous conviction under any subsection of 1030, he or she may not receive more than ten years and/or a fine for violating subsections (a)(2) or (a)(3).¹⁹⁵

Section 1030(a)(4) forbids the access of a protected computer, intending to defraud and obtain something of value.¹⁹⁶ This section is a felony and does not punish intentional access or use valued at less than \$5,000 in any one year.¹⁹⁷

Section 1030(a)(5) is aimed at combating computer hacking, and has three subsections. The first makes it criminal to knowingly cause the transmission of a program, code, or command resulting in intentionally caused damage to a protected computer.¹⁹⁸ This subsection is a felony, and may result in a fine and/or up to five years in prison, ten with a previous section 1030

¹⁸⁵ 18 U.S.C.A § 1030(e)(2) (2000).

¹⁸⁶ See Laura J. Nicholson, et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207, 213 (2000).

¹⁸⁷ § 1030(a)(1). See generally Nicholson et al., *supra* note 154, at 213.

¹⁸⁸ § 1030(c)(1)(A)-(B).

¹⁸⁹ § 1030(a)(2). See generally Nicholson et al., *supra* note 154, at 213-14.

¹⁹⁰ § 1030(a)(3). See generally Nicholson, et al., *supra* note 154, at 213-14.

¹⁹¹ *Id.*

¹⁹² § 1030(c)(2)(B).

¹⁹³ § 1030(c)(2)(A).

¹⁹⁴ § 1030(c)(2)(B).

¹⁹⁵ § 1030(c)(2)(C).

¹⁹⁶ § 1030(a)(4). See Laura J. Nicholson et al., *supra* note 154, at 213-14.

¹⁹⁷ § 1030(a)(4).

¹⁹⁸ § 1030(a)(5)(A). See Laura J. Nicholson, et al., *supra* note 154, at 213-14. Section 1030(a)(5)(A) does not require that the perpetrator access without authorization. § 1030(a)(5)(A).

conviction.¹⁹⁹ The second and third, subsections (B) and (C), prohibit the intentional access of a protected computer, without authorization and as a result causing damage, recklessly,²⁰⁰ or otherwise.²⁰¹ Subsection (B) requires a reckless *mens rea*, whereas (C) has no *mens rea* requirement. Subsection (B) is a felony carrying the possibility of fine and/or incarceration as in section (a)(5)(A).²⁰² However, because subsection (C) has no *mens rea* requirement it is a misdemeanor, carrying the possibility of a fine and/or up to one year in prison.²⁰³ If done for financial gain, in furtherance of a criminal or tortuous act, or for information valued at more than \$5,000, section (a)(5)(C) is a felony carrying the possibility of five years.²⁰⁴ If the defendant has a previous section 1030 conviction he or she may receive up to ten years.²⁰⁵

An adult convicted of violating any subsection of 1030 is subject to punishment under the United States Sentencing Guidelines (Guidelines), which supplements section 1030(c)'s statutory sentencing confines.²⁰⁶ The Guidelines dictate the base offense level for violations of section 1030(a)(1) through (a)(7).²⁰⁷ They also establish a six-month minimum sentence for those who violate subsections 1030(a)(4) and (a)(5).²⁰⁸ The court may also depart up or down from a defendant's base level offense. For example, a defendant may receive a vulnerable victim enhancement. When a defendant targets a victim based on the victim's unusually high vulnerability to the crime, the defendant may receive a two-level enhancement.²⁰⁹ According to the Sentencing Commission, this guideline, section 3A1.1(b), "can apply to a wide range of

¹⁹⁹ § 1030(c)(3)(A), (B).

²⁰⁰ § 1030(a)(5)(B). This section prohibits causing damage recklessly. *Id.*

²⁰¹ § 1030(a)(5)(C). This section simply prohibits causing damage and does not have a *mens rea* requirement. *Id.* Sections 1030(a)(6) and (a)(7) prohibit the trafficking of passwords and transmission of any threat to cause damage to a protected computer with intent to extort something of value. § 1030(6), (7).

²⁰² § 1030(c)(3)(A), (B).

²⁰³ § 1030(c)(2)(A).

²⁰⁴ § 1030(c)(2)(B)(i)-(iii). Following is a chart to help the reader better understand the *mens rea* required for 1030(a)(5)(A), (B) and (C). *See* Nicholson et al., *supra* note 154, at 220.

	Trespasser	Authorized User
Intentional Damage (a)(5)(A)	Felony	Felony
Reckless Damage (a)(5)(B)	Felony	No crime
Negligent, or Otherwise (a)(5)(C)	Misdemeanor	No Crime

²⁰⁵ § 1030(c)(3)(B).

²⁰⁶ *See* Nicholson et al., *supra* note 154, at 218.

²⁰⁷ *See* Nicholson et al., *supra* note 154, at 218. U.S. Sentencing Guideline section 2B1.1, larceny and embezzlement, govern violations of section 1030(a)(2). Section 2B2.3, trespass, governs violations of section 1030(a)(3). U.S. Sentencing Guideline section 2F1.1, fraud and deceit, governs violations of section 1030(a)(4). U.S. Sentencing Guideline section 2B1.3, property damage or destruction governs violations of section 1030(a)(5)(A). *Id.* at n.74.

²⁰⁸ *See* Nicholson et al., *supra* note 154, at 219.

²⁰⁹ *See Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses*, United States Sentencing Commission Report to Congress, (June 1996) [hereinafter *1996 Sentencing Commission Report to Congress*].

criminal behavior, including computer fraud.”²¹⁰ Thus, a Court will sentence an adult convicted of a subsection 1030 offense according to the statutory confines and the United States Sentencing Guidelines.

VI. CONVICTION AND SENTENCING OF JUVENILES FOR VIOLATING THE COMPUTER FRAUD AND ABUSE ACT – THE FEDERAL JUVENILE DELINQUENCY ACT

Juveniles, persons under age eighteen,²¹¹ who commit computer crimes, are not subject to direct prosecution under the Computer Fraud and Abuse Act. Rather, minors fall under the Federal Juvenile Delinquency Act (FJDA).²¹² Instead of charging a juvenile with directly violating a statute, the Attorney General prosecutes a juvenile for an act of juvenile delinquency. A person is a “juvenile delinquent” when he violates U.S. law, and his acts “would have been a [federal] crime if committed by an adult.”²¹³ The minor must commit the alleged offense prior to his eighteenth birthday to qualify for prosecution under the FJDA.²¹⁴

The purpose of the FJDA is to “remove juveniles from ordinary criminal process to avoid the stigma of a prior criminal conviction and to encourage treatment and rehabilitation.”²¹⁵ The act reflects the legally recognized belief that juveniles are less culpable than adults for their criminal acts, because they have poor judgment, lack experience,²¹⁶ and “as a class are less mature and responsible than adults.”²¹⁷ The Supreme Court has recognized that “youth crime . . . is not exclusively the offender’s fault; offenses by the young also represent a failure of family, school, and the social system, which share responsibility for the development of America’s youth.”²¹⁸ Thus, although “[c]rimes committed by youths may be just as harmful to victims as those committed by older persons, . . . they deserve less punishment because adolescents may have less capacity to control their conduct and to think in long-range terms than adults.”²¹⁹ The FJDA reflects this belief in that the Attorney General, normally, must proceed against a minor as a juvenile, not an adult. In addition, a juvenile delinquency adjudication is not a criminal conviction, but merely an adjudication of status.²²⁰

To gain jurisdiction over a minor, the Attorney General must follow the certification procedures laid out in the first unnumbered paragraph of section 5032. Section 5032 requires the Attorney General to certify one of three things to gain jurisdiction: that the state juvenile or other court does not have, or refuses to assume jurisdiction; that the state does not have adequate programs and services available to meet the minor’s needs; or that the offense charged is a firearms, drug trafficking or importation offense, or a violent felony and there is a substantial

²¹⁰ See 1996 Sentencing Commission Report to Congress, *supra* note 181.

²¹¹ 18 U.S.C.A. § 5031 (2000).

²¹² 18 U.S.C.A. § 5031-5042 (2000).

²¹³ § 5031.

²¹⁴ § 5031.

²¹⁵ See Amy J. Standefer, *The Federal Juvenile Delinquency Act: A Disparate Impact On Native American Juveniles*, 84 MINN. L. REV. 473, 478 (1999).

²¹⁶ *Id.*

²¹⁷ See *Thompson v. Oklahoma*, 487 U.S. 815, 834 (1987).

²¹⁸ See *Thompson*, 487 U.S. at 834 (citing *Eddings v. Oklahoma*, 445 U.S. 104, 115 (1979)).

²¹⁹ See *Thompson*, 487 U.S. at 834.

²²⁰ See Standefer, *supra* note 183, at 482.

Federal interest.²²¹ Examples of a substantial Federal interests include “assault on, or assassination of a Federal official, an aircraft hijacking, a kidnapping involving the crossing of State boundaries, a major espionage or sabotage offense, participation in large-scale drug trafficking, or significant and willful destruction of property belonging in to the United States.”²²² In the end, if the Attorney General fails to follow these certification procedures, the minor “shall be surrendered to the appropriate legal authorities of such state.” The FJDA’s certification requirement exhibits a belief that state authorities best handle juvenile matters,²²³ and exhibits a “clear congressional intent to limit the types of cases that the executive should bring in federal court.”²²⁴

The FJDA also provides procedures to place minors back into the Federal criminal system, by providing for discretionary transfer to adult criminal court on a case by case basis. On motion of the minor or Attorney General, the district court may conduct a hearing and determine whether transfer is “in the interest of justice.”²²⁵ In making this determination the judge “shall” consider the minor’s age, social and juvenile delinquency background, the nature of the offense, intellectual and psychological maturity, availability and amenability to treatment, among others.²²⁶

After adjudication, the district court must hold a dispositional hearing to sentence the minor.²²⁷ At the hearing the court has four options for sentencing. The court may “suspend the findings of juvenile delinquency, order the minor to pay restitution, place the minor on probation, or place the minor in a juvenile detention center.”²²⁸ Because section 5037 provides separate sentencing rules for minors under age eighteen at the time of disposition and minors between ages eighteen and twenty-one, the court must consider a juvenile’s age at the dispositional hearing when determining a minor’s sentence. For example, a person who committed a crime while under age eighteen, but who is between eighteen and twenty-one at the time of disposition is to be sentenced under the FJDA’s provisions for this age group.²²⁹

²²¹ 18 U.S.C.A. § 5032 (2000).

²²² See Standefer, *supra* note 183, at n.25 (citing H.R. Rep. No. 980103, reprinted in 1984 U.S.C.C.A.N. 3182, 3529).

²²³ *Id.* at n.26.

²²⁴ See Standefer, *supra* note 183, at n.26 (quoting Major Richard L. Palmatier, Jr., *Criminal offenses by Juveniles on the Federal Installation: A Primer on 18 U.S.C. § 5032*, ARMY LAW., Jan 1994 at 3).

²²⁵ § 5032.

²²⁶ § 5032. Whether the Attorney General may motion to transfer a minor depends on the minor’s age and the offense alleged. *Id.* The Attorney General may motion to transfer when the juvenile is fifteen years or older and the alleged crime involves a firearm, controlled substance violation, or violent offense. *Id.* Where the juveniles is alleged to have committed an enumerated crime of violence the Attorney General may motion for transfer when the juvenile is thirteen years of age or older. *Id.* The FJDA does not place an age limit at which a juvenile may request transfer.

The FJDA also contains provisions for mandatory transfer. *Id.* In these situations the juvenile is automatically transferred to the adult criminal system under certain circumstances. While a juvenile alleged to have committed a section 1030 offense may qualify for discretionary transfer, mandatory transfer does not apply because section 1030 is not specifically named by the FJDA.

²²⁷ 18 U.S.C.A. § 5037 (2000) (requiring a dispositional hearing no later than twenty court days after the juvenile delinquency hearing).

²²⁸ § 5037(a).

²²⁹ See *U.S. v. Doe*, 631 F.2d 110 (9th Cir. 1980) *cert. denied* 449 U.S. 867.

After determining the minor's age at disposition, the court may sentence a minor under eighteen at the time of disposition to serve probation until he or she turns twenty-one, or the maximum amount a similarly situated adult would receive, whichever is less.²³⁰ A minor between eighteen and twenty-one years of age at disposition, may receive three years or the maximum amount of probation authorized for a similarly situated adult, whichever is shorter.²³¹ For example, the Ninth Circuit in *United States v. Gonzales-Cervantes*²³² held that a juvenile "can be given a term of probationary sentence equal to that which an adult could receive."²³³ Based on this principle, the court upheld the district court's imposition of a probationary period that extended beyond the maximum prison sentence authorized for a similarly situated adult, but was less than the five year maximum probationary sentence for an adult.²³⁴

If the judge decides to imprison a juvenile younger than eighteen he or she has two options. The judge may order incarceration until age twenty-one, or up to the maximum amount of prison time authorized for a similarly situated adult, whichever is less.²³⁵ At bottom, a minor sentenced prior to his or her eighteenth birthday cannot be sentenced past age twenty-one. But, in determining the appropriate amount of incarceration, the court must look to the United States Sentencing Guidelines. A minor may not receive more than the maximum sentence permitted by the Guidelines.²³⁶ The Guidelines "tie the maximum sentence for juveniles to the maximum for adults, rather than making juvenile sentences more severe than adult sentences."²³⁷ For example, in *United States v. R.L.C.*, the district court sentenced the minor to three years, the maximum amount allowed under the underlying statute. The Eighth Circuit reversed, imposing the maximum allowable sentence under the Guidelines of twenty-one months.²³⁸ However, regardless of the proper Guideline amount, a court may not incarcerate a minor, sentenced while under age eighteen, past age twenty-one. In sum, the section 5037 mandate that detention shall not exceed the "maximum term of imprisonment that would be authorized if the juvenile had been tried and convicted as an adult[,] refers to the maximum length of sentence to which a similarly situated adult would be subject if convicted of the adult counterpart of the offense and sentenced under the statute requiring application of the Guidelines."²³⁹

If the minor is between eighteen and twenty-one at disposition, he or she may receive up to five years if the underlying offense was a Class A, B, or C felony. So, a juvenile who commits a Class A, B or C felony, any felony for which the adult punishment exceeds ten years,²⁴⁰ may receive up to five years in prison, which would leave the minor in jail beyond his or her twenty-first birthday. For minors between eighteen and twenty-one committing other underlying crimes, they may receive no more than three years, or the maximum term of imprisonment allowed by the Guidelines for a similarly situated adult, whichever is less.²⁴¹

²³⁰ § 5037(b)(1)(A)-(B).

²³¹ § 5037(b)(2)(A)-(B).

²³² 668 F.2d 1073 (9th Cir. 1982).

²³³ *Id.* at 1076.

²³⁴ *Id.* at 1077.

²³⁵ § 5037(c)(1)(A)-(B).

²³⁶ *See United States v. R.L.C.*, 503 U.S. 291, 305 (1992).

²³⁷ *See R.L.C.*, 503 U.S. at 304.

²³⁸ *Id.* at 295-96.

²³⁹ *Id.* at 306.

²⁴⁰ 18 U.S.C.A. § 3559(a)(1)-(3).

²⁴¹ § 5037(c)(2)(A), (B)(i)-(ii).

The following example applies the foregoing principles of federal computer and juvenile law by applying the Computer Fraud and Abuse Act and the FJDA to a sixteen year-old named Mike, living in Fairfax, Virginia, accused of violating section 1030(a)(5)(B) for entering Wake Forest's computer system and removing parts of the operating system from numerous computers in the computer science department's lab, causing the cancellation of several computer classes and impeding several others. The evidence also showed that Mike gained access using a password given to him by a friend at the university. Finally, the FBI tracked down Mike's friend at Wake Forest, who told them he gave the password to Mike and asked him to do something bad to the computer science department in retaliation for his D+ on his Computer Science 101 exam.²⁴² As a result of his action, Wake Forest had to rebuild their operating system and reissue more than 1,500 user-identifications, costing close to \$6,300.

Thus, the Attorney General has the burden of proving that the young man intentionally accessed a protected computer without authorization and as a result recklessly caused damage.²⁴³ Based on these facts it appears that Mike "intentionally accessed," by obtaining and using a password from a friend at the university to enter the computer science department's system. In addition, Mike was not authorized, because he was not a student at the university, indeed he had no affiliation with the university save a few high school friends. Mike also meets the damage element, because his acts resulted in the removal of parts of the system's operating system. To fix the damage Wake Forest had to rebuild the operating system and reissue more than 1,500 user identifications. This will cost more than \$6,300. Mike's acts also interrupted class. Finally, the statement by Mike's friend makes it look as though the juvenile went into the computer system intending to damage it in some manner. Thus, the evidence seems to show intentional damage, but at the least should show "reckless" damage.

Once the Attorney General determines that he or she should prosecute the case under federal law, he or she must go through certification procedures under section 5032. The Attorney General may show that that the state juvenile or other court does not have, or refuses to assume jurisdiction, or that the state does not have adequate programs and services available to meet Mike's needs. In this case, assume the Attorney General has proof that the Virginia juvenile court has refused to take jurisdiction over the young man.²⁴⁴

Once certified, Mike would have a juvenile delinquency hearing. Based on the evidence the court will probably adjudicate him a juvenile delinquent, because if an adult, he would have violated section 1030(a)(5)(B). Then, less than twenty court days from this adjudication, the court would hold a dispositional hearing to sentence Mike. Because Mike is still sixteen, he falls under the rules set down for minors under age eighteen at disposition. The judge may fine the juvenile, or impose probation. But, assuming the judge determines incarceration is necessary he

²⁴² While this raises issues of conspiracy and accomplice liability, among others, for purposes of this example, I am going to stick to the basics to demonstrate federal juvenile procedures.

²⁴³ § 1030(a)(5)(B).

²⁴⁴ The Attorney General cannot get certification under section 5032's provision allowing certification where the offense charged is a firearms, drug trafficking or importation offense, or a violent felony and there is a substantial Federal interest. As the law stands today, computer hacking does not fall under any one of these categories. Therefore the Attorney General must proceed under a theory of state abandonment, as our fictitious Attorney General has.

must consult the Guidelines section 2B1.3²⁴⁵ to figure a sentencing range for a similarly situated adult. Section 2B1.3 begins with a base level of four (4).²⁴⁶ It then adds levels for specific offense characteristics.²⁴⁷ First, the loss table in section 2B1.1 adds 4 levels to the base, because Mike caused more than \$5,000 of damage.²⁴⁸ Second, because the offense involved more than minimal planning we add two more points.²⁴⁹ In the end, we have an offense level of ten, with a notation that “[i]f the defendant is convicted under 18 U.S.C. § 1030(a)(5), which Mike was, the minimum guideline sentence, notwithstanding any other adjustment, shall be six months’ imprisonment.”²⁵⁰ Thus, assuming no prior convictions, our similarly situated adult would have an offense level of ten (10), which translates into between a six (6) and twelve (12) month sentence. Now, section 5037 and *R.L.C.* allows the court to impose detention not to extend beyond the minor’s twenty-first birthday, or the maximum term authorized by the Guidelines for a similarly situated adult, whichever is less. So, Mike may receive detention not to exceed twelve months.²⁵¹

VI. SUGGESTIONS FOR REFORM

Reformers in the juvenile computer crime debate call for more punitive measures. For example, Senator Schumer introduced a bill that would authorize the federal prosecution of juveniles for felony violations of 18 U.S.C. 1030 without certification that the state does not have or declines prosecution, as is required for crimes other than drug and violent crimes. Other suggestions for reform include parental liability to force parents to take control of their children to protect society, greatly restricted computer and modem use, and limited ability to enter the computer industry as an employee.

VIII. INTERSECTION OF VIRGINIA AND FEDERAL LAW

Both Virginia and the federal government will in most cases reject jurisdiction if assumed by the other. Under federal law to take jurisdiction over a case involving a juvenile, the Attorney General must certify that the state juvenile or other court does not have, or refuses to assume

²⁴⁵ THOMAS W. HUTCHISON, ET AL., FEDERAL SENTENCING LAW AND PRACTICE § 2B1.3(a) (2000).

²⁴⁶ *Id.*

²⁴⁷ See HUTCHISON, *supra* note 213, § 2B1.3(b).

²⁴⁸ *Id.* at § 2B1.1, § 2B1.3(b)(1).

²⁴⁹ *Id.* § 2B1.3(b)(3).

²⁵⁰ See HUTCHISON, *supra* note 213, § 2B1.3(d)(1).

²⁵¹ The court may depart from this if it finds “an aggravating or mitigating circumstance of a kind, or degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines that should result in a sentence different from that described.” See *R.L.C.*, 503 U.S. at 304.

jurisdiction. So the Attorney General may take jurisdiction over the juvenile if the state waives jurisdiction. Similarly, under the Virginia code “[j]urisdiction of cases involving federal law by a child shall be concurrent and shall be assumed if waived by the federal court or the U.S. attorney.”²⁵² So the federal government may take jurisdiction where Virginia refuses to do so, and Virginia may take jurisdiction of the case only if the federal government waives jurisdiction.

²⁵² Va. Code Ann. § 16.1-244(B) (Michie 2000).

APPENDIX

§ 8.01-328.1: When personal jurisdiction over person may be exercised

- A. A court may exercise personal jurisdiction over a person, who acts directly or by an agent, as to a cause of action arising from the person's:
1. Transacting any business in this Commonwealth;
 2. Contracting to supply services or things in this Commonwealth;
 3. Causing tortious injury by an act or omission in this Commonwealth;
 4. Causing tortious injury in this Commonwealth by an act or omission outside this Commonwealth if he regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in this Commonwealth;
 5. Causing injury in this Commonwealth to any person by breach of warranty expressly or impliedly made in the sale of goods outside this Commonwealth when he might reasonably have expected such person to use, consume, or be affected by the goods in this Commonwealth, provided that he also regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered in this Commonwealth;
 6. Having an interest in, using, or possessing real property in this Commonwealth;
 7. Contracting to insure any person, property, or risk located within this Commonwealth at the time of contracting;
 8. Having (i) executed an agreement in this Commonwealth which obligates the person to pay spousal support or child support to a domiciliary of this Commonwealth, or to a person who has satisfied the residency requirements in suits for annulments or divorce for members of the armed forces pursuant to § 20-97 provided proof of service of process on a nonresident party is made by a law-enforcement officer or other person authorized to serve process in the jurisdiction where the nonresident party is located, (ii) been ordered to pay spousal support or child support pursuant to an order entered by any court of competent jurisdiction in this Commonwealth having in personam jurisdiction over such person, or (iii) shown by personal conduct in this Commonwealth, as alleged by affidavit, that the person conceived or fathered a child in this Commonwealth; or
 9. Having maintained within this Commonwealth a matrimonial domicile at the time of separation of the parties upon which grounds for divorce or separate maintenance is based, or at the time a cause of action arose for divorce or separate maintenance or at the time of commencement of such suit, if the other party to the matrimonial relationship resides herein. Jurisdiction in subdivision 9 of this subsection is valid only upon proof of service of process pursuant to § 8.01-296 on the nonresident party by a person authorized under the provisions of § 8.01-320. Jurisdiction under subdivision 8 (iii) of this subsection is valid only upon proof of personal service on a nonresident pursuant to § 8.01-320.
- B. Using a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth. For purposes of this subsection, “use” and “computer network” shall have the same meanings as those contained in § 18.2-152.2.
- C. When jurisdiction over a person is based solely upon this section, only a cause of action arising from acts enumerated in this section may be asserted against him; however, nothing contained in this chapter shall limit, restrict or otherwise affect the jurisdiction of

any court of this Commonwealth over foreign corporations which are subject to service of process pursuant to the provisions of any other statute.

§ 18.2-152.2: Definitions

“Computer” means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term “computer” includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

“Computer data” means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. “Computer data” may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

“Computer network” means two or more computers connected by a network.

“Computer operation” means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A “computer operation” for a particular computer may also be any function for which that computer was generally designed.

“Computer program” means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

“Computer services” means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

“Computer software” means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

“Electronic mail service provider” means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end- users of electronic mail services the ability to send or receive electronic mail.

“Financial instrument” includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof.

“Network” means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.

“Owner” means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, or computer software.

“Person” shall include any individual, partnership, association, corporation or joint venture.

“Property” shall include:

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
 - a. Tangible or intangible;
 - b. In a format readable by humans or by a computer;
 - c. In transit between computers or within a computer network or between any devices which comprise a computer; or
 - d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

A person “uses” a computer or computer network when he:

1. Attempts to cause or causes a computer or computer network to perform or to stop performing computer operations;
2. Attempts to cause or causes the withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or
3. Attempts to cause or causes another person to put false information into a computer.

A person is “without authority” when (i) he has no right or permission of the owner to use a computer or he uses a computer in a manner exceeding such right or permission or (ii) he uses a computer, a computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.