

LEGAL IMPLICATIONS OF ACCESSING ELECTRONICALLY-STORED DATA

**Gregg L. Bernstein, Esq.
Peter Nothstein, Esq.¹**

I. EXPECTATIONS OF PRIVACY

A. Computers

1. In October, 2007, Judge John P. Miller of the Baltimore City Circuit Court held that a police lieutenant had a reasonable expectation of privacy in his privately owned laptop. The police internal affairs department had seized and then searched the laptop. The Court ruled that the police had not met their burden under the Fourth Amendment to justify the search. The Court did not address, however, the broader issue of the privacy implications when an employee voluntarily connects to an employer's network. The defendant was accused of using his computer to send sexually explicit emails, and access vulgar and explicit videos and web sites. *Daily Record, Week in Review - Legal Edition*, Oct. 9, 2007 [**Tab A**].
2. Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals' expectations of privacy in computers have been likened to their expectations of privacy in "a suitcase or briefcase." *United States v. Aaron*, 33 Fed. Appx. 180, 184 (6th Cir. 2006) (unpublished).
3. However, when dealing with the contents of a computer, the courts often look to measures taken by the owner to protect the contents. Password protection of files is often determinative of the expectation of privacy in computer files. Password-protected files have been compared to a "locked footlocker inside the bedroom." *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001). In *Trulock* roommates both used a computer located in one bedroom and each had joint access to the hard drive. Both protected their personal files with passwords; and did not have access to each other's passwords. Although one roommate had authority to consent to a general search of the computer, her authority did not extend to other roommate's password-protected files.
4. Defendant's wife had apparent authority to consent to search of her husband's password-protected files contained in home computer, and thus, evidence seized from

¹ Gregg Bernstein is a partner at Zuckerman Spaeder LLP. Peter Nothstein is an associate with the firm.

those files after wife consented to allow law enforcement officers to take computer and conduct complete search was not required to be suppressed; computer was leased in wife's name, it was located in common area of their home, and it was turned on when officers arrived at home even though defendant was not present at the time, such that it was objectively reasonable for officers to believe that wife had authority to consent to search of entire computer, including password-protected files, and during the forensic analysis of the computer itself, nothing the officers saw indicated that any computer files were encrypted or password protected. *United States v. Buckner*, 473 F.3d 551 (4th Cir. 2007).

5. Under totality of circumstances, Bureau of Immigration and Customs Enforcement (ICE) agents could reasonably have believed defendant's father had authority to consent to search of defendant's home computer, and thus, father had apparent authority to consent; although computer was in defendant's bedroom in his father's home rather than in common area, father had unlimited access to bedroom, and agents knew that father owned home and paid for home's internet service, and that email address associated with father was used to register on website that provided access to child pornography, computer was in plain view on desk and appeared available for use by household members, and although agents did not ask father about his use of computer, father said nothing indicating need for such questions. *United States v. Andrus*, 483 F.3d 711 (10th Cir. 2007).
6. City employee did not have reasonable expectation of privacy in personal computer that he brought to city hall for work-related use, hooked up to city's network for file sharing, kept continuously on, and failed to password protect or take any other steps to prevent third-party use despite computer's location in public area, and thus discovery of pornographic images on computer by another city worker was not a Fourth Amendment violation. *United States v. Barrows*, 481 F.3d 1246 (10th Cir. 2007).

7. Shared/Networked Computers

- a. The mere act of accessing a network does not, in itself, extinguish privacy expectations, nor does the fact that others may have occasional access to the computer. *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001).
- b. However, privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user. *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

B. E-mail

1. Sending

- a. Email is generally treated like letters or phone calls: there is an expectation of privacy in the contents of the communication, but not in the fact of a communication, such as when a call is made, or to whom an email is sent. However, many email technologies raise serious questions about how reasonable is the expectation of privacy. For instance, many ISPs run searches in email content to reveal viruses or unwanted “spam” messages. Likewise, some internet-based email services run text and keyword searches in message content to place targeted ads on the email interface. One could argue that because of these “searches” in email content, there truly is no expectation of privacy.
 - i. Similarly, with computer files, there are indexing and search programs that search all files on a hard drive, sometimes regardless of password protection. Those results may not be stored in a protected manner, possibly undermining the reasonable expectation of privacy in the contents.
- b. E-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties. Communication by both Internet and telephone requires people to “voluntarily turn[] over [information] to third parties.” *United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007)
- c. We have not addressed previously the existence of a legitimate expectation of privacy in text messages or e-mails. Those circuits that have addressed the question have compared e-mails with letters sent by postal mail. Although letters are protected by the Fourth Amendment, “if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery.” *United States v. Jones*, 149 Fed. Appx. 954 (11th Cir. 2005) (quoting *United States v. King*, 55 F.3d 1193, 1195-96 (6th Cir. 1995))
- d. The transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny. *United States v. Maxwell*, 45 M.J. 406, 418 (U.S.A.F.1996)
- e. In *Warshak v. United States*, a panel of the Sixth Circuit held, in interpreting the Stored Communications Act, that individuals have an expectation of privacy in the contents of their emails. *Warshak v. United States*, 06-4092, slip op. at 12 (6th

Cir. June 18, 2007). The court also held that there is no expectation of privacy in the facts of the transmission: to whom the message is sent and when. The Sixth Circuit recently vacated its decision and agreed to hear the case *en banc*.

2. Received/Stored -

- a. A person's reasonable expectation of privacy may be diminished in “transmissions over the Internet or e-mail that have already arrived at the recipient.” *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007)
- b. Similarly, an individual sending an e-mail loses “a legitimate expectation of privacy in an e-mail that had already reached its recipient.” *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004)

II. FEDERAL STATUTES

A. **Electronic Communications Privacy Act (18 U.S.C. §§ 2510, et. seq.) (also known as the “Wiretap Act”) [Tab B]**

1. Prohibits (18 U.S.C. § 2511):

- a. Interception of wire, oral or electronic communications, or use of a device to intercept such communications.
- b. Disclosure of the contents of a communication, by any person knowing or having reason to know that the information was obtained in violation of the section; or disclosure of communications obtained in a criminal investigation pursuant to this section.
 - i. Willful disclosure or use of information by a law enforcement officer or governmental entity beyond the extent permitted is a violation for purposes of the civil action (below) (18 U.S.C. § 2520(g)).
- c. Use of the contents of a communication, by any person knowing or having reason to know that the information was obtained by interception in violation of the section.

2. Definitions: (18 U.S.C. § 2510)

- i. “Intercept”: means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device
 1. There is a temporal requirement to “interception” wherein the “acquisition” must take place contemporaneously with the transmission of the message.
 2. Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication" (part of the definition of "wire communication") reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage." *Steve Jackson Games*, 36 F.3d at 461-62; *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir.1998)

- ii. “Contents”: when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.
- iii. “Electronic communication”: means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--
 - 1. Any wire or oral communication;
 - 2. Any communication made through a tone-only paging device;
 - 3. Any communication from a tracking device (as defined in section 3117 of this title); or
 - 4. Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
- iv. “Electronic communications system”: means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;
- v. “Electronic communication service”: means any service which provides to users thereof the ability to send or receive wire or electronic communications;
- vi. “Person”: means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation
- vii. “Use”: Not defined in the statute, and courts have taken different approaches. Some have interpreted the term as passive, allowing for simple listening to satisfy “use” with others requiring a more active “use”:
 - 1. The District Court of Utah has held that “use” is satisfied when “the contents of . . . wiretapped conversations were relied upon in formulating . . . expert opinions,” as well as discussion of the contents of the illegally wiretapped communications with other parties. The court took a relatively broad reading of the term “use,” stating: “[t]his Court thinks that it strains logic to conclude

that reading a document or listening to a tape does not amount to ‘use’ of those items.” *Thompson v. Dulaney*, 838 F.Supp. 1535, 1547 (D. Utah 1993).

2. The Sixth Circuit in *Dorris v. Absher* relied on the dictionary definition of “use,” specifically “to put into action or service.” 179 F.3d 420, 426 (6th Cir. 1999). The court disagreed with *Thompson* in holding that “listening alone is insufficient to impose liability for “using” illegally intercepted communications.” *Id.*

3. Evidentiary Prohibition (18 U.S.C. § 2515)

- a. No intercepted communication, or part thereof or evidence derived therefrom, are admissible as evidence at any hearing or government proceeding, if obtained in violation of the Wiretap Act.

4. Permissible Disclosure (18 U.S.C. § 2517)

- a. A person who has received wire, oral or electronic communication, by means authorized by the Wiretap Act, may disclose the information.
- b. A privileged communication does not lose its privileged character because it was obtained in violation of the chapter.

5. Civil Action (18 U.S.C. § 2520)

- a. Any person whose communication is intercepted, disclosed, or intentionally used in violation of the chapter has a civil cause of action against any entity (other than the United States) for:
 - i. Preliminary or equitable relief;
 - ii. Actual damages:
 1. If the violation is for viewing or interception of communications on non-scrambled or non-encrypted private satellite video feed or radio communication, and the conduct is not for a tortious or illegal purpose or for purposes of commercial advantage or gain, damages are:
 - a. For first offense: the greater of actual damages and statutory damages between \$50 and \$500.
 - b. For second offense: the greater of actual damages and statutory damages between \$100 and \$1000.

2. For any other action, the court can assess the greater of:
 - a. The sum of actual damages to the plaintiff and profits made as a result of the violation; or
 - b. Statutory damages: the greater of \$100 per day or \$10,000.
- iii. Punitive damages;
- iv. Attorney's fees and costs.
- b. Good faith reliance on a court order, warrant, subpoena, legislative authorization, request of law enforcement under § 2518(7), or good faith determination that the Wiretap Act allowed the conduct in question.
- c. Statute of limitations is two years.

B. Federal Stored Wire and Electronic Communications and Transactional Records Act (18 U.S.C. §§ 2701, *et seq.*) [Tab C]

- a. Prohibits (18 U.S.C. § 2701):
 - i. Access without authorization (or exceeded authorization) of a facility through which an electronic communication service is provided; and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.
 - ii. Disclose the contents of stored communications, unless to an intended recipient, as necessary to provide service, by consent, or to law enforcement.
- d. Definitions:
 - i. "Access": The Act does not define "access," but at least one court has held that "access" is identical to "intercept" under the federal wiretapping statute when the communication in question was intercepted or accessed while not in transmission. *United States v. Moriarty*, 962 F. Sup. 217, 221 (D. Mass. 1997). The court noted that "[t]here may well be a factual distinction . . . between accessing a voice mail (or e-mail) system . . . and actually listening to (or reading) stored messages. Yet these acts are simply aspects of 'access.'" *Id.*
 1. The Ninth Circuit has held somewhat differently. First, the court held that "access" shall be given its plain meaning: "to get at" or

“gain access to.” *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998); *Crowley v. CyberSource Corp.*, 166 F.Supp.2d 1263, 1271 (N.D.Cal. 2001). Part of the Ninth Circuit’s reasoning is that “access” in violation of 18 U.S.C. § 2701 is a lesser included offense (or tort) of “interception” in violation of the Wiretap Act, 18 U.S.C. § 2510, because “[t]he word “intercept” entails actually acquiring the contents of a communication, whereas the word “access” merely involves being in position to acquire the contents of a communication.” *Smith*, 155 F.3d at 1058.

- ii. “Electronic storage” (18 U.S.C. § 2510): means --
 1. any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
 2. any storage of such communication by an electronic communication service for purposes of backup protection of such communication.
- iii. “Facility”
 1. There is no definition of “facility” in the Stored Communications Act or the Wiretap act, and there do not seem to be cases defining the term. However, in the criminal title, there is a definition of “wire communication facility” that may be instructive. The gambling subsection defines a “wire communication facility” as “any and all instrumentalities, personnel, and services (among other things, the receipt, forwarding, or delivery of communications) used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission.” 18 U.S.C. § 1081.
 2. Taking from this definition the “wire communication” aspects, it would appear that “facility” could have a very broad definition, encompassing “any and all instrumentalities, personnel, and services (among other things, the receipt, forwarding, or delivery of communications) used or useful in the transmission of writings, signs, pictures, and sounds of all kinds.”
 3. However, at least one court has held that a “facility” can be as simple as a computer’s security software. The use of special software to evade the Internet service provider’s filtering mechanisms violated the Act’s prohibition of impairment of

computer facilities. The defendants were web site operators who maintained membership with the service provider but, the court held, abused the membership by sending unauthorized and unsolicited spam e-mail to other service provider customers. *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998).

4. The question of whether a personal computer is a facility is somewhat of an open one, though a few courts have held that it is or could be. In *In re Toys R Us, Inc., Privacy Litigation*, 2001 WL 34517252 (N.D. Cal. 2001) (unpublished), the court stated:
 - a. Toys R Us argues that “facility” cannot refer to a personal computer. Toys R Us, however, cites no cases in which such a limited interpretation of “facility” has been accepted. Moreover, cases cited by Toys R Us, on other issues, have rejected, either expressly or implicitly, such a theory. *See, e.g., Chance v. Avenue A, Inc.*, No. C00-1464C, slip op. at 11 (W.D. Wash.2001) (holding plaintiffs offered sufficient evidence to prove individual computers are “facilities”); *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 508 (S.D.N.Y.2001) (implicitly holding personal computer could be “facility;” stating “[a]ssuming that the communications are considered to be in ‘electronic storage,’ it appears that plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under § 2701(a), absent [a statutory exception]”).
5. In *DoubleClick*, the court did not analyze whether a PC could be a facility, but stated: “plaintiffs argue that “[t]he individual plaintiff (‘user’) owns the personal computer (‘facility’), while the Web sites she visits do not.” 154 F. Supp. 2d at 508. In *Chance v. Avenue A, Inc.*, the Western District of Washington held that individual computers could be facilities:
 - a. While both parties agree that Internet service providers are “facilities” covered by the Act, they dispute whether a user's individual computer provides any “electronic communication service.” Viewing this factual dispute in the light most favorable to the nonmovant, as is required on summary judgment, it is possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under

the Act. Although this observation of the disputed facts initially works in Plaintiffs' favor, the subsequent implications of this rather strained interpretation of a "facility through which an electronic communication service is provided" are fatal to their cause of action. 165 F.Supp.2d 1153, 1160-61 (W.D. Wash. 2001).

6. However, in *In re Pharmatrak, Inc. Privacy Litigation*, 220 F.Supp.2d 4 (D. Mass. 2002) vacated on other grounds), the court stated that: "Defendants are correct that an individual Plaintiff's personal computer is not a "facility through which an electronic communication service is provided" for the purposes of § 2701." *Id.* at *2. The Court's reasoning was as follows:
 - a. Plaintiffs find it noteworthy that "[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications," and that "[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications." Fair enough, but without a telephone, most consumers would not be able to access telephone lines, and without televisions, most consumers would not be able to access cable television. Just as telephones and televisions are necessary devices by which consumers access particular services, personal computers are necessary devices by which consumers connect to the Internet. While it is possible for modern computers to perform server-like functions, there is no evidence that any of the Plaintiffs used their computers in this way. While computers and telephones certainly provide services in the general sense of the word, that is not enough for the purposes of the ECPA. The relevant service is Internet access, and the service is provided through ISPs or other servers, not though Plaintiffs' PCs.
 - b. "Punishment" (18 U.S.C. § 2701(b)): If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act
 - i. First offense: a fine and/or imprisonment for up to 5 years,
 - ii. Second offense: a fine under and/or imprisonment for up to 10 years
 - iii. In any other case:

7. First Offense: a fine and/or imprisonment for not more than 1 year
 8. Second offense: a fine and/or imprisonment for not more than 5 years
- iv. Disclosure:
- c. Civil Action (18 U.S.C. § 2707): Any person or entity aggrieved by a knowing or intentional violation of this chapter may, recover
- i. Preliminary and other equitable or declaratory relief;
 - ii. Actual damage suffered and any profits made by the violator as a result of the violation, but no less than \$1,000;
 - iii. Punitive damages, if the violation is willful or intentional;
 - iv. Attorney's fees and costs.
 - v. Defense: A good faith reliance on a court warrant or order, or other official order, or request of law enforcement officer is a complete defense.
 - vi. Statute of limitation is two years

C. Computer Fraud and Abuse Act (18 U.S.C. § 1030) [Tab D]

1. Prohibits (18 U.S.C. § 1030(a)): one who knowingly accessed a computer without authorization or exceeding authorized access, obtains government information. However, also prohibits unauthorized access of financial record of a financial institution, of a credit card issuer, or contained in a file of a consumer reporting agency.
2. Penalty (18 U.S.C. § 1030(c)):
 - a. First offense: a fine and/or imprisonment for not more than one year; or
 - i. A fine and/or imprisonment for not more than 5 years, if (i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds \$5,000.
 - b. Second offense: a fine and/or imprisonment for not more than ten years, or both.
3. Definitions (18 U.S.C. § 1030(e)(6)):

- a. "Exceeds authorized access": means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.
4. Civil Action (18 U.S.C. § 1030(g):
- a. Those who are damages by a violation of the section have a civil cause of action, and can obtain compensatory damages, injunctive or other equitable relief. Damages are limited to economic damages.
 - b. Statute of limitations is 2 years.

D. Case Law Interpreting Terms

- a. Access:
 - i. SCA's prohibition against "accessing" computers can be violated when someone sends an e-mail message from his own computer which is then transmitted through other computers until it reaches its destination, thereby making use of, or "accessing," all those computers.
 - ii. Bulk e-mailers ("spammers") sent unauthorized and unsolicited bulk advertisements for its discount optical and dental service plans to service provider's customers, but genuine issues of fact prevented summary judgment. The court questioned whether the service provider's members harvesting of member e-mail addresses from the system so as to send unsolicited advertising, though clearly in violation of the service provider's membership agreement, constituted "unauthorized access." *America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255 (N.D. Iowa 2000),
 - iii. Unauthorized use of special programs known as "search robots" to extract names of new registrants to the Internet from an Internet domain name registrar's customer lists, constituted access. *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000).
 - iv. Regardless of whether operator's use agreement created an enforceable contract for purposes of a breach of contract claim pursuant to state law, defendant software licensee knew that operator prohibited the use of "any deep-link, page-scrape, robot, spider or other automatic device, program, algorithm or methodology" which defendant's software did. *Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004).

b. Standing of non-owners

- i. Computer Fraud and Abuse Act, providing cause of action against any person who intentionally accesses a computer without authorization or exceeds authorized access, and obtains protected information, was not restricted to computer's owner, and could extend to provide cause of action for unauthorized access to information stored on a third party's computer. *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

a. Authorized users - acting without authorization

- i. A user, authorized to use one computer, acts "without authorization" when using that computer to access another, which it has no authorization to do so.
- ii. Although acknowledging that Congress was primarily aiming at "outsiders" when it drafted this subsection, the court noted that its coverage was not limited to "outsiders," and therefore even someone with some authorization for access to one computer, may violate its proscriptions when he accesses others. *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991),
- iii. Employees were "without authorization" to access information from their employer's computers when they began to appropriate the employer's trade secrets for the benefit of the competitor. The court applied principles of agency law to conclude that the employees' authorized access to the employer's computers ended at the moment when they became agents of the competitor and began appropriating information from the employer's computer for the competitor's benefit. *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000)
- iv. Internet dating service was entitled to a temporary restraining order prohibiting a former programmer from hacking its website and diverting its clients and users to a pornography website. *YourNetDating, Inc. v. Mitchell*, 88 F. Supp. 2d 870 (N.D. Ill. 2000).
- v. Former chief executive officer (CEO) had not been authorized to take proprietary information and delete relevant electronic files. Although CEO deleted files while still officer and director of corporation; CEO breached his duty of loyalty and terminated his agency relationship to company when he decided to delete all information from corporation's server and his company computer night before his termination and after knowing that he was being asked to step down and give up his duties. *ViChip Corp. v. Lee*, 438 F. Supp. 2d 1087 (N.D. Cal. 2006).

III. MARYLAND STATUTES

A. **Maryland Wiretapping Statute (MD. CODE ANN., CTS. & JUD. PROC, §§ 10-401, et seq.) [Tab E]**

1. Prevents (§ 10-402(a)): Prevents:

- a. Willful *intercepting, divulging or using* (or endeavoring to do the same) oral, wire and electronic communications, or divulging contents of intercepted communications, by those knowing or having reason to know that the information was intercepted unlawfully.

2. Definitions (§ 10-401) (applies to both Maryland statutes)

- a. "Intercept": means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
- b. "Electronic communication": means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system.
 - i. "Electronic communication" does not include:
 1. The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; any wire or oral communication; any communication made through a tone-only paging device; or any communication from a tracking device.
- c. "Electronic communications system": means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of electronic communications.
- d. "Electronic communication service": means any service that provides to users of the service the ability to send or receive wire or electronic communications.
- e. "Electronic storage": means --
 - i. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission of the communication; and

- ii. Any storage of a wire or electronic communication by an electronic communication service for purposes of backup protection of the communication.
3. Penalty (§ 10-402(b)): Up to 5 years imprisonment and/or \$10K fine.
4. Civil Liability (§ 10-410): There is a cause of action for violation of the statute, and can recover:
 - a. Actual damages, but not less than liquidated damages, calculated at \$100 per day or \$1,000, whichever is higher.
 - b. Attorneys fees and costs
 - c. Good faith reliance on court order is a complete defense.
5. Evidence (§ 10-405): Illegally intercepted communications are generally not admissible before any state authority.
6. Privilege (§ 10-407(d)): The privileged character of a communication not lost if intercepted, legally or illegally.

B. Maryland Stored Communications Act (MD. CODE ANN., CTS. & JUD. PROC, §§ 10-4A-01, *et seq.*) [Tab F]

1. Prevents (§ 10-4A-02(a)): A person may not
 - a. Obtain, alter, or prevent access to electronically stored wire or electronic communications by intentionally accessing a facility through which an electronic communication service is provided without authorization or by intentionally exceeding authorization.
 - b. Divulge the contents of an electronic communication, but may do so: to an addressee or intended recipient, or a subscriber of an electronic communication service, to law enforcement, or as necessarily incident to the rendition of services, etc. (§ 10-4A-03)
2. Penalties (§ 10-4A-02(b)): If done for “commercial advantage, malicious destruction or damage, or private commercial gain”:
 - a. First offense: \$250K fine and/or 1 year imprisonment;
 - b. Second offense: \$250K fine and/or up to 2 years in prison.
 - c. In any other case, \$5K fine and/or up to 6 months in prison

3. Civil Actions (§ 10-4A-08): a person or entity aggrieved by a knowing or intentional violation of the subtitle has a cause of action against the person or entity that engaged in the violation, for:
 - a. Preliminary and equitable relief,
 - b. Actual damages to the plaintiff , plus any profits made by violator as a result of the violation, but in no case shall it be less than \$1,000.
 - c. Punitive damages
 - d. Attorneys fees and costs.
 - a. Defense: good faith reliance on court order, warrant, subpoena, legislative authorization, or good faith determination that action was allowed by 10-402(d) permitted action is a complete defense
 - b. Statute of limitations is 2 years.

IV. ETHICAL IMPLICATIONS

1. There were no decisions or other guidance relating directly to electronic communications, but as email and other electronic data is commonly analogized to tangible property, the ethics rules with regard to handling incriminating evidence from a client is instructive. Generally, Maryland and almost all other jurisdictions require an attorney who receives incriminating evidence from a client to turn it over to the authorities. This would thus seem to apply to communications or electronic data that has come into a client's possession in violation of one of the laws above.
2. Maryland Rule of Professional Conduct (identical to the Model rule) states:
 - a. Rule 3.4 Fairness to Opposing Party and Counsel
 - i. A lawyer shall not: unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;
3. Under Maryland law, as in most other jurisdictions, “[i]t is an abuse of a lawyer's professional responsibility knowingly to take possession of and secrete the fruits and instrumentalities of a crime. [The attorney's] acts bear no reasonable relation to the privilege and duty to refuse to divulge a client's confidential communication.” *Rubin v. State*, 325 Md. 552, 602 A.2d 677, 686-87 (Md.,1992) (citations omitted). Therefore, “physical evidence of crime in the possession of a criminal defense attorney is not subject to a privilege but must be delivered to the prosecution.” *Id.* (citing *Commonwealth v. Stenhach*, 514 A.2d 114, 119 (Pa. 1986))
4. There appears to be no Maryland precedent that deals directly with the attorney's obligations if presented with a communication or electronically stored data that has been obtained in violation of one of the rules above. However, as noted in *Rubin*, Maryland does follow the majority rule that the attorney must disclose evidence to the authorities.
 - a. Destruction of Evidence - Attorney Guilty of Misprision of a Felony
 - i. In February, 2007, Connecticut lawyer Phillip Russell pleaded guilty to misprision of a felony in the U.S. District Court in Connecticut. *See [Tab G]* Russell represented a church in Greenwich, CT that had discovered child pornography on an employee's computer. The church had taken possession of the computer and wrapped it up, “treating it as evidence.” Plea Agreement *[Tab H]* at 9. Russell confronted the employee, advised

him that the possession of the images was a federal crime, and referred him to a criminal defense lawyer. Russell then took possession of the computer, dismantled, and then destroyed it, without informing any government official of the commission of a crime.

- ii. In his order denying Russell's motion to dismiss the indictment, Judge Nevas stated that although Russell claimed to have no knowledge of any official proceeding against the employee, the facts as alleged by the complaint, particularly the type of criminal exposure, the fact that Russell knew it to be a crime and referred the employee to a criminal defense attorney sufficiently alleged a "nexus between Russell's conduct and an official proceeding or investigation." See [Tab I] at 18. Ultimately, the court noted, the jury would have to decide if the official proceeding was foreseeable or anticipated by Russell. *Id.* at 14.

5. ALI Restatement of the Law, The Law Governing Lawyers

- a. § 119 Physical Evidence of a Client Crime: With respect to physical evidence of a client crime, a lawyer:
 - i. May, when reasonably necessary for purposes of the representation, take possession of the evidence and retain it for the time reasonably necessary to examine it and subject it to tests that do not alter or destroy material characteristics of the evidence; but
 - ii. Following possession under Subsection (1), the lawyer must notify prosecuting authorities of the lawyer's possession of the evidence or turn the evidence over to them.

6. ABA Standards for Criminal Justice, Defense Function

- a. Defense Standard 4-4.6 provides:
 - i. Defense counsel who receives a physical item under circumstances implicating a client in criminal conduct should disclose the location of or should deliver that item to law enforcement authorities only: (1) if required by law or court order, or (2) as provided in paragraph (iv).
 - ii. Unless required to disclose, defense counsel should return the item to the source from whom defense counsel received it, except as provided in paragraph (iii) and (iv). In returning the item to the source, defense counsel should advise the source of the legal consequences pertaining to possession or destruction of the item. Defense counsel should also prepare a written

record of these events for his or her file, but should not give the source a copy of such record.

- iii. Defense counsel may receive the item for a reasonable period of time during which defense counsel: (1) intends to return it to the owner; (2) reasonably fears that return of the item to the source will result in destruction of the item; (3) reasonably fears that return of the item to the source will result in physical harm to anyone; (4) intends to test, examine, inspect, or use the item in any way as part of defense counsel's representation of the client; or (5) cannot return it to the source. If defense counsel tests or examines the item, he or she should thereafter return it to the source unless there is reason to believe that the evidence might be altered or destroyed or used to harm another or return is otherwise impossible. If defense counsel retains the item, he or she should retain it in his or her law office in a manner that does not impede the lawful ability of law enforcement authorities to obtain the item.
- iv. If the item received is contraband, i.e., an item possession of which is in and of itself a crime such as narcotics, defense counsel may suggest that the client destroy it where there is no pending case or investigation relating to this evidence and where such destruction is clearly not in violation of any criminal statute. If such destruction is not permitted by law or if in defense counsel's judgment he or she cannot retain the item, whether or not it is contraband, in a way that does not pose an unreasonable risk of physical harm to anyone, defense counsel should disclose the location of or should deliver the item to law enforcement authorities.