

6-11-2004

# Ethical Risks From the Use of Technology

Andrew Beckerman-Rodau

*Suffolk University Law School*, arodau@suffolk.edu

Follow this and additional works at: [http://lsr.nellco.org/suffolk\\_ip](http://lsr.nellco.org/suffolk_ip)



Part of the [Ethics and Professional Responsibility Commons](#), and the [Science and Technology Commons](#)

---

## Recommended Citation

Beckerman-Rodau, Andrew, "Ethical Risks From the Use of Technology" (2004). *Suffolk University Law School Intellectual Property*. Paper 7.

[http://lsr.nellco.org/suffolk\\_ip/7](http://lsr.nellco.org/suffolk_ip/7)

This Article is brought to you for free and open access by the Suffolk University Law School at NELCO Legal Scholarship Repository. It has been accepted for inclusion in Suffolk University Law School Intellectual Property by an authorized administrator of NELCO Legal Scholarship Repository. For more information, please contact [tracy.thompson@nellco.org](mailto:tracy.thompson@nellco.org).



## **ETHICAL RISKS FROM THE USE OF TECHNOLOGY**

By Andrew Beckerman-Rodau  
Suffolk University Law School – Boston, MA  
E-mail: [arodau@suffolk.edu](mailto:arodau@suffolk.edu)

Web page: [www.law.suffolk.edu/arodau](http://www.law.suffolk.edu/arodau)  
Copyright 2004 by Professor Andrew Beckerman-Rodau

**(Originally published in 31 Rutgers Comp. & Tech. L. J. 1 (2004))**

---

---

## **ETHICAL RISKS FROM THE USE OF TECHNOLOGY**

**BY ANDREW BECKERMAN-RODAU\***

### **ABSTRACT**

The pervasive use of modern technology has resulted in law firms increasingly creating and maintaining files, litigation materials, confidential client information and other data in digital form. This form of data is easy to update, transfer and search. Hence, it can save time and increase efficiency while minimizing errors. Nevertheless, certain risks accompany use of digital data. For example, client data must be maintained in confidence. It must be preserved so that it can be recovered in the future if it is needed. Also, it must be preserved such that it can be produced with reasonable assurance it is in its original unmodified form. These risks create the potential for an attorney to run afoul of rules of professional conduct. To avoid this, an attorney today must be both cognizant of these risks and take reasonable steps to minimize such risks. This article will identify these risks, identify the applicable rules of professional conduct and suggest reasonable actions an attorney must take to avoid violating these rules.

---

\* Professor of Law & Co-director of the Intellectual Property Law Concentration at Suffolk University Law School, Boston, Massachusetts. B.S., 1976, Hofstra University; J.D., 1981, Western New England College; L.L.M., 1986, Temple University. Website: [www.law.suffolk.edu/arodau](http://www.law.suffolk.edu/arodau); E-mail: [arodau@suffolk.edu](mailto:arodau@suffolk.edu). This article is based on materials prepared for and distributed at a continuing legal education program on ethics presented at Suffolk University Law School on June 11, 2004. Copyright 2004 by Andrew Beckerman-Rodau.

TABLE OF CONTENTS

INTRODUCTION.....3

I. ETHICAL CONCERNS THAT ARISE FROM THE USE OF  
COMPUTER TECHNOLOGY IN THE PRACTICE OF LAW.....6

    A. Maintaining confidential nature of client  
    information .....6

    B. Meeting the reasonableness standard ..... 9

II. DATA SECURITY ISSUES ARISING FROM THE USE OF  
DIGITAL DATA..... 11

    A. Introduction ..... 11

    B. Low-tech access – physical security measures .....12

    C. Passwords .....13

    D. Protecting data integrity .....15

        1. Data backups .....15

        2. Virus protection .....16

        3. Spyware protection .....19

        4. Computer use policy .....20

        5. Firewall software ..... 21

        6. Attorney and employee education .....22

        7. Modems and wireless access points .....22

        8. Automating data integrity protections .....24

        9. Storage media longevity .....24

    E. Traveling – security concerns..... 25

    F. Unintended document replication ..... 28

    G. Equipment replacement issues ..... 29

    H. Legacy support issues ..... 31

    I. The hidden data problem ..... 32

    J. The need for computer personnel ..... 33

CONCLUSION ..... 34

## INTRODUCTION

Many aspects of the practice of law have changed over the last two decades. The use of technology has dramatically increased.<sup>1</sup> Attorneys typically do not rely on support staff to take notes in shorthand. Dictating devices, carbon paper and IBM Selectric typewriters are no longer ubiquitous items in a law office. Today, computers appear almost universally in law offices on the desks of both support staff and attorneys.<sup>2</sup> Documents are created both by support staff and attorneys on computers using popular word processing software such as WORD or WORDPERFECT. Drafts may be electronically transmitted from an attorney's desktop computer to a support staff member via an internal network since connecting office computers together via a network is relatively easy and inexpensive and consequently quite common today. The widespread and inexpensively priced availability of both dialup and high speed Internet connections has resulted in office computers being connected both to internal networks and to the external Internet. Internet connections allow broad access to information and resources used by attorneys. The Internet enables mundane

---

1. See generally Molly Warner Lien, *Technocentrism and the Soul of the Common Law Lawyer*, 48 AM. U. L. REV. 85 (1998) (discussing the effect of technology on the practice of law). This is consistent with the increased utilization of computer technology in every aspect of society. See, e.g., Keith Reed, *Logan Troopers to Get Roving Database Access*, BOSTON GLOBE, June 22, 2004, at F1 (reporting that Massachusetts state troopers working at Logan International Airport in Boston will be issued small BlackBerry devices that will enable them to use wireless Internet access to instantly obtain detailed information on almost every person in the U.S.); see also Michael J. Miller, *Forward Thinking*, PC MAG., June 8, 2004, at 8 (stating that 73% of adults in the U.S. use computers and 63% use the Internet). Today, Internet use is growing at a significant rate worldwide. See, e.g., Yilu Zhao, *China's Web Portals Open a Door to Risk*, N.Y. TIMES, Mar. 7, 2004, at 7 (noting that there are currently 80 million Internet users in China and the number of users are growing annually at a double-digit percentage rate). In 2003, the number of worldwide Internet users was estimated at 649 million people. Marie Szanislo, *Point, Click and Cheat; Virtual Affairs Are Leading to Very Real Divorces*, BOSTON GLOBE, Dec. 14, 2003, at 3.

2. "Most analysts agree that the adaptation of technology in law offices represents one of the most revolutionary and challenging innovations in the practice of law." Barry L. Brickner, *Computer Usage by Michigan Lawyers*, 83 MICH. BAR J. 40, 44 (2004).

uses such as e-mail or instant-messaging.<sup>3</sup> Additionally, searching case law and other types of research are increasingly being conducted via the Internet. Large commercial databases such as LEXIS-NEXIS<sup>4</sup> and WESTLAW<sup>5</sup> provide instantaneous access to virtually all U.S. law and many other resources.<sup>6</sup> Many courts now provide information, including in some cases complete opinions, via websites on the Internet.<sup>7</sup> Non-profit services such as the Cornell Legal Information Institute at Cornell Law School provide free automatic e-mails alerting subscribers to recent Supreme Court decisions.<sup>8</sup> It is also quite common for law firms to maintain extensive web sites available to anyone with Internet access.<sup>9</sup> Finally, electronic communications with clients is increasingly common. It can include simply exchanging e-mails or sending documents as e-mail attachments.<sup>10</sup> More advanced uses can

---

3. See generally Christine Neylon O'Brien, *The Impact of Employer E-Mail Policies on Employee Rights to Engage in Concerted Activities Protected by the National Labor Relations Act*, 106 DICK. L. REV. 573, 573 (2002) (noting communicating via e-mail is commonplace today).

4. At <http://www.lexisnexis.com> (last visited Aug. 19, 2004).

5. At <http://www.westlaw.com> (last visited Aug. 19, 2004).

6. One commentator has argued that "[t]he range and depth of these databases are phenomenal and have changed forever the practice of law." Justin D. Leonard, *Cyberlawyering and the Small Business: Software Makes Hard Law (But Good Sense)*, 7 J. SMALL & EMERGING BUS. L. 323, 344 (2003).

7. See, e.g., SUPREME COURT OF THE UNITED STATES, at <http://www.supremecourtus.gov/> (official U.S. Supreme Court website) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal); see also THE FEDERAL JUDICIARY, at <http://www.uscourts.gov/links.html> (Federal Judiciary website with links to all federal courts) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal); see also NATIONAL CENTER FOR STATE COURTS, at [http://www.ncsconline.org/D\\_KIS/info\\_court\\_web\\_sites.html](http://www.ncsconline.org/D_KIS/info_court_web_sites.html) (provides links to most state courts) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

8. The Legal Information Institute is accessible on-line at <http://www.law.cornell.edu/> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

9. See, e.g., NATIONAL CENTER FOR STATE COURTS, at [http://www.ncsconline.org/D\\_KIS/Firms.html](http://www.ncsconline.org/D_KIS/Firms.html) (collection of links to a few law firm websites) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

10. Businesses in North America sent 40 billion e-mail messages in 1995; in

involve communal editing of documents by individuals at different locations via electronic connections over the Internet.<sup>11</sup>

The widespread use of computer technology in the practice of law is here and will continue to grow as business and commercial enterprises continue an ever increasing reliance on such technology in the interests of efficiency and profit maximization.<sup>12</sup> Consequently, attorneys will continue to use such technology since it will be demanded by clients. Such reliance on computers can raise ethical risks for attorneys.<sup>13</sup> This article addresses the general ethical issues which are a concern. It then provides a primer on technology issues that can trigger ethical concerns. Finally, it offers recommendations on minimizing running afoul of these ethical concerns in the practice of law.

---

2001, it is estimated that they sent 1.4 trillion messages. See Elizabeth Weinstein, *Help! I'm Drowning in E-Mail! Many Users Give up Hope, but Some Devise Tricks that Keep Them Afloat*, WALL ST. J., Jan. 10, 2002, at B1.

11. See Kathryn A. Romley, *Law Firm Administration: A Special Report; Let's Meet Online - Getting Together in Cyberspace Avoids Travel and Streamlines Document Drafting*, LEGAL TIMES, Nov. 18, 2002, at 40 (noting on-line meeting can include real time joint editing of documents).

12. See generally Robert J. Howe, *The Impact of the Internet on the Practice of Law: Death Spiral or Never-Ending Work?*, 8 VA. J.L. & TECH. 5 (2003) (discussing effect of Internet technology on the practice of law); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 746 (E.D. Mich. 1999) (noting that the creation of the Internet resulted in a worldwide communication revolution).

13. See, e.g., Lawrence Duncan MacLachlan, *Gandy Dancers on the Web: How the Internet Has Raised the Bar on Lawyers' Professional Responsibility to Research and Know the Law*, 13 GEO. J. LEGAL ETHICS 607, 621-626 (2000) (asserting that the availability of Internet raises the ethical standard for attorney research obligations).

I. ETHICAL CONCERNS THAT ARISE FROM THE USE OF COMPUTER TECHNOLOGY IN THE PRACTICE OF LAW

A. *Maintaining confidential nature of client information*

In the course of representing clients, lawyers receive confidential information. Such information may relate to the client personally or to a business enterprise she is involved in. Maintaining the confidentiality of such information is a basic premise of the U.S. legal system.<sup>14</sup> It enables a client to freely speak with an attorney in the course of a client-attorney relationship.<sup>15</sup> Absent this ability, a client would may be unwilling to freely communicate with his or her lawyer thereby making it difficult for the attorney to represent the client to the best of his or her ability.<sup>16</sup> Consequently, attorneys are required to maintain the confidentiality of most client information.

The ABA Model Rules of Professional Conduct provide, in part:

RULE 1.6: Confidentiality of Information

- (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry

---

14. See *Chinatown Apartments, Inc. v. New York City Transit Auth. et al.*, 421 N.Y.S.2d 958, 959 (N.Y. Sup. Ct. 1978) ("A fiduciary relationship exists between lawyer and client and attendant with it is a regard for the confidentiality of communications . . . . Client security in the soundness of the fiduciary relationship is vital to the smooth functioning of our adversarial system of jurisprudence."); see generally *In Re Gonzalez*, 773 A.2d 1026, 1031 (D.C. 2001) ("[It is a] fundamental principle that the attorney owes a fiduciary duty to his client and must serve the client's interests with the utmost loyalty and devotion.").

15. "The attorney-client privilege in both federal and state court is intended to promote the free exchange of information between an attorney and client." William L. Stephens, Jr., *Convenience vs. Confidentiality: An Evaluation of the Effects of Computer Technology on the Attorney-Client Privilege*, 35 DUQ. L. REV. 1011, 1014 (1997). See also *In re Sean H. et al.*, 586 A.2d 1171, 1176 (Conn. App. Ct. 1991) (explaining that the rationale for the attorney-client confidentiality is that clients will only fully disclose all facts to attorney if such disclosure is protected by confidentiality).

16. See *In re Genusa*, 381 So. 2d 504, 505 (La. 1980) (stating that an attorney must know all facts in order for client to obtain full advantage of our legal system).

out the representation or the disclosure is permitted \* \* \* by [certain limited and specific situations].<sup>17</sup>

Official comments to Rule 1.6 state, in part:

A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer \* \* \*.<sup>18</sup>

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. "Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information . . . A client . . . may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule."<sup>19</sup> "The duty of confidentiality continues after the client-lawyer relationship has terminated."<sup>20</sup>

Representation of a client often requires an attorney to utilize non-attorneys which may include support personnel, paralegals, accountants, investigators, law student interns and experts.<sup>21</sup> Ethical rules binding attorneys do not bind non-attorneys.<sup>22</sup> However, an attorney may be responsible for insuring that such personnel comply with the ethical obligations binding the attorney.<sup>23</sup> Hence, an attorney must take appropriate steps to insure

---

17. THOMAS D. MORGAN & RONALD D. ROTUNDA, 2003 SELECTED STANDARDS ON PROFESSIONAL RESPONSIBILITY 25 (2003).

18. *Id.* at 31 (Model Rules of Prof. Conduct R. 1.6 cmt. 15 (2003)).

19. *Id.* at 31-32 (Model Rules of Prof. Conduct R. 1.6 cmt. 16 (2003)).

20. *Id.* at 32 (Model Rules of Prof. Conduct R. 1.6 cmt. 17 (2003)).

21. *See Daines v. Alcatel*, 194 F.R.D. 678, 682 (E.D. Wa. 2000) (noting that non-attorney law firm employees are routinely exposed to confidential client information).

22. *See In re Burns*, 657 N.E.2d 738, 740 (Ind. 1995) (recognizing that the Rules of Professional Conduct do not apply to non-attorneys or to former attorneys).

23. *See Daines*, 194 F.R.D. at 681-82 (noting that the Rules of Professional Conduct require attorney to make certain non-attorney employees abide by these

that all personnel, including technology staff, safeguard confidential client information.<sup>24</sup>

The ABA Model Rules of Professional Conduct provide, in part:

RULE 5.3: Responsibility Regarding Nonlawyer Assistants

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner, a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, and the law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.<sup>25</sup>

Official comments to Rule 5.3 state, in part:

Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give

---

rules, and attorney may be responsible for violations of these rules by non-attorney employees).

24. See generally Saul Hansell, *AOL Worker Is Accused Of E-Mail Theft*, N.Y. TIMES, June 24, 2004, at C1 (involving an AOL employee who sold customer confidential data to third party to send spam).

25. See MORGAN & ROTUNDA, *supra* note 17, at 114.

---

---

such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.<sup>26</sup>

[The Rule] \* \* \* requires lawyers with managerial authority within a law firm, and the firm itself, to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that nonlawyers in the firm will act in a way compatible with the Rules of Professional Conduct.<sup>27</sup>

### B. *Meeting the reasonableness standard*

The above ethical rules and official comments generally require attorneys to take *reasonable* steps<sup>28</sup> to insure client confidentiality is maintained both by the attorney and other employees and agents who have access to client information in the normal representation of a client.<sup>29</sup> Reasonableness, which is a basic standard used in negligence law,<sup>30</sup> is a variable standard.<sup>31</sup> The existing state of technology, the general customs in a particular profession, a cost-benefit ratio, potential risks and consequences, and the typical

---

26. *Id.* (Model Rules of Prof. Conduct R. 5.3 cmt. 1 (2003)).

27. *Id.* (Model Rules of Prof. Conduct R. 5.3 cmt. 2 (2003)).

28. "Reasonable" is defined as "fair, proper, or moderate under the circumstances." BLACK'S LAW DICTIONARY 1272 (7th ed. 1999).

29. See MORGAN & ROTUNDA, *supra* notes 25-27 and accompanying text.

30. Typically, reasonableness is an objective standard determined by what a reasonable person of ordinary prudence would do under the relevant facts. W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 32 (5th ed. 1984) (quoting Green, *The Negligence Issue*, 37 YALE L.J. 1029 (1928)) (discussing generally the reasonable person standard).

31. See generally Eric T. Freyfogle, *Water Justice*, 1986 U. ILL. L. REV. 481, 505 (1986) (noting reasonable water use pursuant to a reasonable use rule varies over time since what is reasonable varies over time); Kimberlie Young, *An Examination of Parental Discipline as a Defense of Justification: It's Time for a Kinder, Gentler Approach*, 46 NAVAL L. REV. 1, 13 (1999) (noting with regard to parental discipline what is reasonable can change in light of changing societal attitudes).

knowledge of persons in the particular profession all relate to determining reasonableness.<sup>32</sup> Additionally, an obligation to inquire or ascertain relevant information may be applicable to whether reasonable conduct has been engaged in.<sup>33</sup>

In light of this, it is important to fully understand the potential risks of reliance on technology as a prerequisite to evaluating the reasonableness of conduct.<sup>34</sup> Knowledge of such risks and the corresponding consequences provide a baseline for knowing what actions must be taken to maintain confidential client information. Additionally, it also facilitates determining what actions, such as employee training, may be necessary to meet the reasonableness standard.

The next section examines the technological risks that can potentially compromise confidential client information in today's computerized law firm environment. It also discusses methods and techniques for minimizing such risks.

---

32. See KEETON ET AL., *supra* note 30, § 33, at 193-96 (discussing the relevance of custom).

33. See *generally id.* § 32, at 184 – 85.

34. This may require hiring a consultant to evaluate risks associated with a computer system. On June 22, 2004, a study released by Massachusetts found that the computer system used by the state court system was insecure. Unauthorized parties could easily obtain access to e-mail, court files and other digital data stored on the network. Among other things, the study found that hundreds of former employees still had access to the system. Additionally, employees were not required to change passwords on a regular basis. John Ellement, *Audit Finds Security Flaws in Court's Data System*, BOSTON GLOBE, June 23, 2004, at F12. See *generally* Suruchi Mohan, *The Stuff of Nightmares: Remote Access Poses Security Risks that Will Keep You up at Night*, COMPUTERWORLD, Jan. 2, 1995, at 66 (involving a terminated reporter, whose wireless access privileges were not terminated, who used such access to enable competitor to scoop former employer).

## II. DATA SECURITY ISSUES ARISING FROM THE USE OF DIGITAL DATA

### A. Introduction

Movement from paper documents to digital documents has many advantages. It is easier to manage documents because they can be more easily stored, located, indexed, reproduced, modified and searched.<sup>35</sup> However, these same advantages increase opportunities for inadvertent disclosure of confidential data and unauthorized acquisition of such documents.<sup>36</sup> If attorneys and other law firm personnel are not adequately informed or trained, numerous

---

35. See generally Julianne M. Sullivan, *Will The Privacy Act of 1974 Still Hold Up in 2004? How Advancing Technology Has Created a Need for Change in the "System of Records" Analysis*, 39 CAL. W. L. REV. 395, 403 (2003) (noting that unlike paper databases which must be indexed, the text of documents contained in a computer database can be key-word searched); see also Gregory S. Johnson, *A Practitioner's Overview of Digital Discovery*, 33 GONZ. L. REV. 347, 358 (1997-98) ("[D]igital data can be analyzed more quickly and cost-effectively than 'hard-copy' documents. . .").

36. See generally Colleen L. Rest, *Electronic Mail and Confidential Client Attorney Communications: Risk Management*, 48 CASE W. RES. L. REV. 309, 316 (1998) (recognizing that in contrast to paper documents, it is easy to inadvertently send an e-mail to the wrong e-mail address). Client information discussed on a cell phone or in an e-mail message may create an ethical risk. Such communications can be intercepted by third parties. See David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 485 (1998); see also Brett Glass, *Encryption: Think Your E-mail Is Secure? How About the Files on Your Hard Drive? Think Again*, PC MAG., June 17, 2003, at 100 (noting that most e-mail is sent unencrypted making it easy to intercept). The issue of client confidentiality when an attorney client discussion occurs over a cell phone or via e-mail is an issue addressed in ethical opinions issued by several states. See Karin Mika, *Of Cell Phones and Electronic Mail: Disclosure of Confidential Information Under Disciplinary Rule 4-101 and Model Rule 1.6*, 13 NOTRE DAME J. L. ETHICS & PUB. POL'Y 121, 126-27 (1999). See generally Skip Walter, *Plaintiff's Law Firms No Longer As Disadvantaged: Technology, Legal Rulings are Leveling Playing Field Between Large, Small Firms*, 26 NAT'L L.J., July 5, 2004, at S3 (noting significantly more digital data is available via discovery in a legal proceeding that was previously available when documents were maintained only in paper form); Leigh Jones, *The Surging Evolution of E-Discovery*, 26 NAT'L L.J., Aug. 2, 2004, at 1 (noting increasing cost and complexity of the discovery process when digital data is involved).

opportunities exist for the inadvertent release of confidential client data.<sup>37</sup> Additionally, reliance on digital data makes unauthorized deliberate diversion or acquisition of documents by both employees and third parties easier to achieve as compared to an environment utilizing paper documents. Reliance on digital data combined with networking of computers, both internally and externally, makes it easier for unauthorized diversion of documents to go undetected. Finally, inadequate precautions can result in unintended loss of digital documents<sup>38</sup> as well as the risk that documents can be the subject of unauthorized alteration.<sup>39</sup>

B. *Low-tech access – physical security measures*

The ease with which digital data can be accessed, searched and copied makes controlling access to digital data critical. The most basic risk to digital data is an unattended computer. During the work day, employees and vendors installing software, and technical personnel may have access to computers. Additionally, after hours both maintenance staff and cleaning contractors routinely have access to office space which gives them access to any unattended computer.<sup>40</sup>

Computers are ubiquitous tools scattered about the majority of workplaces today. They handle the many tasks – both mundane and complex – that are necessary to operate a law firm or other enterprise. Nevertheless, each computer is like a file cabinet containing both firm and client data. Additionally, a networked computer is like a door into a room containing all of the firm's and

---

37. *See generally* U.S. v. Rigas, 281 F. Supp. 2d 733, 735-36 (S.D.N.Y. 2003) (involving copies of a computer hard drive, made pursuant to discovery, which mistakenly contained confidential information despite reasonable efforts to prevent such occurrence).

38. *See generally*, Isikoff, *infra* note 100.

39. *See generally* Jill Witkowski, *Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images*, 10 WASH. U. J.L. & POL'Y 267 (2002) (noting that digital data, whether text, photographs or audio recordings, can be easily altered).

40. *See generally* Erik Rhey, *Security Checklist: Run a Business-Class Hardware Firewall*, PC MAG., June 28, 2004, at 93 (suggesting using a visitor sign-in/sign-out log, locking computers whenever employees are away from their desks, and checking IDs of all service people and other non-employees).

---

---

clients' data. In light of this, physical security measures are critical. If a firm would not leave all its data and files openly available on an unrestricted basis to all personnel, then it should not do the same thing with office computers.

Thus, the location of computers should be evaluated in light of who needs access to particular machines. Also, it should be determined if all machines need to be networked. Disks, CDs, backup tapes and any other portable data media should not be left in easily accessible locations. At a minimum, such media should be kept in a locked desk drawer or file cabinet.

### *C. Passwords*

Passwords, a commonly used security device, are employed by many devices and systems, such as ATMs. At a minimum, all computers should have a password installed that must be entered before anyone will be able to use the computer. Typically, this means the computer should have a password that is required to access computer data when it is turned on. Additionally, in many workplaces, computers are left on all the time. Such machines should lock out users by requiring a password. The ability to add such passwords is already built into most computers. It merely requires a few steps to be activated.

The use of passwords will only be effective if an appropriate password policy is utilized. This means that employee passwords should not be names, phone numbers, birth dates or other things which can be easily guessed.<sup>41</sup> Preferably, passwords should include numbers, letters and other characters. Additionally, they should be case sensitive so that capital and small letters can be mixed together.<sup>42</sup> The computer network can be programmed so

---

41. See generally Tom Powledge, *Protect Important Data from Unnecessary Risk*, N.J.L.J., Feb. 13, 2004 (noting security risk created by using easy to remember passwords).

42. Suggestions for creating good passwords by the Carnegie Mellon School of Computer Science available at [http://www-2.cs.cmu.edu/~help/security/choosing\\_passwords.html](http://www-2.cs.cmu.edu/~help/security/choosing_passwords.html) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). See also Purdue University Guidelines for Good Passwords, at [http://www.adpc.purdue.edu/BSCompt/WebZone/guidelines\\_to\\_good\\_passwords](http://www.adpc.purdue.edu/BSCompt/WebZone/guidelines_to_good_passwords).

that it only accepts proper passwords. If an employee attempts to create an improper or weak password, the system can be setup so that it rejects it and provides a pop-up window explaining what was wrong with the password. Finally, passwords should be periodically changed.<sup>43</sup>

The proliferation of passwords needed by employees often undermines the above policies. Today, an attorney might have a power-on password<sup>44</sup> on her computer, a network log-on password, an e-mail password, a WESTLAW password and a LEXIS-NEXIS password. Additionally, she may have an ATM password, a phone card password and other passwords for a variety of things. The average person will have difficulty remembering so many different passwords. Hence, users tend to pick easy to remember passwords such as names, phone numbers, etc. If the above password policy is put in place so that such weak passwords cannot be used, another common problem often occurs. The user will write down the passwords in a convenient place such as on a Post-It note stuck to the side of the monitor or inside a desk drawer.<sup>45</sup> Obviously, such conduct defeats the purpose of any password policy.

One solution is to create a single password system. Employees often dislike having to use several strong, arbitrary passwords.<sup>46</sup> Periodically changing passwords is universally disliked.

---

htm (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal); Virginia Tech Guidelines for Good Passwords, at [http://www.computing.vt.edu/accounts\\_and\\_access/pickinggoodpasswords.html](http://www.computing.vt.edu/accounts_and_access/pickinggoodpasswords.html) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

43. See John Ellement, *Audit Finds Security Flaws in Court's Data System*, THE BOSTON GLOBE, June 23, 2004, at F12 (noting that failing to require employees to periodically change passwords is a potential security problem). Additionally, failing to terminate access to a computer network by former employees is a potential security problem. *Id.*

44. This type of password must be entered before the computer's operating system software will run. This function is generally provided on most computers. See generally William H. Pratt & Jonathan F. Putnam, *On the Road Again: Getting the Most from a Laptop PC*, N.Y.L.J., May 19, 1997, at S4 (recognizing that a power-on password is necessary for someone to log on to your computer).

45. See Powledge, *supra* note 41.

46. See Frank Hayes, *What Users Want*, COMPUTERWORLD, Feb. 2, 2004, at 42.

---

---

Consequently, a good compromise is to enable users to have only a single password for everything. Such a system can store passwords for a variety of systems or services that will automatically be sent, as appropriate, when the single password is entered.

#### D. *Protecting data integrity*

As documents and related data are increasingly being kept only in digital form,<sup>47</sup> it is important to maintain the integrity of the data so that it can be retrieved and used, as needed, in the future. Insuring such integrity requires attention to a number of technological issues and concerns.

##### 1. *Data backups*

First, all digital data should be backed up on a regular basis.<sup>48</sup> A variety of storage devices exist today for such backups.<sup>49</sup> Additionally, simple software exists which enables a computer to automatically back itself up on a regular basis with only minimal human intervention.

It is common for networks to backup data onto a second hard drive or magnetic tape or both. In a networked office environment, individual desktop computers can store all data files on a network server which can then be backed up on a regular schedule. If data files are stored on individual desktop computers, back ups can be automatically made over the network. Additionally, inexpensive external hard drives can be connected to desktop computers for backing up data locally.<sup>50</sup> Such hard drives can be set up to

---

47. See generally Gregory S. Johnson, *A Practitioner's Overview of Digital Discovery*, 33 GONZ. L. REV. 347, 348 (1997-98) (noting that today it is estimated that much business data is kept only in digital form).

48. See generally Joseph Cleveland, *Career Watch*, COMPUTERWORLD, Apr. 26, 2004, at 36 ("With the volume of sensitive data generated every second growing rapidly, data integrity, backup systems and database security have become increasingly important aspects of the job of database administrators.").

49. For example, an external computer hard drive can be connected to a computer and used to backup data. A variety of companies make such drives that have very large storage capacity. See, e.g., at <http://www.iomega.com/na/landing.jsp> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

50. See *id.*

automatically backup all files as they are changed in real time by the computer user.

Critical data can be backed up to off-site locations. Companies exist today that provide secure off-site data backups for a monthly fee.<sup>51</sup>

## 2. *Virus protection*

It is a fact of life that malevolent individuals will create and disseminate software code whose sole purpose is to interfere with the use of computers. Such code, commonly called a virus,<sup>52</sup> may have only minimal effects on a computer or computer network.<sup>53</sup> In contrast, some viruses can destroy data and completely cripple a computer or network. Avoiding viruses is impossible. Nevertheless, some simple precautions can substantially eliminate the risk associated with viruses.

The first level of defense is installing virus protection software on all computers. This software is commonly available at a relatively low cost.<sup>54</sup> Virus protection software must be updated on

---

51. See, e.g., Jerri Stroud, *Data-Backup Firm Offers Business Owners a Safety Net*, ST. LOUIS POST-DISPATCH, Mar. 8, 2004, at C1 (noting that software automatically backups business data, encrypts it and automatically sends it to a secure off-site location).

52. See Dan Thanh Dang, *'MyDoom' Virus Infects E-mail*, BALT. SUN, Jan. 28, 2004, at 1D ("A computer virus is a program or a piece of code designed to spread itself to multiple files and applications on a single computer."). Other types of malicious software also exist. "A worm - similar to a virus - also replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting down a system." *Id.* "A Trojan horse is a destructive program that disguises itself as something else." Sheryl Canter, *Effective Immunity: Viruses Keep Spreading, and PCs Keep Getting Infected. What Can You Do to Stay Secure?*, PC MAG., Aug. 19, 2003, at 66.

53. See David Bank, *Search Engines Are Attacked by Latest Virus*, WALL ST. J., July 27, 2004, at D5 (noting that a recent virus caused user delays for GOOGLE search service). See generally *Welcome to Virus Protection & Software Primer*, Clemson University, at <http://virtual.clemson.edu/client/repprob/vprimer.htm> (last visited on Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

54. One commonly used virus protection program is Norton Antivirus. See Norton Anti-Virus 2005, Symantec, at [http://www.symantec.com/nav/nav\\_9xnt/](http://www.symantec.com/nav/nav_9xnt/) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). Another commonly used program is made by McAfee. See McAfee

a regular basis or it rapidly becomes useless. Most of these programs can be setup to automatically download new virus definitions over the Internet on a regular basis. Weekly updates are a necessity if this software is to be an effective tool.<sup>55</sup>

If computers are networked in an office environment, virus updates can be sent to all desktop computers automatically via the network. This is often a better alternative than relying on individual computer users to update the software.

Virus creators often exploit known flaws in operating system software.<sup>56</sup> Microsoft Windows, the operating system used on most computers, is a favorite target of virus creators.<sup>57</sup> To thwart these individuals, Microsoft makes available software updates or patches to fix such flaws. These updates are available from Microsoft for free via the Internet.<sup>58</sup> Windows can even be configured to automatically notify the user or automatically download and install these updates or both. In many cases, regularly installing these updates will immunize your computer from new and disruptive viruses.<sup>59</sup>

E-mail has become a source of unwanted mail (commonly called

---

Virus Protection, at <http://us.mcafee.com/> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

55. See Leon Erlanger, *Top Five Myths About Safe Surfing*, PC MAG., Dec. 9, 2003, at 84 (recognizing that antivirus software is "only as good as its last update").

56. See Steve Lohr, *PC Demand Helps Microsoft Beat Earnings Estimates*, N.Y. TIMES, Oct. 24, 2003, at C6.

57. See Cade Metz, *Should You Switch?* (sidebar to *Is Microsoft to Blame?*), PC MAG., Aug. 3, 2004, at 76 (noting that even though some experts assert Windows has fewer security flaws than other operating systems, it is the most targeted due to its market dominance.).

58. See Microsoft Windows Update, at <http://v4.windowsupdate.microsoft.com/en/default.asp> (last visited Aug. 19, 2004) (Microsoft website for downloading operating system updates) (on file with the Rutgers Computer and Technology Law Journal). See also Microsoft Office Online, at <http://office.microsoft.com/OfficeUpdate/default.aspx> (last visited Aug. 19, 2004) (Microsoft website for downloading updates to Microsoft Office) (on file with the Rutgers Computer and Technology Law Journal).

59. See James Gallo, *Proper Care Yields Smooth Computing*, BALTIMORE SUN, Feb. 12, 2004, at 9D.

SPAM).<sup>60</sup> Such e-mail is clearly an annoyance. However, it can also provide a gateway for viruses to infect a computer or a computer network. Traditionally, most such viruses were contained in e-mail attachments.<sup>61</sup> Enterprising virus creators have expanded their attacks so that viruses can be obtained even from e-mail without attachments.<sup>62</sup> Nevertheless, a few simple actions can greatly minimize the likelihood of viruses affecting a computer.<sup>63</sup> First, most antivirus programs can be set up to scan e-mail for viruses.<sup>64</sup> Second, e-mail systems can be configured to reject all e-mail attachments. Although blocking all attachments is very effective, it may compromise usability of e-mail such that it is counterproductive.<sup>65</sup> A middle ground is to only block certain types of e-mail attachments such as types most likely to contain viruses.<sup>66</sup> These are generally not the types of files routinely sent as file attachments, so in most cases this only has minimal effect on system usability. Finally, file attachments, which are unexpected<sup>67</sup>

---

60. Today, more than 50% of all e-mails are unwanted SPAM. See Tim Lemke, *Microsoft Works on Outsmarting Spam*, WASH. TIMES, Feb. 25, 2004, at C8.

61. See Thanh Dang, *supra* note 52, at 1D (recognizing that viruses are commonly spread through e-mail attachments). See generally Byron Acohido, *Virus Makers' War Bombs Businesses*, USA TODAY, Apr. 12, 2004, at 3B (noting that not opening e-mail attachments can effectively block many viruses).

62. See Erlanger, *supra* note 55, at 84 (recognizing that some viruses can be activated merely by reading an e-mail).

63. See Barbara Yost, *S\*P\*A\*M: Where is All That \*Junk\* E-\*mail Coming From, and HOW Can "Y.ou" Ma.ke it STOP?*, ARIZ. REPUBLICAN, June 24, 2004, at 1E (offering suggestions on reducing SPAM).

64. This normally requires setting up the antivirus program to "scan all incoming traffic," such as e-mail. Erlanger, *supra* note 55, at 84.

65. See Richard J. Dalton Jr., *Catching E-Mail Bad Apples; New Tactics to Keep Tainted Files Away*, NEWSDAY, Feb. 17, 2004, at A47 (noting that blocking all e-mail attachments is not practical).

66. Typically, viruses are contained in program files or other executable files. Such files commonly have the file extensions ".com," ".exe," or ".vbs." See Canter, *supra* note 52, at 66.

67. Some viruses "hi-jack" the address book in an e-mail program and send virus-laden attachments to everyone listed in the address book. See generally Erlanger, *supra* note 55, at 84; Russell Glitman, *Mail Utilities: From Juggling Multiple E-mail Accounts and Swatting Swarms of Junk Mail to Managing Business Correspondence Around the Clock, It's No Wonder E-mail Can Drive You Crazy*, PC MAG., June 17, 2003, at 18. Hence, even if an attachment appears

or from unknown users, should never be opened.

### 3. *Spyware protection*

In addition to viruses, both legitimate enterprises and malevolent individuals have created and disseminated programs that illicitly collect and transmit data from a computer. Typically, these programs, called spyware,<sup>68</sup> are unintentionally downloaded to a computer from the Internet.<sup>69</sup> Often they are included, without any notice or warning, in things that are downloaded from the Internet.<sup>70</sup> For example, downloading a free software program from the Internet may result in unwanted software being downloaded without your knowledge.<sup>71</sup> Such software may come from a commercial enterprise which collects data on the web sites you visit on the computer, or it may be a program that collects critical data, such as usernames and passwords for later use in illegally penetrating the computer from a remote location.<sup>72</sup>

Relatively inexpensive software is available both to block such software from downloading and to remove any such software that

---

to come from a known sender, it should not be opened if it is unexpected. First, an e-mail can be sent to the sender asking if she sent an attachment. Only when she verifies having sent the attachment should it be opened.

68. Spyware, also sometimes referred to as "adware," refers to "a wide range of software programs that track a computer user's online activities and often flood the screen with annoying pop-up ads." Mary Kissel, *Lawmakers Move Toward Placing Restrictions on Spyware Programs*, WALL ST. J., June 24, 2004, at D2. In response to the growing spyware problem, Dell Inc., the large computer manufacturer, has launched a web page containing information to help consumers eliminate viruses and spyware from their computers. Russell Gold, *Dell Debuts Site in Battle Against Spyware, Viruses*, WALL ST. J., July 20, 2004, at D2. The increasing sophistication of spyware has exacerbated the problem. As a result, it is easier for it to surreptitiously infect a computer, it is frequently more harmful and it is often difficult to eradicate. Lee Gomes, *Spyware Is Easy to Get, Difficult to Remove, Increasingly Malicious*, WALL ST. J., July 12, 2004, at B1.

69. See Gomes, *supra* note 68.

70. One of the problems with spyware is that many users are unaware it is present on a computer. See *id.*

71. See generally Kevin J. Delaney, *Web-Data Hackers Thwarted, but PCs Are Still Vulnerable*, WALL ST. J., June 28, 2004, at B5 (recognizing that hidden code on legitimate web sites allowed third party to steal passwords).

72. See *id.* This type of unwanted software is sometimes referred to as a "Trojan horse." See Stroud, *supra* note 51.

is on a computer.<sup>73</sup> Like antivirus programs, this software should be updated frequently and run on a periodic basis.<sup>74</sup>

#### 4. *Computer use policy*

A clearly thought out computer use policy is critical to protecting data integrity.<sup>75</sup> Such a policy should be reduced to an understandable written form that is disseminated to everyone.<sup>76</sup> The policy should be tailored to the particular enterprise since that will dictate the type of computer restrictions which are reasonable and those that are unreasonable and hence interfere with day-to-day work.<sup>77</sup>

For example, employee access to the Internet may be difficult to limit if such access is needed on an on-going basis by employees. In contrast, limiting such access may be both reasonable and

---

73. "Ad-Aware" is one of many programs that are effective tools for dealing with such spyware. For information on Ad-Aware and to download a free version for personal use, see <http://www.lavasoft.de/> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). Additionally, antivirus programs may catch some of these unwanted programs. It may also be beneficial to install pop-up blocker software. Pop-up ads, which are ads that pop-up in their own window when you are web browsing, are becoming popular. Such ads can be both an annoyance and a source of unwanted software being loaded on your system. Numerous free and inexpensive pop-up blocker programs are available. Additionally, the next version of Microsoft's Internet Explorer (software used to surf the Internet) is supposed to contain built in pop-up blocker software. See Patrick Marshall, *Microsoft's Big Fix*, SEATTLE TIMES, Aug. 28, 2004, at C6.

74. See generally Delaney, *supra* note 71 (noting that an antivirus program, a firewall program and installation of most current software patches are necessary to combat spyware).

75. See generally William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK. L. REV. 91, 110-11 (2003) (explaining that attorneys and consultants routinely advise employers to adopt clear computer use policies that are communicated to employees).

76. See, e.g., University of California at Berkeley Computer Use Policy, at <http://itpolicy.berkeley.edu:7015/usepolicy.html> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal); Seattle University Computer Use Policy, at <http://www.seattleu.edu/it/policies/cupolicy.asp> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

77. See generally Kimberly D. Richard, *Electronic Evidence: To Produce or Not to Produce, That is the Question*, 21 WHITTIER L. REV. 463, 484-85 (1999) (listing items that a computer use policy should address).

desirable if it is not necessary for the day-to-day activities of employees.

In today's business world, unlimited e-mail access is a necessity in most work environments, including law firms. However, reliance on SPAM filters, clear rules about dealing with attachments and blocking certain types of e-mail attachments can significantly reduce any problems related to e-mail usage. Additionally, both attorneys and employees need to be educated about what should and what should not be written in an e-mail message in light of the relative permanence of such writings.<sup>78</sup>

A rigid rule should exist, in most cases, barring the installation of any software without permission. Installation of unauthorized software can inadvertently infect a computer and the network it is connected to with viruses and/or other unwanted software.<sup>79</sup> Additionally, disks, CDs or other media from home should not be used in office computers. Again, this can inadvertently introduce viruses and/or unwanted software into the system.<sup>80</sup>

#### 5. Firewall software

Any computer connected to the Internet is a potential target for third parties trying to gain unauthorized access to the computer. Hackers seeking to damage or steal data and other unauthorized users constantly probe systems looking for easy entry. Firewall software blocks a large amount of unauthorized entry.<sup>81</sup> Hence, it

---

78. See Powledge, *supra* note 41, at 30. This is especially critical in light of the amount of digital data that can be obtained via electronic discovery. See Walter, *supra* note 36, at 53. Plus, the difficulty of eradicating digital data, especially in the case of e-mail messages, has resulted in such data being a source of corporate liability. David K. Thornquist, *Digging Deeper, in New Places: Electronic Discovery Has Had a Big Impact on How Due Diligence Is Now Conducted in Financial Ventures*, 26 NAT'L L.J. 19 (May 24, 2004).

79. See Thanh Dang, *supra* note 52, at 1D ("Viruses are usually spread by users sending e-mail attachments, trading programs on CDs or diskettes or copying files to file servers."). Additionally, employee-installed software can create employer liability if the software is not owned or properly licensed by the person installing it. See Ray K. Harris & James D. Burgess, *Compliance Planning for Intellectual Property Crimes*, 2 BUFF. INTELL. PROP. L.J. 1, 28-29 (2003).

80. See Thanh Dang, *supra* note 52, at 1D.

81. "A firewall is software that resides at a network's connection point (or

should be installed on all computers that are connected to the Internet. This software, once installed, runs in the background. The newest version of the Windows operating system, Windows XP, contains a built in firewall which merely has to be turned on for it to be made operational. More robust firewall software is also available and is relatively inexpensive.<sup>82</sup>

#### 6. *Attorney and employee education*

It is critical that attorneys and employees are educated about the risks of using computers and relying on digital data.<sup>83</sup> Only day-to-day adherence to appropriate practices can insure data integrity. However, adherence to such practices will only occur if computer users understand the need for such practices. Education in the form of periodic meetings and written computer use policies can emphasize the importance of such practices.<sup>84</sup>

#### 7. *Modems and wireless access points*

If desktop computers in an office environment are connected to the Internet via an internal network, any dial-up modems<sup>85</sup> on

---

points) to the Internet. The firewall analyzes data streams, either allowing or disallowing data to pass based on a series of network security policies or rules." Checkpoint Sys., Inc. v. Check Point Software Tech., Inc., 104 F. Supp. 2d 427, 440 (D.N.J. 2000).

82. Commonly used firewall software includes "BlackIce" and "Zone Alarm." For information on BlackIce, see BlackIce PC Protection Firewall, at <http://www.blackice.com/PCProtection-Firewall.htm> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). For information on Zone Alarm, see <http://www.zonelabs.com/store/content/home.jsp> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

83. See generally Powledge, *supra* note 41, at 30 (noting the importance of attorneys being aware of potential risks to computer files).

84. See generally Lisa J. Sotto, *For the Record: New Risks in Records Management Require New Procedures*, N.Y.L.J., Aug. 12, 2003, at 5 (recognizing that a well-drafted computer use policy can apprise employees of what should and should not be put in an e-mail message).

85. Dial-up modems (also called ordinary modems) are devices which allow a computer to connect to the Internet via an ordinary copper phone line. See WEBOPEDIA at, [http://webopedia.internet.com/quick\\_ref/dialup\\_modem\\_standards.asp](http://webopedia.internet.com/quick_ref/dialup_modem_standards.asp) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). Sometimes this is referred to as dial-up

individual computers should be removed or disconnected. Additionally, employee-installed wireless access points,<sup>86</sup> which are easily installed in an office to allow use of a wireless-enabled laptop, should be removed. Both of these devices allow easy unauthorized third party access to the network.<sup>87</sup> A dial-up modem connected to a phone line<sup>88</sup> and an unencrypted wireless access point may effectively allow a third party to bypass all security measures utilized to protect the network and computers connected to the network.<sup>89</sup>

---

Internet access. Issues with dial-up modems will slowly disappear as more and more computers and networks rely on high speed or broadband Internet access. Nevertheless, many current computers still include dial-up modems, which are often left connected to an active phone line even if the dial-up modem is no longer used. Similar devices called broadband modems, cable modems or DSL modems allow a computer to be connected to high speed or broadband Internet access as opposed to slower dialup Internet access. See TECHENCYCLOPEDIA, at <http://www.techweb.com/encyclopedia/defineterm?term=broadband&x=22&y=8> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

86. Wireless access points are simply small devices that can be connected to most computers. They allow a wireless link between the computer and a laptop. Such devices are relatively inexpensive and installable on most computers in a matter of minutes. Additionally, wireless-enabled laptops are becoming standard today. "WiFi" is the term often used to refer to wireless Internet access. It is short for wireless fidelity which is "the signal standard used to transmit data over local networks using radio signals . . ." Bob Tedeschi, *Cyber Scout: Cutting the Cord*, N.Y. TIMES, Dec. 7, 2003, sec. 5 at 6. The networks that handle WiFi are typically called "hot spots." *Id.*

87. See generally Suruchi Mohan, *The Stuff of Nightmares: Remote Access Poses Security Risks that Will Keep You up at Night*, COMPUTERWORLD, Jan. 2, 1995, at 66 (recognizing that the increased use of digital data which is remotely accessible increases security risks to such data). See also Hiawatha Bray, *Laptops at the FleetCenter at Risk of Breaches, Attack*, BOSTON GLOBE, July 22, 2004, at C1 (discussing the risk of wireless enabled laptops at the 2004 Democratic National Convention in Boston).

88. In the typical networked office environment safety precautions are located between the network and its connection to the Internet. Hence, if an individual computer user connects her computer directly to the Internet via a dialup modem she is effectively bypassing all network security safeguards.

89. Wireless access points are essentially radio receivers/transmitters. As such, the signals they send out cannot be contained. Thus, operation of an unencrypted wireless access point opens a potential doorway into the network which bypasses all network security measures. See generally Bruce Mohl, *Tap into Neighbor's WiFi? Why Not, Some Say*, BOSTON GLOBE, July 4, 2004, at C1

### 8. Automating data integrity protections

The above recommendations may seem daunting to anyone other than a computer programmer. However, backup programs, antivirus programs and antispymware programs can be setup to run automatically.<sup>90</sup> For example, computers can be left on at night and the above programs can be setup to run automatically at 2 AM on a nightly basis. This provides significant protection with minimal human intervention.<sup>91</sup>

### 9. Storage media longevity

It is unknown how long various data storage media, such as disks, tapes, CDs or DVDs, will last. Storage media which rely on magnetic technology, such as disks and tapes, are prone to failure over time.<sup>92</sup> CDs and DVDs, when introduced, were generally believed to have a very long lifespan since they did not rely on magnetic technology.<sup>93</sup> However, mishandling of CDs and DVDs, and defects in manufacturing can shorten the life of this media substantially.<sup>94</sup> Consequently, it is advisable to store client data on multiple media to ensure that it is accessible in the future. Additionally, storing it off-site at a commercial data backup facility

---

(noting that many people gain unauthorized access to wireless access points).

90. See generally Michael Totty, *Business Solutions – How to Protect Your Network*, WALL ST. J., July 26, 2004, at R8 (discussing programs that automate collection and installation of software patches which fix software vulnerabilities).

91. See Joseph L. Kashi, *Hi-Tech in the Law Office: Data Backup: Not Glamorous, but Needed*, 22 ALASKA BAR RAG 16 (1998) (discussing the importance of backing up data and recommending nightly automated backups).

92. See Ken Feinstein, *The Road to Recovery: If Your Hard Drive Crashes and You Haven't Backed up Your Data, One of These Four Utilities Could Come to the Rescue; Data-Recovery Software*, COMPUTER SHOPPER, Sept. 1, 2003, No. 9, Vol. 23 at 130 (noting floppy disks are prone to failure).

93. See, e.g., Shaun Sparks, *Busting the Code: The Anti-Trafficking Provision of the Digital Millennium Copyright Act and Free Expression in Digital Media*, 6 INT'L J. COMM. L. & POLICY 1, 4 (2000/2001) (stating that data on DVD does not degrade).

94. See Lee Gomes, *Portal, – Beware the Fading Dye: Writeable CDs, DVDs Vary a Lot in Quality*, WALL ST. J., June 21, 2004, at B1; see also Arlyn Tobias Gajilan, *History: We're Losing It: They Told Us Digital Data Would Last Forever. They Lied. How Do We Save the Past Before it All Disappears?*, NEWSWEEK, July 12, 1999, at 47 (noting how fragile electronic storage media is).

may be necessary to ensure future access to the information.

*E. Traveling - security concerns*

Traveling with a laptop computer is a commonplace occurrence for attorneys. It allows you to carry with you a substantial amount of data and documents in digital form.<sup>95</sup> This can include e-mails, correspondence, client files, research and work-product such as briefs or memos.<sup>96</sup> Additionally, usernames and passwords for accessing e-mail and other networks are often on a laptop. Frequently, usernames and passwords may be permanently stored in an application, such as an e-mail program, so anyone using the computer can access this application.

Some basic hazards can arise from traveling with a laptop. First, users should be cognizant of the files they are using in relation to whether they are in a public or private area. It may not be advisable to display confidential data or information on a computer screen if unknown third parties can view the screen. For example, on an airplane nearby passengers can easily view your laptop screen.

Increasingly, hotels provide wireless Internet access for laptops. Restaurants<sup>97</sup> and other places also provide so-called "hotspots" where wireless Internet access is available.<sup>98</sup> This allows a user to send or receive e-mail. Often, the office network can be connected

---

95. See generally Gary McWilliams, *Technology: On the Road Again: Ten New Technologies Companies are Using to Keep Their Mobile Workers Connected and Productive*, WALL ST. J., July 26, 2004, at R1 (discussing technology used by employees to keep connected to their office when traveling).

96. See generally Perkins Coie, *Protect Your Trade Secrets!*, WASH. EMP. L. LETTER, Feb., 2004, at 2 (noting that many business executives travel extensively with laptops that contain substantial proprietary data loss of which could be devastating).

97. McDonald's Corporation plans to offer wireless Internet access in 6,000 U.S. restaurants. Peter J. Howe, *WiFi Set for Landing*, BOSTON GLOBE, June 23, 2004, at C1.

98. It is estimated that at least 15,000 hotspots will be available in the U.S and Canada by the end of the year. Such access is now available at Logan International Airport in Boston, Massachusetts. *Id.* On-line web sites even exist to facilitate finding hotspots. See, e.g., *Find Public Access Wi-Fi Hotspots*, at <http://www.wifinder.com/index.php> (worldwide directory of public access hot spots) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

to via a wireless hotspot. This allows convenient sharing of documents and other information while traveling. However, such wireless access is not risk free. First, public wireless networks are typically not secure.<sup>99</sup> This means data transmitted between your laptop and the wireless receiver/transmitter is sent unencrypted. This can allow third party interception of usernames, passwords, e-mails and documents. Password interception can be particularly problematic since it can enable unauthorized third party access to your office network. This provides another reason to periodically change e-mail and network access passwords.

Accidental loss or theft of laptops is also a concern since it can allow third parties to obtain data stored on the laptop.<sup>100</sup> Additionally, it may allow unauthorized access to your e-mail account and office network if usernames and passwords are stored on the laptop. Use of a laptop password can act as a first defense to unauthorized access to the machine. Such a password must be entered before a user can access files on the laptop. However,

---

99. T-Mobile, a company that provides publicly accessible hot-spots in airports and a variety of other locations, has the following security policy on its website:

The T-Mobile HotSpot network is based on evolving wireless technology and is not inherently secure. We therefore cannot guarantee the privacy of your data and communications while using the HotSpot service. Wireless LAN (local area network) services, like T-Mobile HotSpot, include over-the-air communications that may be illicitly intercepted by equipment and software designed for that purpose.

See T-Mobile Hot Spot Security Statement, *at*

<http://selfcare.hotspot.tmobile.com/security.htm> (last visited Aug. 19, 2004)

(on file with the Rutgers Computer and Technology Law Journal).

100. See Michael Isikoff, *Missing a Laptop of DEA Informants*, NEWSWEEK, June 7, 2004, at 12 (noting that missing DEA laptop contains sensitive data related to DEA investigations and information about confidential informants); Brad Smith, *Computer Theft Vexes Agencies Across Nation*, TAMPA TRIBUNE, Aug. 8, 2002, at 1 ("More than 300 FBI laptops containing sensitive national security information were stolen or misplaced during the past decade."); Michael Alexander, *Slimmer and Lighter Laptops Easy Theft Targets*, COMPUTERWORLD, Sept. 30, 1991, at 12 (reporting theft of laptop containing military invasion plans); see generally Bruce Brammall, *Paying Bills Via SMS Reminder*, DAILY TELEGRAPH (Sydney), May 21, 2002, (local), at 3 (noting that in Australia, the cost to businesses due to stolen laptops exceeds costs due to hacking, virus infections and computer fraud).

typically such passwords can be overcome. As a result, increasingly more travelers carry confidential or sensitive data on small memory devices called "key-chain drives."<sup>101</sup> Such devices are actually memory chips whose capacity during the last year has greatly increased while their price has substantially decreased. Currently, small pocket sized key-chain drives cost less than one-hundred dollars and can hold over one-hundred megabytes of data.<sup>102</sup> These devices have no moving parts which makes them very reliable. Additionally, they can be plugged into virtually any computer with a USB port.<sup>103</sup> Once attached, the computer views them as simply another hard drive or storage device which you can read data from or store data to.<sup>104</sup> Software is even available to encrypt the data on the key-chain drive.<sup>105</sup> Using one of these devices allows confidential data to be carried separately from a laptop so loss of the laptop will not result in loss of the data.<sup>106</sup>

Another method of protecting confidential data is to only maintain it on a computer at the office which can be accessed via the Internet. A remote laptop user can connect to the office computer from any location, worldwide, where Internet access is

---

101. Such devices are small enough to attach to a keychain. These devices, also known as USB drives, consist of small plastic cases stuffed with memory chips which retain data without electrical power. *See* TECHENCLYOPEDIA, *USB Drive*, at <http://www.techweb.com/encyclopedia/defineterm?term=USBdrive> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

102. One-hundred megabytes is a significant amount of data. A single megabyte of data roughly corresponds to 250 single-spaced typewritten pages. *See* Michael Pastore, *How to Survive the Information Revolution*, EPUBLISHERS WEEKLY, at [http://www.zorbapress.com/epweekly/f\\_epw/inforev1.htm](http://www.zorbapress.com/epweekly/f_epw/inforev1.htm) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). More expensive keychain drives can hold up to two gigabytes of data. *See, e.g.,* Search Storage.com Definitions, at [http://searchStorage.techtarget.com/sDefinition/0,290660,sid5\\_gci869057,00.html](http://searchStorage.techtarget.com/sDefinition/0,290660,sid5_gci869057,00.html) (last visited Nov. 30, 2004) (on file with the Rutgers Computer and Technology Law Journal).

103. A USB port is standard in all computers built during the last four or five years. *See generally* TECHENCLYOPEDIA, *USB Port*, at <http://www.techweb.com/encyclopedia/defineterm.jhtml> (last visited Oct. 27, 2004) (on file with the Rutgers Computer and Technology Law Journal).

104. *See* Search Storage.com, *supra* note 102.

105. *See id.*

106. *See id.*

available. Such systems have been in use for a long time. However, the level of security varies considerably on such systems.<sup>107</sup> Some simply require a username and password to connect to them. Then unencrypted data is exchanged between the office computer and the remote laptop. This arrangement provides the lowest level of security – especially when a wireless Internet connection is utilized. A more secure method involves using a virtual private network (VPN) Internet connection.<sup>108</sup> A VPN provides an encrypted connection which has a high level of security.<sup>109</sup>

#### F. *Unintended document replication*

A rule of thumb with regard to digital data is that once you create a document on a computer it may be impossible to retrieve and/or destroy all copies of that document. For example, many word processing programs, such as Microsoft WORD or WORDPERFECT, are set up to automatically save backup copies of all documents created.<sup>110</sup> Documents stored on a server, which is becoming more common today,<sup>111</sup> are often periodically backed up on removable storage media such as magnetic tape.<sup>112</sup> Deleted documents, as noted below,<sup>113</sup> are still often recoverable. Copies of documents are often shared among various individuals.<sup>114</sup> Frequently, they are shared in electronic form either by delivering a disk to another party or by sending the file as an e-mail attachment. Sending such attachments can create numerous copies including a

---

107. See generally Mark J. Maier, *Backdoor Liability from Internet Telecommuters*, 6 COMPUTER L. REV. & TECH. J. 27, 27 (2001) (discussing the risks from employees remotely accessing company network).

108. A VPN provides a private encrypted connection over a public network such as the Internet. *Id.* at 45-50.

109. See *id.* at 46-47.

110. See Gregory I. Rasin & Joseph P. Moan, *Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace*, 66 MO. L. REV. 793, 800 (2001).

111. See Gregory S. Johnson, *A Practitioner's Overview of Digital Discovery*, 33 GONZ. L. REV. 347, 369 (1997-98).

112. See *id.* at 361.

113. See *infra* Part II G. Equipment replacement issues.

114. See Johnson, *supra* note 111, at 369.

copy in the "sent" mailbox of the document originator and a copy in the "in" mailbox of the recipient.<sup>115</sup> Additionally, if the mail system mailboxes are on a server or network, it may be periodically backed up so that an additional copy exists on a backup media for the sender's mail system and on a backup media for the recipient's mail system.<sup>116</sup>

In litigation, copies of electronic media are commonly sought during discovery.<sup>117</sup> Consequently, many documents which were not intended to be available may become accessible to opposing counsel due to copies of documents which were unintentionally created and retained.<sup>118</sup>

### G. *Equipment replacement issues*

Rapidly advancing technology has resulted in a short lifespan for computers. Typically, desktop computers and laptops are replaced every three to five years.<sup>119</sup> Most computers today have relatively large hard drives which accumulate massive amounts of data during the computer's lifespan. When a computer is disposed of, the hard drive can easily be removed and much of the stored data can be retrieved from the hard drive. Even deleted files can be retrieved from the hard drive with conventional software tools.<sup>120</sup>

---

115. *See id.* at 367.

116. *See id.*

117. *See* Thornquist, *supra* note 78.

118. *See generally* Jerold S. Solovy & Robert L. Byman, *Discovery in the E-Age*, 26 NAT'L L.J. 11 (Mar. 15, 2004) (emphasizing the importance of a document retention program to minimize surprises resulting from documents being unearthed during discovery, despite the belief the documents were permanently deleted).

119. *See* Bill Howard, *Affordable, Portable Speed Demon*, PC MAG., Mar. 16, 2004, at 37 (noting that most laptops have a useful lifespan of three years).

120. In *U.S. v. Stulock*, it was stated:

that when a computer file is deleted, the contents of the file are not irretrievably lost. The space occupied by the file is flagged as available, and until new data is stored in that location the deleted file can be recovered using an undelete tool. In addition to the contents of the file, information about when the file was created, last modified, and last accessed can be recovered.

308 F.3d 922, 924 (8th Cir. 2002); *see also* Sheryl Canter, *All Is Not Lost; Here's How to Get Back Data You Thought Was Long Gone-or How to Delete it for*

Two solutions exist for preventing confidential data from being recovered from hard drives on old computers. The most effective solution is to remove and physically destroy hard drives prior to disposing of old computers.<sup>121</sup> A second solution is to use software which erases data on the hard drive in such a way that it is very difficult to retrieve it.<sup>122</sup> Typically, such programs write random data multiple times on every part of the hard drive.<sup>123</sup> The result is that it is extremely difficult, although not impossible, to recover any data files.<sup>124</sup>

The same issues that apply to hard drives apply to floppy disks, zip disks and magnetic tapes. Consequently, these media should be physically destroyed prior to disposal. Likewise, other data storage media, such as CDs, should also be physically destroyed before they are discarded. It may also be advantageous to avoid repeated reuse of such media. Otherwise, such media can end up "floating" around the enterprise with sensitive data on them.

It may be advantageous to consider a computer storage media

---

*Good*, PC MAG., Oct. 1, 2003, at 60 (recognizing that virtually any deleted file, even if it has been overwritten or the hard drive has been reformatted, can be recovered using specialized hardware and software).

121. The U.S. Department of Defense requires physical destruction of hard drives that contain top secret data. *See infra* note 123.

122. *See, e.g.*, Konstantinos Karagiannis, *Data Erasers: Emptying Your Recycle Bin Doesn't Eradicate Your Files*, PC MAG., Oct. 1, 2003, at 85 (discussing eraser programs).

123. The U.S. Department of Defense standard for erasing files on hard drives involves overwriting data files multiple times. *See* The National Indust. Sec. Program Operating Manual, available at [http://www.dss.mil/isec/nispom\\_0195.pdf](http://www.dss.mil/isec/nispom_0195.pdf) (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). This manual lists detailed erasure standards for different types of data storage mediums. *See* Manual at 8-3-5 to 8-3-6. However, if a hard drive contains "top secret" data it must be physically destroyed. *Id.* Commercial programs that meet the above Department of Defense erasure standards are generally available. For example, "Evidence Eliminator" is an inexpensive program that is very effective. For information on this program see <http://www.evidenceeliminator.us/> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). "Eraser" is a free program which is also available. *See* <http://www.heidi.ie/eraser/> (last visited Aug. 19, 2004) (on file with the Rutgers Computer and Technology Law Journal). *See generally* Karagiannis, *supra* 122, at 85.

124. *See generally* Canter, *supra* note 120, at 60.

retention policy analogous to such policies adopted today for paper files. Pursuant to such policies, paper documents, in many companies, are periodically destroyed. Such destruction has typically involved shredding. However, recently many companies have switched to outside contractors who pulverize discarded documents to ensure that they can not be reconstructed.<sup>125</sup> Similar policies for computer data would involve periodic permanent physical destruction of hard drives and other computer data storage media.

Increasingly, much of the conventional office equipment in use today contains computer data storage devices. For example, modern fax and copy machines use scanning technology which involves creating and storing a digital image of the document being faxed or copied. In the future, it may be necessary to ascertain if data can be retrieved from such storage media devices; and, if such retrieval is possible, it may be critical to permanently erase or physically destroy any storage media prior to the disposal of office equipment.

#### H. *Legacy support issues*

Computers are a relatively young technology which means hardware, software and standards continuously evolve. As computers continuously become more powerful, software becomes more sophisticated. This can result in a legacy problem when the newest versions of software are unable to read older files.<sup>126</sup> As a result, maintaining client files in digital form means they must be converted to new file types as new versions of software are utilized. This is an unreasonable approach, however, because it would

---

125. See generally Douglas Heingartner, *Back Together Again*, N.Y. TIMES, July 17, 2003, at G1 (stating that the U.S. government pulverizes, pulps or chemically decomposes sensitive data in lieu of shredding it because technology makes it possible to reassemble shredded documents).

126. See generally Gajilan, *supra* note 94, at 47 (noting how both hardware and software needed to retrieve old data often disappear in the name of progress); Dennis M. Kennedy, *Technolawyer.com: Battle for Control: Legal Technology Predictions for 2003*, 63 OR. ST. B. BULL. 27, 27 (2003) (recognizing that the compatibility with other programs, security and lack of customer support are issues related to using older software).

require continuously converting files. In contrast, another approach involves maintaining old copies of programs to insure files maintained in digital form will be readable in the future. This latter approach was recommended in a recent Maine ethics opinion addressing storage of client data in digital form.<sup>127</sup>

### *I. The hidden data problem*

Modern software, such as the widely used EXCEL spreadsheet program, PowerPoint and the ubiquitous word-processing program WORD, often store hidden data in documents created with these programs.<sup>128</sup> Such data, called "metadata,"<sup>129</sup> enhances certain software features such as editing. Typically, metadata is hidden in the sense that it is not immediately visible when opening a file.<sup>130</sup> Some of this data can be easily retrieved with minimal effort. However, other data is more deeply hidden in the sense that it is difficult to retrieve.

If an attorney only provides printed versions of documents, called hard-copy, hidden data is not an issue.<sup>131</sup> However, attorneys increasingly receive and send data in digital form.<sup>132</sup> This can be problematic if the digital document contains metadata. The recipient of the document or some third party may be able to

---

127. See Prof'l Ethics Comm'n of the Bd. of Overseers of the Bar, Op. No. 183 (Jan. 28, 2004).

128. See David A. Karp, *Revealing Codes; Warning: Hidden Data in Word and Other Office Documents May Prove Harmful to Your Career*, PC MAG., June 8, 2004, at 82.

129. "[Metadata is] information about data, such as its meaning, relationships to other data, origin, usage and format." NAACP v. Acusport Corp., 210 F.R.D. 268, 280 (E.D.N.Y. 2002). "Metadata are the electronic equivalent of a routing slip-showing when the document was created, edited, sent and received." Solovy & Byman, *supra* note 118, at 11.

130. Additionally, metadata is not included in printed or hardcopy versions of a document. See generally Zenith Elec. Corp. v. WH-TV Broad. Corp., 2004 U.S. Dist. LEXIS 13657, at \*22 (N.D. Ill. Feb. 4, 2004) (stating that the litigant sought electronic copies of documents in lieu of paper copies in order to have access to metadata only available from the electronic copies).

131. See *id.*

132. See generally Angela West, *Meeting Demands with Technology*, 26 NAT'L L.J., Mar. 22, 2004, at S1 (noting that the legal clients today seek law firms who both have and know how to use technology).

extract metadata from the document at a later date. Such data might contain confidential information that a client does not wish to disclose.<sup>133</sup>

Several solutions exist to this problem. First, documents can be converted into "portable document format" which creates a graphical image of the original document.<sup>134</sup> Typically, hidden data is not copied into this document format. Additionally, this document format is commonly used today so most recipients should be able to open such documents easily. The one negative is that documents in this format can not be easily edited.

The second solution is to use a software utility to remove metadata from documents as a routine matter once a document is completed.<sup>135</sup> This prevents retrieval of metadata from the document. It may also reduce the effectiveness of editing since such features as undelete may no longer be able to retrieve previously deleted data. However, the document can still be subject to new changes or modifications unlike a document in a graphical format which is difficult to change or modify once it is created.

#### *J. The need for computer personnel*

As computers and related technology have moved into both the business and legal world, the need for secretarial assistance has decreased in some cases. However, the increasing complexity of computer systems and the need to maintain data integrity and block unauthorized access may necessitate law firms hiring technology staff. Most large law firms already employ technology specialists.

---

133. See Karp, *supra* note 128, at 82 ("If you plan on sharing or publishing your Office document, you may be sharing more than you intend.").

134. "'Portable document format' is commonly referred to as 'PDF.' Portable document format (".pdf") documents retain the original formatting of documents. They are often used with on-line government documents, and are especially useful with forms, where retention of original formatting is essential." Diana Botluk, *Researching Telecommunications Law on the Internet*, 6 COMM'LAW CONSPECTUS 51, 53 n.18 (1998). A free program, called Adobe Acrobat Reader, is available to read PDF documents. See Adobe Acrobat Reader, at <http://www.adobe.com> (last visited August 19, 2004) (on file with the Rutgers Computer and Technology Law Journal).

135. See Karp, *supra* note 128, at 82.

Medium and small firms may likewise have to hire such personnel. Failure to do so may be considered unreasonable conduct leading to liability in the event confidential client data is disclosed, lost or otherwise compromised.

#### CONCLUSION

Reliance on paper documents could avoid many of the issues discussed in this article. However, the use of computers and digital data is, and will continue to be, a fact of life in the legal world. Moreover, businesses today rely on computer data transmission and storage so attorneys will have to utilize such technology to serve clients. In light of this, attorneys must become educated about the use of digital data and the potential risks of utilization and storage of such data. Appreciation of these risks will allow attorneys to take reasonable steps to preserve client data in accordance with ethical obligations.