

## ELECTRONIC DATA: A COMMENTARY ON THE LAW IN VIRGINIA IN 2007

*The Honorable Thomas D. Horne* \*

### I. INTRODUCTION

Just like the day we learned to ride a bike, most of us probably recall the day we were first introduced to the brave new world of computers. Little then did we realize, nor do we yet fully recognize, the power locked within the chip that processes our insatiable need for information. It is our good fortune that legal and ethical standards, rather than technology, continue to guide a principled approach to the practice of law. Computers and computer-generated data are tools only for processing information, a means to achieving an end result. Skilled advocacy and accurate decision-making depend on the collection and collation of information in a variety of forms. Now, electronic data provides the principal medium used in the pursuit of these goals.

Electronic data provides a lawyer with another source from which to obtain, retain, and disseminate information, albeit a different and novel source. Thus, it should be accorded a like dignity to that of handwritten and transcribed histories. However, the accuracy, cost, ease of recovery, and manageability of such data makes it an increasingly favored tool and target for the practitioner. So enchanted have some become with such data that clearly identifiable legal issues become clouded by bits and bytes of electronically maintained information. Litigation has become a

---

\* Judge, 20th Judicial Circuit. B.A., Muhlenberg College; J.D., Marshall-Wythe School of Law, College of William and Mary. Judge Horne wishes to thank Erin M. Martinko (B.A., 1999, Cornell University; J.D., Candidate, 2008, George Mason University School of Law), Edward J. O'Shea, III (B.A., 1999, University of Pennsylvania; J.D., Candidate, 2008, George Mason University School of Law), and Joanne V. Frye (B.A., 2001, Washington & Jefferson College; J.D., 2004, University of Richmond School of Law).

search of the information universe about one's adversary, like a similarly ill-fated search for the fountain of youth.

This article addresses several issues related to the role of electronic data: how courts and legislatures wrestle with questions concerning digital information in an attempt to maintain *stare decisis*, current legislative attempts to respond to public policy concerns about such data, and the current expansion of the common law. Both the civil and criminal law are explored here, as well as vexing questions about jurisdiction, evidence, and cost. In each section, seminal cases and legislation are introduced and then expanded upon with a discussion of the relevant principles. Each review of a specific legal topic contains thoughts on the future course of this burgeoning area of the law.

Hopefully, the reader will take from this article a better understanding of how legal issues relating to electronic data may be approached and understood. Surprisingly, once the practitioner cuts through the shroud of science and follows Alice through the looking glass, existing legal concepts remain effective and are a constant reminder that law finds its strength in the harmonizing of the old with the new, stability and custom with social change.

Concerns for confidentiality, security, and a desire to communicate ideas to either a single person or to a vast audience portend a potent mixture for litigation. Applying extant rules and statutes to legal issues arising from new technologies is not easy. Traditional molds may result in costly, inequitable, or unconstitutional results. This article will attempt to explore some of these issues from the perspective of the daily practice of law. In resolving disputes through trial or settlement, lawyers and courts are faced with not only the practical application of law to fact, but also broad policy considerations.

Lastly, I undertake this task with a sense of timidity because my knowledge of both the language and mechanics of computers, cell phones, and a host of other digital devices, is limited by both age and education.

## II. ELECTRONIC DATA: A PRIMER

Electronic data includes information stored in electronic form that can be produced or restored through the application of programs or software specifically designed to input, store, transmit,

interpret, and reproduce information or data in either electronic or print media. It may include the information specifically requested, the hard drive of a computer, a floppy disk, or a compact disk. Electronic data generally cannot be read or deciphered without the use and application of a software program specifically designed to read or interpret such data. The software program used to recapture or restore such data or the identity of such a program may, therefore, be discoverable. The best evidence of stored data in electronic form is found in the medium used for storage.

The General Assembly provided a definitional source of computer terms.<sup>1</sup> These terms include: computer; computer data; computer network; computer program; computer services; computer software; and electronic mail service provider.<sup>2</sup> The statutory definitions, however, are not as clear as they may appear. For example, a defendant was convicted by the Virginia Beach City Circuit Court under Virginia Code section 18.2-178 for obtaining a computer software package by false pretense, with intent to defraud, when she paid for the item with an uncollectible check.<sup>3</sup> The defendant appealed her conviction, arguing that the set of specifications the company delivered, which could be used to develop a computer program, did not, as charged in the indictment, constitute computer software or a computer program under Virginia Code section 18.2-152.2.<sup>4</sup>

The Court of Appeals of Virginia overturned the defendant's conviction,<sup>5</sup> holding that the specifications were neither a computer program, that is, "an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations;"<sup>6</sup> or computer software defined as a "set of computer programs, procedures and associated documentation concerned with computer data . . ."<sup>7</sup> The court reasoned that while the specifications described a computer program that could be created, it was not currently in a form that could be executed by a computer, or

---

1. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 2007).

2. *Id.*

3. *O'Connor v. Commonwealth*, 16 Va. App. 416, 417, 430 S.E.2d 567, 567-68 (Ct. App. 1993).

4. *See id.*

5. *Id.* at 418, 430 S.E.2d at 568.

6. VA. CODE ANN. § 18.2-152.2 (Cum. Supp. 2007).

7. *Id.*

cause a computer to perform an operation, and did not relate to an actual computer program in existence.<sup>8</sup>

### III. JURISDICTION

Our inquiry begins with the keystone of dispute resolution—personal jurisdiction. Given the universal nature of electronic communications, the practitioner might first ask, can my client be heard in a Virginia court on an issue dealing with electronic data? Under familiar principles, for a court in the Commonwealth to exercise personal jurisdiction over a non-resident defendant, the plaintiff must demonstrate that his allegations fall within the Virginia Long-Arm Statute<sup>9</sup> and that his cause meets the “minimum contacts” requirements of the Due Process Clause of the Fourteenth Amendment.<sup>10</sup>

In *Krantz v. Air Line Pilots Ass'n, Int'l* the court found jurisdiction where a claim by a non-resident for tortious interference with a contract was predicated upon a defendant, a non-resident member of a labor organization located in Virginia, posting information on a computer bulletin board maintained by the organization.<sup>11</sup> The defendant's union placed the plaintiff's name on a “scab list” after he withdrew from an airline pilots' strike.<sup>12</sup> After learning the plaintiff had a successful job interview with another airline, the defendant recorded a message, on his own personal computer in New York, indicating that the plaintiff was a “scab.”<sup>13</sup> The defendant then transmitted the message over an electronic switchboard system, operated by the union from its headquarters in Virginia, to union members employed at the other airline.<sup>14</sup>

The Supreme Court of Virginia considered the two-pronged analysis in finding that the plaintiff had established jurisdiction to pursue his claim in the Commonwealth by first addressing the

---

8. *O'Connor*, 16 Va. App. at 418, 430 S.E.2d at 568.

9. VA. CODE ANN. § 8.01-328.1 (Repl. Vol. 2007).

10. *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

11. 245 Va. 202, 202–207, 427 S.E.2d 326, 326–29 (1993).

12. *Id.* at 204, 427 S.E.2d at 327.

13. *Id.*

14. *Id.* at 204–05, 427 S.E.2d at 327.

application of the Long-Arm Statute to the facts.<sup>15</sup> The court examined whether the defendant had engaged in some “purposeful activity in Virginia,” and whether the result to be obtained was governed by prior case law indicating that fraudulent or defamatory statements made outside the forum state and then transmitted by telephone or mail were not “acts” within the forum jurisdiction.<sup>16</sup> Ultimately, the court determined that the defendant’s tortious interference was only completed through the specific use of the computer system operated within the Commonwealth and the subsequent acts of union members who received his message regarding the plaintiff.<sup>17</sup> The court reasoned that without the use of the computer switchboard in Virginia, the defendant could not have obtained the assistance of others, which was necessary to establish an element of tortious interference.<sup>18</sup> The court chose not to decide whether the prior case law correctly limited the applicability of long-arm statutes, so as not to include telephone or mail contacts, because the subsequent acts required to complete the tortious interference in this case rendered those cases inapplicable.<sup>19</sup>

Addressing the Due Process prong of the jurisdictional analysis, the court held that the defendant engaged in purposeful activity through his use of the computer system operated within the Commonwealth and the defendant had the minimum contacts necessary for the plaintiff to maintain his action so that the action did not “offend ‘traditional notions of fair play and substantial justice.’”<sup>20</sup>

As early as 1980, the Supreme Court of the United States observed that the limitations imposed by the Due Process Clause on state long-arm statutes had been significantly relaxed due to “a fundamental transformation in the American economy.”<sup>21</sup> The pervasive use of the Internet in both personal and business transactions has further transformed our economy and allows an

---

15. *See id.* at 205–07, 427 S.E.2d at 328–29.

16. *Id.* at 205–06, 427 S.E.2d at 328–29.

17. *See id.* at 206, 427 S.E.2d at 328.

18. *Id.*

19. *Id.*

20. *Id.* at 207, 427 S.E.2d at 328–29; *see* VA. CODE ANN. § 8.01-328.1(B) (Repl. Vol. 2006) (“Using a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth.”).

21. *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 292–93 (1980).

online act within one state to have ramifications far beyond those implicated in a long-distance telephone call, or the mailing of a letter to a recipient in another state.

Virginia practitioners should be advised of the varied subsequent impacts of an Internet posting or activity conducted physically in one location, but with the assistance of a computer system operated elsewhere. While the case law and Code of Virginia are clear regarding the specific use of computer systems located within the Commonwealth,<sup>22</sup> current decisions regarding Internet postings are less clear.

In 2002, the United States District Court for the Eastern District of Virginia, in *Verizon Online Services, Inc. v. Ralsky*, found personal jurisdiction based upon Internet use where the defendants reasonably should have expected to be subject to Virginia courts because they were “deliberately exploiting” Verizon’s e-mail services for financial gain by transmitting millions of unsolicited bulk e-mails to the plaintiff through the Internet Service Provider (“ISP”) located in Virginia.<sup>23</sup> The court cited *Bochan v. La Fontaine* in reaching its decision on jurisdiction.<sup>24</sup> The court in *Bochan* noted that Virginia courts commonly premise the exercise of personal jurisdiction based upon Internet activity by examining both the nature and quality of the activity.<sup>25</sup> Generally, courts determine whether e-mail has been sent for pecuniary gain rather than personal purposes, and in the case of the former the courts find personal jurisdiction.<sup>26</sup>

In 1999, the Loudoun County Circuit Court was confronted with a defamation action commenced in Virginia in which the plaintiff, a Pennsylvania judge, asserted that an unknown individual had published defamatory material on a website located on America Online, an ISP with its principal place of business in Loudoun County, Virginia.<sup>27</sup> The plaintiff caused a subpoena duces tecum to be issued from the clerk of the circuit court requiring the service provider produce documents identifying the individual who owned the website because no service of process could

---

22. See, e.g., VA. CODE ANN. § 8.01-328.1(B) (Repl. Vol. 2007).

23. 203 F. Supp. 2d 601, 616 (E.D. Va. 2002).

24. *Id.* (citing *Bochan v. La Fontaine*, 68 Supp. 2d 692, 701 (E.D. Va. 1999)).

25. See *Bochan*, 68 F. Supp. 2d at 701; see also *Ralsky*, 203 F. Supp. 2d at 616.

26. *Ralsky*, 203 F. Supp. 2d at 616.

27. *Melvin v. Doe*, 49 Va. Cir. 257, 257 (Cir. Ct. 1999) (Loudoun County).

be effected on the defendant in Virginia.<sup>28</sup> The defendant then challenged the jurisdiction of the court by motion and special appearance.<sup>29</sup> In determining whether it had jurisdiction, the court considered whether the allegations could be reconciled with the Virginia Long-Arm Statute.<sup>30</sup> Relying in part on *Krantz*, the court found the allegations sufficient to establish a prima facie showing for the exercise of jurisdiction under the statute because the service provider's server was located within the Commonwealth and because the server's operation was integral to publication.<sup>31</sup> Therefore, the pleading stated a tortious injury caused by an act or omission in the Commonwealth sufficient to satisfy the requirements of Virginia Code section 8.01-328.1(A)(3).<sup>32</sup>

The trial court, however, did not find the facts, as pled, sufficient to satisfy the second prong of the jurisdictional analysis—the “minimum contacts” requirement.<sup>33</sup> The Internet posting in question did not specifically target a Virginia audience and the plaintiff did not allege that the defendant lives, works, or maintains any personal or business relationships in the Commonwealth.<sup>34</sup> To the contrary, the pleadings established a matter of local interest that before the creation of the Internet would only have been published in print by peradventure in the Commonwealth.<sup>35</sup> Accordingly, without prejudice to proceeding in a proper forum, the case was dismissed.<sup>36</sup> Here, the ISP's location as a place for passive, non-commercial postings was not enough to satisfy the “minimum contacts” requirement.<sup>37</sup>

As will be seen, the Virginia General Assembly has been a powerful voice in adapting new technologies to existing law. In 2000, the General Assembly enacted the Uniform Computer Information Transactions Act (“UCITA”) governing computer information transactions.<sup>38</sup> The legislature also added section 8.01-

---

28. *Id.*

29. *Id.*

30. *Id.* at 258.

31. *Id.*

32. *Id.* (quoting *Bochan v. La Fontaine*, 68 F. Supp. 2d 692, 699 (E.D. Va. 1999)).

33. *Id.*

34. *Id.* at 259.

35. *See id.*

36. *See id.*

37. *See id.*

38. Act. of Apr. 9, 2000, ch. 996, 2000 Va. Acts 2228 (codified at VA. CODE ANN. §§ 59.1-501 to 509.2 (Repl. Vol. 2006)); J. Douglas Cuthbertson & Glen L. Gross, *Annual Sur-*

407.1 to the Virginia Code, providing a helpful and detailed procedure for obtaining subscriber information from ISPs in civil actions “where it is alleged that an anonymous individual has engaged in tortious Internet communications.”<sup>39</sup> In such cases, the practitioner confronted with such an issue should be aware of time-sensitive deadlines for making requests, including the requirement that a subpoena and supporting material must be filed with the court at least thirty days prior to the date disclosure is sought.<sup>40</sup>

The Supreme Court of Virginia, by its decision in *America Online, Inc. v. Nam Tai Electronics*, gave guidance for a practitioner seeking discovery of the identity of Internet correspondents.<sup>41</sup> In *Nam Tai*, the plaintiff corporation brought an action for libel and unfair business practices in California arising from certain postings on an Internet message board involving publicly

---

vey of Virginia Law: Technology Law, 37 U. RICH L. REV. 341, 341 (2002).

39. Cuthbertson & Gross, *supra* note 38, at 353.

40. For example, Virginia Code provides:

At least thirty days prior to the date on which disclosure is sought, a party seeking information identifying an anonymous communicator shall file with the appropriate circuit court a complete copy of the subpoena and all items annexed or incorporated therein, along with supporting material showing:

a. That one or more communications that are or may be tortious or illegal have been made by the anonymous communicator, or that the party requesting the subpoena has a legitimate, good faith basis to contend that such party is the victim of conduct actionable in the jurisdiction where the suit was filed. A copy of the communications that are the subject of the action or subpoena shall be submitted.

b. That other reasonable efforts to identify the anonymous communicator have proven fruitless.

c. That the identity of the anonymous communicator is important, is centrally needed to advance the claim, relates to a core claim or defense, or is directly and materially relevant to that claim or defense.

d. That no motion to dismiss, motion for judgment on the pleadings, or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff is pending. The pendency of such a motion may be considered by the court in determining whether to enforce, suspend or strike the proposed disclosure obligation under the subpoena.

e. That the individuals or entities to whom the subpoena is addressed are likely to have responsive information.

f. If the subpoena sought relates to an action pending in another jurisdiction, the application shall contain a copy of the pleadings in such action, along with the mandate, writ or commission of the court where the action is pending that authorizes the discovery of the information sought in the Commonwealth.

VA. CODE ANN. § 8.01-407.1(A)(1) (Repl. Vol. 2007).

41. 264 Va. 583, 590–95, 571 S.E.2d 128, 132–35 (2002).

traded stock in the corporation.<sup>42</sup> Pursuant to a commission issued by the California court, a subpoena duces tecum was issued directing the ISP to produce subscriber information relating to the author of a posting made under an anonymous screen name.<sup>43</sup> The ISP, with corporate offices located in Loudoun County, Virginia, filed a motion to quash on behalf of its anonymous subscriber.<sup>44</sup> The Supreme Court of Virginia affirmed the decision of the trial court that declined America Online's request to quash the subpoena.<sup>45</sup> Interestingly, the Virginia court requested a clarifying order from the California court prior to deciding the motion.<sup>46</sup> In so doing, the Supreme Court of Virginia noted the similarities between the procedures governing such motions in California and Virginia.<sup>47</sup>

#### IV. DISCOVERY

In preparation for both civil and criminal trials, a lawyer may be required to take steps that are directly related to electronic data. Thus, he or she may be called upon to preserve, acquire, catalogue, or protect electronic data. As part of the pretrial discovery process, it may be necessary to identify electronic data and to prepare suitable responses to specific discovery requests.

Discovery may include depositions, written interrogatories, requests for admissions, and subpoenas to third parties. Before a response can be initiated or a request tailored to the issues presented in a case, it is important to identify what data is requested, in what form it is kept, and how it is relevant to the issues presented by the underlying action. The Rules of the Supreme Court of Virginia provide:

---

42. *See id.* at 586, 571 S.E.2d at 129.

43. *See id.* at 587–88, 571 S.E.2d at 130.

44. *Id.*

45. *Id.* at 596, 571 S.E.2d at 135.

46. *Id.* at 589, 571 S.E.2d at 131.

47. *See id.* at 591, 571 S.E.2d at 132; *see also* America Online, Inc. v. Anonymous Publicly Traded Co., 261 Va. 350, 360, 542 S.E.2d 377, 383 (2001) (“Virginia courts should grant comity to any order of a foreign court of competent jurisdiction, entered in accordance with the procedural and substantive law prevailing in its judicatory domain, when that law, in terms of moral standards, societal values, personal rights, and public policy, is reasonably comparable to that of Virginia.” (quoting *Oehl v. Oehl*, 221 Va. 618, 623, 272 S.E.2d 441, 444 (1980))).

Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter.<sup>48</sup>

Practitioners must take care in assessing the importance of moving for discovery of such data because it may be both costly and time consuming. When relevant to the issues, however, no more powerful evidence can be obtained. The strength of such evidence comes from the neutrality of the third parties involved in the obtaining and retention of such data; such as telecommunications carriers, cable companies, and ISPs.

In seeking electronic data, a host of issues may arise that are unfamiliar to the practitioner who was raised on “paper discovery.” Notice is an important consideration in evaluating a search for such data. For example, ISPs are required to notify subscribers of requests for subscribers’ information, and the ISPs may assert privilege claims on their behalf.<sup>49</sup> Requesting parties may wish to employ experts, when necessary, and be prepared to adhere to protective orders limiting access and the use of the materials. Deleted data may be recaptured or restored later, unlike a paper placed in the trash for delivery to the dump. Deleted data will likely be the first thing sought and the last thing a party may want to produce.

Ownership of a computer does not automatically grant access to matters otherwise privileged. A test that could be applied in the case of a computer owned by another or subject to use by more than one person is whether the creator or user of such information had an expectation of privacy in the communications made or kept; or whether the use of the computer was for an employer or for company business.

Factors to consider in the protection of such data from disclosure would be the nature of the data transmitted, the authority of the person accessing the data, and the expectation of privacy of the person involved in the communication. Discovery requests should be carefully tailored to avoid being attacked as overreach-

---

48. VA. SUP. CT. R. 4:1.

49. See VA. CODE ANN. § 8.01-407.1(A)(3)–(4) (Repl. Vol. 2007).

ing. Specific requests must only consist of data that is relevant to the subject matter involved in the underlying action.<sup>50</sup> This may include a request for the identification of the place where the data is stored, the production of a hard drive, compact disk or floppy disk, as well as the identification of, or access to, the application software necessary to access the data.

Impediments to production may include such issues as: relevancy and materiality; privilege; adherence to procedural guidelines; record keeping and capture; over-reaching (burdensome discovery); spoliation; duplication; authentication; interpretation; and the need for expert assistance.<sup>51</sup> The Rules of the Supreme Court of Virginia require the production of data compilations in a reasonably useable form, including material translated by detection devices.<sup>52</sup> Therefore, electronic data compilations are “documents” that are subject to production.<sup>53</sup> The fact that computers may contain encrypted information does not appear to limit access because the information could be obtained, albeit with greater difficulty. It is best to request both printed and electronic versions.

Any claim of privilege regarding electronic data must include a privilege list, known in practice as a “Vaughn Index.”<sup>54</sup> In developing a privilege list, the separation of privileged material from that which is not privileged may prove difficult when the disputed material is contained in computer storage. For instance, personal privileged e-mail may be stored on a company computer. Where a company permits the use of its computer for personal use, such material may remain recoverable even after the employee has ceased work with the business and turned in the computer. Employers should be advised with respect to such issues, and employees should be reminded of the nature of e-mail transmissions and the manner in which they are kept and retained.

Interesting issues arise when evaluating discovery requests and privilege claims related to electronic communications transmitted through ISPs. If a privilege claim is asserted or contested,

---

50. *See* VA. SUP. CT. R. 4:1.

51. *See id.*

52. VA. SUP. CT. R. 4:9.

53. *See id.*

54. *See* VA. SUP. CT. R. 4:1(b)(6); *see generally* Vaughn v. Rosen, 484 F.2d 820, 827–28 (D.C. Cir. 1973) (setting forth indexing requirement) .

factors to consider might include: agreements between individuals and communications carriers such as ISPs; access to passwords necessary to unlock the stored data; past use of the storage medium; and agreements between the owner and user. E-mail content can be accessed by the ISP, and data deleted from the hard drive of the sending or receiving computer may still be accessed on a server. Additionally, information retained by Internet companies may be recovered by subpoena or court order.

There is a difference, however, between stored and intercepted electronic data. An oral communication is protected where the speaker expects the conversation not to be intercepted and circumstances justify that belief.<sup>55</sup> E-mail may likewise be privileged where the author has a reasonable expectation of privacy in such communication, even though the e-mail is subject to inspection by an ISP or employer. Encryption, although unnecessary to invoke the privilege, does heighten the level of security in the conversation or transmission. Ownership of the storage medium and the expectation of privacy in retaining data in the storage medium serve as guideposts for Virginia courts in deciding claims of privilege. For example, the right to correspond anonymously is protected by the First Amendment,<sup>56</sup> and the Internet has been recognized as a significant medium of communication subject to ordinary First Amendment scrutiny.<sup>57</sup> Furthermore, an ISP has standing to assert some rights of its anonymous subscribers.<sup>58</sup>

The attorney-client privilege and the work product doctrine play an important role in the discovery and use of electronic data if the claim extends to electronic documents prepared by the attorney or supporting staff,<sup>59</sup> or even electronic documents prepared by the client with the intention of securing legal advice on its contents.<sup>60</sup> Electronic communications between officers and

---

55. *Wilks v. Commonwealth*, 217 Va. 885, 888, 234 S.E.2d 250, 252 (1977) (wiretap interception).

56. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341–42 (1995).

57. *See Reno v. ACLU*, 521 U.S. 844, 850, 870 (1997) (ruling that Internet speech is protected by the same level of First Amendment scrutiny as other media).

58. *See, e.g., NAACP v. Alabama*, 357 U.S. 449, 459–60 (1958) (noting that effect on organization is considered where lists of members sought in discovery).

59. *See Commonwealth v. Edwards*, 235 Va. 499, 509–10, 370 S.E.2d 296, 301–02 (1988) (citing *Hickman v. Taylor*, 329 U.S. 495, 511 (1947)).

60. *See Va. Elec. & Power Co. v. Westmoreland-LG&E Partners*, 259 Va. 319, 325, 526 S.E.2d 750, 755 (2000) (citing *Robertson v. Commonwealth*, 181 Va. 520, 539–40, 25 S.E.2d 352, 360 (1943)).

employees of the same entity relayed to corporate counsel for obtaining legal advice are also entitled to the attorney-client privilege.<sup>61</sup> Electronic materials prepared in anticipation of litigation (i.e., work product) are shielded from discovery just like their tangible equivalents, absent a showing of substantial need and undue hardship in obtaining the substantial equivalent of such materials by other means.<sup>62</sup>

Some courts have used a test, as equally applicable to electronic evidence as to other evidence, to determine if materials are considered work product because litigation was reasonably foreseeable at the time the materials were prepared.<sup>63</sup> Once the party asserting privilege meets the burden of demonstrating that the materials in question were prepared in anticipation of litigation, the opposing party must prove a substantial need for the information and the inability to otherwise acquire the materials without undue hardship.<sup>64</sup>

In *Malone v. Ford Motor Co.*, the defendant corporation contended that a computerized database used to manage information, including documents furnished separately in discovery, was work product because counsel assisted in the development and updating of the database in anticipation of litigation.<sup>65</sup> The court held that the database was work product and reasoned that “[t]he mere possibility that a party might not produce all relevant, unprotected documents, is not a sufficient basis for ordering such a party to disclose its entire computerized system of information management.”<sup>66</sup> As rapid technological change continues, varied degrees of capability in taking advantage of technology are inevitable between adverse parties. The court must strike a balance in assessing undue burden claims, respecting the technological abilities of the parties while preventing a perverse incentive to argue lack of technological capabilities in order to avoid electronic discovery requests.

---

61. *Id.* at 326, 526 S.E.2d at 755 (citing *Owens-Corning Fiberglass Corp. v. Watson*, 243 Va. 128, 141, 413 S.E.2d 630, 638 (1992)).

62. VA. SUP. CT. R. 4:1(b)(3); see generally *Hickman*, 329 U.S. at 512 (establishing burden to overcome work product protection).

63. See, e.g., *Larson v. McGuire*, 42 Va. Cir. 40, 42–43 (Cir. Ct. 1997) (Loudoun County).

64. See *id.* at 43.

65. 29 Va. Cir. 456, 456–57 (Cir. Ct. 1992) (Loudoun County).

66. *Id.* at 459 (quoting *Lawyers Title Ins. Corp. v. U.S. Fid. & Guar. Co.*, 122 F.R.D. 567, 570 (N.D. Cal. 1988)).

During the pretrial phase of litigation, Virginia practitioners should work with their clients to ensure electronic data subject to discovery is maintained because spoliation of electronic evidence may merit sanctions if bad faith or prejudice can be proven.<sup>67</sup> In *Gentry v. Toyota Motor Corp.*, an expert employed by the plaintiff's attorney removed a part from a car involved in an auto accident without authorization or permission.<sup>68</sup> The Supreme Court of Virginia ruled that the trial court had abused its discretion when dismissing the case because there was no evidence of bad faith on the part of the plaintiff, who had not authorized the expert's actions.<sup>69</sup> When considering claims of the destruction of evidence it is important to note that there is no independent cause of action for spoliation of evidence in Virginia.<sup>70</sup>

## V. EVIDENTIARY ISSUES

Once the pretrial phase is complete, attention focuses on the trial. In preparing for trial, the lawyer should be mindful of evidentiary issues that may arise to ensure admission of critical pieces of evidence. This would, in most cases, involve the harmonizing of data collection and storage techniques with traditional rules of evidence. A review of extant case authority reveals the extent to which traditional rules of evidence may be applied to the use of electronic data.

The admission of electronic evidence is controlled by common law and statutory proscription. Where there exists a possibility of contamination of evidence, the proponent of the exhibit must demonstrate to a reasonable certainty that the evidence has not been tampered with.<sup>71</sup> The reasonable certainty requirement, however, is not met if a "vital link in the chain of possession is not accounted for. . . ."<sup>72</sup>

---

67. See, e.g., *Gentry v. Toyota Motor Corp.*, 252 Va. 30, 34, 471 S.E.2d 485, 488 (1996).

68. *Id.*, 471 S.E.2d at 486 (1996).

69. *Id.*, 471 S.E.2d at 488. Additionally, the underlying theory of the case ultimately rested on another part in the car that had not been damaged. *Id.*

70. See *Austin v. Consolidation Coal Co.*, 256 Va. 78, 83–84, 501 S.E.2d 161, 163–64 (1998).

71. *Robinson v. Commonwealth*, 212 Va. 136, 138, 183 S.E.2d 179, 180 (1971).

72. *Id.*

The admission of computer data that represents material gathered by persons rather than gathered in response to electronic stimuli is governed by the business records exception to the hearsay rule.<sup>73</sup> The reliability of electronic data is controlled by familiar principles. Where the reliability of data generated by a computer is dependent on proof of scientific accuracy, however, expert testimony may be required. For example, information gathered by a “call trap” placed on a telephone to record calls to a residence requires a showing of reliability.<sup>74</sup>

In *Penny v. Commonwealth*, the Court of Appeals of Virginia held that once the reliability of a call trap device has been proven, the results attendant to its use may be received into evidence.<sup>75</sup> The court in *Penny*, however, made clear that the “requirement of proof of reliability for each call trap may not necessarily apply to other instances involving computer generated data.”<sup>76</sup> Because the call trap is generally utilized for litigation purposes in an adversarial process “of ferreting out criminal agents,” the court reasoned an additional check for reliability is necessary.<sup>77</sup> The court reasoned that call trap evidence is just the recording of electronic events without human interaction.<sup>78</sup> Therefore, hearsay concerns are unfounded as no out-of-court declarant exists who could be subject to cross-examination.<sup>79</sup>

In *Tatum v. Commonwealth*, the Court of Appeals of Virginia found that “caller ID” data is also not hearsay because it is based on computer generated information and is not a record of human input and observation.<sup>80</sup>

Call trap and caller ID evidence of telephone communications are treated differently than computer recordings of the content of conversation.<sup>81</sup> Under Virginia Code section 8.01-420.2, “[n]o me-

---

73. See *Frye v. Commonwealth*, 231 Va. 370, 387, 345 S.E.2d 267, 279–80 (1986) (finding the business records exception to the hearsay rule applies to computer printout from the National Crime Information Center).

74. *Penny v. Commonwealth*, 6 Va. App. 494, 499, 370 S.E.2d 314, 317 (Ct. App. 1988).

75. *Id.*

76. *Id.* at 500 n.3, 370 S.E.2d at 317 n.3.

77. *Id.*

78. *Id.* at 498, 370 S.E.2d at 317.

79. *See id.*

80. 17 Va. App. 585, 588, 440 S.E.2d 133, 135 (Ct. App. 1994).

81. *See, e.g.*, VA. CODE ANN. § 8.01-420.2 (Repl. Vol. 2000) (limitations on admissibility in civil proceedings of recordings of telephone conversations).

chanical recording, electronic or otherwise, of a telephone conversation” can be admitted into evidence in any civil proceeding unless all parties to the conversation are aware they are being recorded and certain other conditions are met.<sup>82</sup> Under Virginia Code section 19.2-61(b), an oral communication intercepted electronically is also protected where the speaker expects the conversation not to be intercepted and the circumstances justify that belief.<sup>83</sup> The constitutional expectation of privacy under the Fourth Amendment is applied in such circumstances.<sup>84</sup> The contents of an intercepted communication and the evidence derived from such communications (both wire and oral) may be subject to suppression in both criminal and civil cases.<sup>85</sup>

Individuals often identify themselves online using screen names or e-mail addresses which complicates the process of identification. The Supreme Court of Virginia ruled that the identity of an individual corresponding over the Internet can be established at trial by direct or circumstantial evidence such as e-mail or participation in group discussions such as “chat rooms.”<sup>86</sup> In *Bloom v. Commonwealth*, the statements made over the Internet by a defendant were properly admitted into evidence under the party admission exception to the hearsay rule.<sup>87</sup> The measure of proof necessary to establish identity and for the admission of such evidence is by a preponderance of the evidence.<sup>88</sup> In *Bloom*, however, the Supreme Court of Virginia explicitly chose not to adopt the trial court’s assertion that conversations over the Internet are analogous to conversations over the telephone reasoning that the

---

82. *Id.* Specifically, “all parties to the conversation were aware the conversation was being recorded or (ii) the portion of the recording to be admitted contains admissions that, if true, would constitute criminal conduct which is the basis for the civil action, and one of the parties was aware of the recording and the proceeding is not one for divorce, separate maintenance or annulment of a marriage. The parties’ knowledge of the recording pursuant to clause (i) shall be demonstrated by a declaration at the beginning of the recorded portion of the conversation to be admitted into evidence that the conversation is being recorded. This section shall not apply to emergency reporting systems operated by police and fire departments and by rescue squads, nor to any communications common carrier utilizing service observing or random monitoring pursuant to § 19.2-62.” *Id.*

83. VA. CODE ANN. § 19.2-61(b) (Cum. Supp. 2007); *see generally* *Wilks v. Commonwealth*, 217 Va. 885, 888, 234 S.E.2d 250, 252 (1977).

84. *See Wilks*, 217 Va. at 888–89, 234 S.E.2d at 252.

85. VA. CODE ANN. § 19.2-65 (Repl. Vol. 2004).

86. *See Bloom v. Commonwealth*, 262 Va. 814, 820–21, 554 S.E.2d 84, 87 (2001).

87. *Id.* at 820, 554 S.E.2d at 87.

88. *Id.* at 821, 554 S.E.2d at 87 (citing *Witt v. Commonwealth*, 215 Va. 670, 674, 212 S.E.2d 293, 296 (1975)).

parties do not have the opportunity for voice recognition during Internet communications.<sup>89</sup>

## VI. CRIMINAL PROSECUTIONS

In addition to civil liability arising from actions performed with computers, and the issues that arise from the use of computers and electronic records in the litigation process, computers may be used in the commission of crimes. Criminal proscriptions that traditionally existed without the use of electronic media have been extended into the digital world. For instance, the alteration of public computer records has been held to constitute forgery despite the absence of a traditional writing on paper.<sup>90</sup> Computer activities may also be used as evidentiary support for traditional crimes.<sup>91</sup>

Crimes specifically arising from the possession and use of computers and computer networks have been identified by the General Assembly in the Virginia Computer Crimes Act (“VCCA”).<sup>92</sup> The Act does not explicitly preclude prosecution under other statutes for crimes that may also fall under the VCCA unless clearly inconsistent with the terms of the Act.<sup>93</sup> The VCCA reflects a continued understanding of the importance of technology in society while balancing the need to protect citizens from the pervasive impact of global computer networks that reach into our homes and businesses.

The VCCA makes it a crime to fraudulently use a computer to obtain property, including money.<sup>94</sup> This prohibition has been read broadly to include activities in furtherance of a theft, such as checking vehicle identification numbers (“VIN”) through the

---

89. *Id.* at 822 n.2, 554 S.E.2d at 88 n.2.

90. *See* *Campbell v. Commonwealth*, 246 Va. 174, 176–78, 431 S.E.2d 648, 649–51 (1993).

91. *See* *Barnes v. Commonwealth*, No. 2693-98-1, 2000 Va. App. LEXIS 204 (Ct. App. Mar. 21, 2000) (unpublished decision). In *Barnes*, evidence of computer searches of a stolen vehicle database were used to show that a police officer was aware that property she received was stolen. *Id.* at \*4–6.

92. Act of Apr. 11, 1984, ch. 751, 1984 Va. Acts 1759 (codified as amended at VA. CODE ANN. §§ 18.2-152.1 to -.15 (Repl. Vol. 2004 & Cum. Supp. 2007)).

93. VA. CODE ANN. § 18.2-152.11 (Repl. Vol. 2004).

94. *Id.* § 18.2-152.3 (Cum. Supp. 2007).

Commonwealth computer network to ascertain whether a vehicle remained on a list of stolen vehicles.<sup>95</sup>

The VCCA also makes it a crime to send spam e-mail, called “Unsolicited Bulk Email” (“UBE”) under certain circumstances.<sup>96</sup> Falsifying the transmission information or trafficking in software designed to falsify that information is a misdemeanor.<sup>97</sup> Sending bulk e-mail to more than a certain number of intended recipients or bulk e-mail that generates more than a certain amount of revenue constitutes a class six felony.<sup>98</sup> Additionally, the employment of a minor to violate the proscriptions on bulk e-mail is a felony.<sup>99</sup> The VCCA also creates civil liability for sending unsolicited bulk e-mail, including significant statutory damages.<sup>100</sup>

A prosecution for a violation of the Virginia spam statute resulted in a challenge based upon, among other things, constitutional Due Process, Free Speech, and Commerce Clause violations.<sup>101</sup> While the trial court’s conviction was affirmed by the court of appeals,<sup>102</sup> the matter is currently on appeal to the Supreme Court of Virginia.<sup>103</sup>

Computer trespass is defined to include a myriad of activities that interfere with the normal functioning of a computer, or using a computer or network to make unauthorized copies of data or software.<sup>104</sup> Computer trespass is a class one misdemeanor unless the trespass causes damage to another’s property in excess of

---

95. *Barnes*, 2000 Va. App. LEXIS 204, at \*4–6.

96. VA. CODE ANN. § 18.2-152.3:1 (Repl. Vol. 2004 & Cum. Supp. 2007).

97. *Id.* § 18.2-152.3:1(A)(2)(ii)–(iii) (Repl. Vol. 2004 & Cum. Supp. 2007). Federal law now supersedes most state anti-spam laws except for those like Virginia’s that prohibit falsity or deceit in any portion of an electronic mail message or attachments thereto. 15 U.S.C. § 7707(b)(1) (Supp. 2007).

98. VA. CODE ANN. § 18.2-152.3:1(B) (Repl. Vol. 2004 & Cum. Supp. 2007). The number of recipients is 10,000 recipients in a day, 100,000 within 30 days, or 1,000,000 in a year; the revenue is \$1,000 for a specific transmission or \$50,000 from the customers of any individual mail provider. *Id.*

99. *Id.* § 18.2-152.3:1(C) (Repl. Vol. 2004 & Cum. Supp. 2007).

100. *Id.* § 18.2-152.12(B)–(C) (Cum. Supp. 2007). If requested, courts have the ability to protect the secrecy and security of parties engaged in litigation that arises out of the VCCA. *Id.* § 18.2-152.12(D) (Cum. Supp. 2007).

101. *See Commonwealth v. Jaynes*, 65 Va. Cir. 355, 357, 363, 365–67 (Cir. Ct. 2004) (Loudoun County).

102. *Jaynes v. Commonwealth*, 48 Va. App. 673, 704, 634 S.E.2d 357, 372 (Ct. App. 2006) (appeal docketed), No. 062388 (Va. Apr. 24, 2007).

103. *See* Supreme Court of Virginia Appeals Docketed, <http://www.courts.state.va.us/scv/appeals/062388.html> (last visited Sept. 17, 2007).

104. *See* VA. CODE ANN. § 18.2-152.4(A) (Cum. Supp. 2007).

\$1,000, in which case it is a class six felony.<sup>105</sup> The section of the statute proscribing computer trespass explicitly does not apply to Virginia ISPs' e-mail filtering activities or to parental monitoring.<sup>106</sup> It also explicitly allows parties to contract around the proscription.<sup>107</sup> The VCCA also creates civil liability for computer trespass regardless of malice.<sup>108</sup>

Recognizing the power of computers and networks to access a great deal of information, the Virginia General Assembly created a protection against invasion of privacy using computers.<sup>109</sup> The VCCA makes it a class one misdemeanor to use a computer or network to examine personal information, such as financial, employment, or identifying information about another person without permission.<sup>110</sup> The violation is upgraded to a class six felony if the perpetrator then sells or distributes the information, commits the violation in the course of committing another crime, or has previously been found guilty of the same act or a substantially similar crime in the United States.<sup>111</sup> There is an exception for persons collecting information that is reasonably needed for computer security, for diagnostics or repair, or for purposes of identifying a computer user.<sup>112</sup> Although the statute requires that the person know he is without authority at the time the information is examined,<sup>113</sup> the statute has been interpreted broadly.<sup>114</sup> Theft

---

105. *Id.* § 18.2-152.4(B) (Cum. Supp. 2007).

106. *See id.* § 18.2-152.4(C) (Cum. Supp. 2007).

107. *Id.*

108. *Id.* § 18.2-152.12(A) (Cum. Supp. 2007). The statute of limitations for actions arising out of this section are contained in section 18.2-152.12(F). If requested, courts have the ability to protect the secrecy and security of parties engaged in litigation that arises out of the VCCA. *Id.* § 18.2-152.12(D) (Cum. Supp. 2007).

109. Act of Apr. 11, 1984, ch. 751, 1984 Va. Acts 1759 (codified as amended at VA. CODE ANN. § 18.2-152.5 (Cum. Supp. 2007)).

110. *See* VA. CODE ANN. § 18.2-152.5(A)–(B) (Cum. Supp. 2007).

111. *See id.* § 18.2-152.5(C)–(E) (Cum. Supp. 2007).

112. *See id.* § 18.2-152.5(F) (Cum. Supp. 2007).

113. *See id.* § 18.2-152.5(A) (Cum. Supp. 2007).

114. *See, e.g.,* *Plasters v. Commonwealth*, No. 1870-99-3, 2000 Va. App. LEXIS 473 (Ct. App. June 27, 2000) (unpublished decision) (decided under prior statute). In *Plasters*, a dispatcher accessed personal information that was contained in the Virginia Criminal Information Network while working as a police dispatcher. *Id.* at \*2–3. The court of appeals held that it did not matter the defendant did not know that accessing the personal information was a crime, and it affirmed the defendant's convictions because of an on-screen warning that information from the system was to be used for criminal justice purposes only. *Id.* at \*5–6. *Plasters* did draw a dissent, which noted that the handbook the employee received did not contain an admonition against viewing the type of information involved, while the release of other information was clearly defined as unauthorized by the hand-

of computer services is also a misdemeanor under the VCCA, or a felony if the value of services stolen is over \$2,500.<sup>115</sup>

The VCCA defines the crime of personal trespass by computer as the use of a computer or computer network to cause physical injury to an individual.<sup>116</sup> This is a class six felony if committed unlawfully but not maliciously, and a class three felony if done maliciously.<sup>117</sup> Malice in this circumstance is defined in accordance with familiar principles as the state of mind that results in the completion of a wrongful act when the mind is within the control of reason and without justification or legal excuse.<sup>118</sup> There has been at least one attempt to apply personal trespass by computer to injuries to the profitability of a business, but it is not clear that this extension can be maintained.<sup>119</sup>

Harassment by computer is also a crime defined by the VCCA.<sup>120</sup> Harassment is a class 1 misdemeanor, which involves using a computer or network to make one of a variety of obscene or vulgar communications with the intent to harass or intimidate.<sup>121</sup>

In Virginia Code section 18.2-152.8, the legislature provides a laundry list of property subject to embezzlement, including computers, networks, financial instruments, data, software, and all other personal property.<sup>122</sup> The taking of these assets, whether tangible or intangible, in a readable format, or even in transit between devices, is considered embezzlement.<sup>123</sup> The provision also

---

book. *Id.* at \*8-9 (Benton, J., dissenting). The overall breadth of the privacy protection may still not be well defined.

115. VA. CODE ANN. § 18.2-152.6 (Cum. Supp. 2007).

116. *Id.* § 18.2-152.7(A) (Cum. Supp. 2007).

117. *Id.* § 18.2-152.7(B) (Cum. Supp. 2007).

118. *Saunders v. Commonwealth*, 31 Va. App. 321, 324, 523 S.E.2d 509, 510 (Ct. App. 2000).

119. *See Saks Fifth Ave., Inc. v. James, Ltd.*, 272 Va. 177, 630 S.E.2d 304 (2006). *Saks* involved a salesperson who switched employment to a competing firm and brought electronic customer records stored on his computer with him; he apparently contacted former customers using e-mail. *Id.* at 182, 630 S.E.2d at 307. *Saks* was a civil dispute, but persons injured by actions taken under *any* section of the Virginia Computer Crimes Act may recover under Virginia Code section 18.2-152.12, which provides for civil actions. VA. CODE ANN. § 18.2-152.12 (Cum. Supp. 2007). However, the trial court struck the evidence as to the claim for conversion based on personal trespass by computer. *See Saks*, 272 Va. at 185 n.11, 630 S.E.2d at 309 n.11.

120. *See* VA. CODE ANN. § 18.2-152.7:1 (Repl. Vol. 2004 & Cum. Supp. 2007).

121. *Id.*

122. *Id.* § 18.2-152.8 (Cum. Supp. 2007).

123. *Id.*

applies to computer services.<sup>124</sup> In *Perk v. Vector Resources Group*, the Supreme Court of Virginia held that the value of information contained in computer files was a matter of fact to be decided at trial.<sup>125</sup> Creating, altering, or deleting computer data in a manner that would constitute forgery on traditional media is deemed to be forgery under the VCCA.<sup>126</sup> The Act also makes it an independent misdemeanor to willfully use encryption in furtherance of any criminal activity.<sup>127</sup>

Computer crimes have not escaped the implications of forfeiture. In Virginia, all computer equipment, software, and other personal property used in a computer crime defined by the VCCA can be subject to forfeiture.<sup>128</sup> There is also a specific statute of limitations provision for crimes arising out of the VCCA—misdemeanors pursuant to the VCCA must be prosecuted within five years of the last act constituting the violation, or one year after the act or identity of the offender was discovered.<sup>129</sup> A criminal prosecution for an act proscribed by the VCCA has a wide choice of venues. Venue may lie where any of the acts in furtherance of the crime were committed, where the owner has a principal place of business, where the offender has control or possession of material used to commit the crime, where access to a computer or network was made, where the offender resides, or where a

---

124. *Id.* § 18.2-152.8(3) (Cum. Supp. 2007).

125. 253 Va. 310, 315, 485 S.E.2d 140, 143 (1997). *Perk* was a civil case based on the computer crimes act. *Id.* The plaintiff, an attorney who had been hired to collect on the defendant's outstanding debts, claimed that he had invested substantial time and money in creating his own computer programs and databases for the project, and that the defense had converted programs, databases, software, and data in violation of the statute. *Id.* at 313, 485 S.E.2d at 142. The defense claimed that the items allegedly converted were nothing more than the plaintiff's client's lists, that they belonged to the employer and that the lists were of no value to the plaintiff once the contract had been terminated. *Id.* at 315, 485 S.E.2d at 143. The trial court granted a demurrer. *Id.* at 312, 485 S.E.2d at 141–42. The Supreme Court of Virginia held that the question of whether those items had value to the contractor other than his obligations to his employer was a matter of proof that cannot be decided on demurrer. *Id.* at 315, 485 S.E.2d at 143.

126. VA. CODE ANN. § 18.2-152.14 (Repl. Vol. 2004); *see also* Commonwealth v. Bechtler, 56 Va. Cir. 186 (Cir. Ct. 2001) (Rockingham County). In *Bechtler*, this section of the VCCA was held not to extend to copies of the seal on the Virginia driver's license, because the image on the license is not actually the Virginia seal, but a mere representation. *Id.* at 187. Because the statute imputes liability for what would be a crime without a computer, the court dismissed the indictment because the underlying conduct would not be considered a forgery. *Id.*

127. VA. CODE ANN. § 18.2-152.15 (Repl. Vol. 2004).

128. *See* VA. CODE ANN. § 19.2-386.17 (Repl. Vol. 2004).

129. *Id.* § 19.2-8 (Cum. Supp. 2007).

computer that was an instrument or object of the crime was at the time of the commission.<sup>130</sup>

One area of traditional criminal law that is particularly relevant to changing electronic technology is wiretapping. Wiretapping laws were enacted to allow law enforcement officers to respond to a different generation of criminal activity with new and innovative technology. Traditional privacy concerns are reflected in the Interception of Wire, Electronic, or Oral Communications Act (“IWEOCA”).<sup>131</sup> The Act has broad applications—defining, for instance, “electronic communication systems” as including computer facilities.<sup>132</sup> The Act makes it a felony to unlawfully:

- i. Intentionally intercept, or procure another to intercept, any wire, electronic, or oral communication;
- ii. Intentionally use, or procure another to use, an electronic, mechanical, or other device to intercept an oral communication;
- iii. Intentionally disclose the contents of a wire, electronic, or oral communication knowing that it was obtained through an interception of a wire, electronic, or oral communication; or
- iv. Intentionally use the contents of a wire, electronic, or oral communication knowing it to have been obtained through interception.<sup>133</sup>

There are, however, exceptions. The exceptions for communications service providers relate primarily to activities arising in the normal course of business or service quality checks, as well as in assistance to law enforcement officers who are authorized to intercept communications.<sup>134</sup> While the statute allows service providers to intercept communications, they are prevented from divulging the contents of any communications.<sup>135</sup> Another exception is made for situations where one of the parties to the communication has consented.<sup>136</sup> Other exceptions are made for communications that are already accessible to the general public and radio

---

130. *Id.* § 19.2-249.2 (Cum. Supp. 2007).

131. *See id.* §§ 19.2-61 to -70.3 (Repl. Vol. 2004 & Cum. Supp. 2007).

132. *Id.* § 19.2-61 (Cum. Supp. 2007).

133. *Id.* § 19.2-62(A) (Repl. Vol. 2004 & Cum. Supp. 2007).

134. *Id.* § 19.2-62(B)(1), (3)(f) (Repl. Vol. 2004 & Cum. Supp. 2007).

135. *Id.* § 19.2-62(C) (Repl. Vol. 2004 & Cum. Supp. 2007).

136. *Id.* § 19.2-62(B)(2) (Repl. Vol. 2004 & Cum. Supp. 2007).

communications such as those made on emergency, nautical, or amateur frequencies.<sup>137</sup>

Detailed procedures are set forth for court ordered authorization of the interception of wire, electronic, and oral communications.<sup>138</sup> Less stringent procedures are provided in the case of the disclosure of customer and subscriber information, excluding the contents of electronic communication.<sup>139</sup> While electronic communication *transfers* are subject to detailed procedures in the IWEOCA, the contents of e-mail stored with a service provider would be subject to the general requirements for the issuance of a search warrant.<sup>140</sup> Virginia makes good faith reliance by a person upon a court order or legislative authorization a complete defense to an action for unlawful interception, disclosure, or use.<sup>141</sup>

IWEOCA defines “pen registers” and tracing devices separately.<sup>142</sup> A pen register is a device that records dialing, routing, addressing, or signal information transmitted by an instrument (but not the contents of the communication) while a “trap and trace device” captures incoming electronic identifiers.<sup>143</sup> The Act excludes any device used for billing from its pen register definition.<sup>144</sup> Pen registers are banned under the Act, absent a court order, and have different exceptions than those for content-based communications.<sup>145</sup> The Act makes it a class one misdemeanor to use a pen register or trap and trace without a court order.<sup>146</sup> The only exceptions to this are for service providers using the routing information to test or maintain equipment, record the fact that a communication occurred to protect from fraud or abuse of service, or where the user consents.<sup>147</sup>

Evidence from pen registers used at the request of one party to a communication is admissible in criminal proceedings. For in-

---

137. *Id.* § 19.2-62(B)(3) (Repl. Vol. 2004 & Cum. Supp. 2007).

138. *Id.* § 19.2-68 (Cum. Supp. 2007).

139. *See id.* § 19.2-70.3 (Repl. Vol. 2004).

140. *See id.* § 19.2-53 (Repl. Vol. 2004).

141. *Id.* § 19.2-69 (Repl. Vol. 2004).

142. *Id.* § 19.2-61 (Cum. Supp. 2007).

143. *Id.*

144. *Id.*

145. *Compare id.* § 19.2-70.1 (Repl. Vol. 2004), *with id.* § 19.2-62(B) (Repl. Vol. 2004 & Cum. Supp. 2007).

146. *Id.* § 19.2-70.1 (Repl. Vol. 2004). The statute provides specific regulations for when a court order will be issued in section 19.2-70.2. *Id.* § 19.2-70.2 (Cum. Supp. 2007).

147. *See id.* § 19.2-70.1 (Repl. Vol. 2004).

stance, in *Harmon v. Commonwealth*, the telephone company, at the customer's request, attached a pen register to the phone line where they were receiving obscene telephone calls.<sup>148</sup> The company took this action without police involvement.<sup>149</sup> The Supreme Court of Virginia upheld the trial court's admission of the evidence from the pen register.<sup>150</sup>

The Virginia wiretap laws, like the VCCA, create civil liability for perpetrators.<sup>151</sup> People whose communications are used or disclosed unlawfully in violation of the Act can recover both compensatory and punitive damages, as well as attorney's fees.<sup>152</sup> An oral communication, however, is protected where the speaker expects the conversation not to be intercepted and the circumstances justify that belief.<sup>153</sup> The contents of an intercepted communication and the evidence derived from those communications (both wire and oral) are subject to suppression in both criminal and civil cases.<sup>154</sup>

## VII. FEDERAL LESSONS

The revised Federal Rules of Civil Procedure may give some guidance in the treatment of electronic discovery requests. The Federal Rules address the emerging role of electronic data in the discovery process by recognizing that "electronic information must be treated on equal footing with paper documents."<sup>155</sup> Federal Rule of Civil Procedure 34(a) now specifically includes "electronically stored information" as discoverable material in a request for production of documents.<sup>156</sup> The revised Federal Rules now require that if a request for electronically stored information

---

148. 209 Va. 574, 575–76, 166 S.E.2d 232, 233 (1969). *Harmon* dealt with application of a federal statute that was substantively similar to Virginia law as to the wiretapping issue. For example, see 47 U.S.C. § 605 (2000).

149. *Harmon*, 209 Va. at 577, 166 S.E.2d at 234–35.

150. *Id.* at 579, 166 S.E.2d at 235.

151. VA. CODE ANN. § 19.2-69 (Repl. Vol. 2004).

152. *Id.* § 19.2-69(1)–(3) (Repl. Vol. 2004).

153. See *Wilks v. Commonwealth*, 217 Va. 885, 889, 234 S.E.2d 250, 252.

154. See VA. CODE ANN. § 19.2-65 (Repl. Vol. 2004). As has been demonstrated in other jurisdictions, however, information stored on a computer may not be subject to suppression. See *White v. White*, 781 A.2d 85, 87 (N.J. Super. Ct. Ch. Div. 2001).

155. Jason Krause, *E-Discovery Gets Real*, 93 A.B.A. J., Feb. 2007, at 44, 46.

156. FED. R. CIV. P. 34(a). *But cf.* VA. SUP. CT. R. 4:9(a) (no provision for "electronically stored information").

does not specify the form for production, the information is to be produced in the form ordinarily maintained or the form reasonably useable.<sup>157</sup> Additionally, the Federal Rules do not require production in more than one form.<sup>158</sup> The importance of electronic data and the possibility of its unprecedented volume is therefore apparent throughout the pretrial process.

If the Commonwealth adopted similar language regarding the production of electronic databases along with electronic documents themselves, issues such as those addressed in *Malone* could easily be resolved.<sup>159</sup> Federal Rule of Civil Procedure 26(b) was also amended to excuse a party from producing discoverable electronic data if it is not “reasonably accessible because of undue burden or cost.”<sup>160</sup> The burden remains on the producing party to make the required showing.<sup>161</sup>

In perhaps the most widely known federal case regarding electronic discovery issues, *Zubulake v. USB Warburg LLC*, the defendant failed to take the necessary steps to ensure that discoverable electronic data was preserved by failing to communicate the litigation hold to all relevant parties.<sup>162</sup> As a result, the production of electronic information was unacceptably delayed and relevant information was destroyed.<sup>163</sup>

Before the Federal Rules were amended, the *Zubulake* court developed a methodical approach (to apply to federal and state litigation) to assess the cost of electronic discovery and to consider if cost shifting is appropriate.<sup>164</sup> In an earlier decision within the *Zubulake* series of cases, the court developed a seven-factor cost-shifting test regarding electronic discovery disputes.<sup>165</sup> Electronic

---

157. FED. R. CIV. P. 34(b)(ii).

158. FED. R. CIV. P. 34(b)(iii). *But cf.* VA. SUP. CT. R. 4:9(b).

159. *See supra* notes 65–66 and accompanying text.

160. FED. R. CIV. P. 26(b)(2)(B); *cf.* VA. SUP. CT. R. 4:1.

161. FED. R. CIV. P. 26(b)(2)(B).

162. 229 F.R.D. 422, 424 (S.D.N.Y. 2004).

163. *Id.*

164. *Id.*

165. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 322 (S.D.N.Y. 2003). The seven factors were:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
- 6.

data can be an amorphous concept, particularly within a business setting where employees generate numerous e-mails, instant messages, and other bits of data as part of their daily activities.<sup>166</sup> Given the vast amounts of electronic data that can be accumulated at both a personal and corporate level, the costs associated with discovery of electronic data in both federal and state litigation can be immense.

The beauty of the new federal system is that even given the unprecedented scale of information stored electronically, the unique impact of electronic data on the discovery process can be managed from the beginning through increased interaction between and disclosure by the parties.<sup>167</sup> Complex issues can be addressed once initial disclosures are made and the parties can rely on the new rules rather than case-by-case decisions on electronic discovery issues.<sup>168</sup> The already robust Virginia common law that has emerged regarding electronic discovery could be greatly enhanced if the Supreme Court of Virginia chose to adopt the amended federal rules.

Lastly, court rules should give clear guidance to the litigants as to what is expected and the consequences of a failure to meet expressed expectations. In the nascent area of the law described in this article, no clearer statement respecting the handling of electronic data in the litigation process is to be found than the following:

[C]ounsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced. In particular, once the duty to preserve attaches, counsel must identify sources of discoverable information . . . when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored. Counsel must also call for employees to produce copies of relevant electronic evidence, and must arrange for the segregation and safeguarding of any archival media . . . that the party has a duty to preserve.

---

The importance of the issues at stake in the litigation; and 7. The relative benefits to the parties of obtaining the information.

*Id.*

166. See Krause, *supra* note 155.

167. See *id.*

168. See *id.*

Once counsel takes these steps (or once a court order is in place), a party is fully on notice of its discovery obligations. If a party acts contrary to counsel's instructions or to a court's order, it acts at its own peril.<sup>169</sup>

### VIII. CONCLUSION

Creativity, advocacy, and a respect for precedent have been the guiding lights for the practice of law ever since man came to realize that disputes could be settled in peace. Sometimes these precepts come in conflict. Lawyers and judges will always be challenged to develop new strategies to address novel substantive and procedural issues arising out of the application of the law to emerging technologies. Courts and legislative bodies must continue to determine whether the traditional rules of the adversary process are capable of affording a fair, prompt, and efficient resolution to situations implicating the use of computers, cell phones, pagers, the Internet, iPods, and a host of electronic media.

The Internet has become a personal companion, a home for public debate, a marketplace, a bank, and a library. It offers access to millions of possible readers. Electronic devices have an impact on every aspect of our daily lives—both business and pleasure. What paper was to thousands of years of recorded history, the computer chip is to the future. Virginia has been a leader in the advancement and use of these new technologies and has managed successfully to apply fundamental concepts of law to new technology without compromising judicial values or allowing the new technology to fundamentally change the system. It is the goal of this article to demonstrate to the practitioner that electronic data and other emerging technologies are nothing to be feared.

Electronic data is just that—data. How that data is used is not solely dependent on technology but also on the moral, legal, and ethical standards that benefit from *stare decisis* and contemporary social thought.

A common law and statutory framework already exists in the Commonwealth to allow for successful litigation strategies that take advantage of the benefits of electronic data. Time-tested le-

---

169. *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 439 (S.D.N.Y. 2004).

gal theories and ethical standards equip practitioners and jurists alike to maintain a principled approach to the practice of law even when technological innovation changes the form of information.