NO, DON'T IM ME—INSTANT MESSAGING, AUTHENTICATION, AND THE BEST EVIDENCE RULE

Andrew M. Grossman[*]

INTRODUCTION

You are defending a client who stands charged with importuning a 14-year old (really a police detective). The crime took place during an instant message conversation, and the only evidence of the crime is an instant message log that the prosecutors would like to admit into evidence. In the log, "Craig478" engages in a conversation with "Nghty14er" that includes references to explicit sexual acts, some mutual fantasizing, and discussion of experience that "Craig478" has had with other minors. Towards the end of the conversation, "Craig478" supplies "Nghty14er" with a phone number, which matches your client's. As well, your client's name is Craig. Has the prosecution provided enough evidence for a prima facie showing of authentication?

According to most of the case law to date, it probably has.[1] As a defense attorney, you worry that this evidence will be unduly prejudicial. Your client denies that he is "Craig478" but has no evidence as to the actual identity of "Craig478" either. Will his denial, combined with a few character witnesses' testimony, effectively rebut the explicit language and graphic depictions of sexual acts in the printed instant message log that the jury will receive? It seems unlikely.

Perhaps your client admits to being "Craig478" but denies that the conversation proceeded as in the proffered log. "Nghty14er" kept trying to steer their chat towards prurient matters, your client tells you, while he was just searching for friends for his solipsist daughter. In addition to sexual innuendo, the chat log is rife with misspellings that are consistently identical in both halves of the conversation. Moreover, the formatting is off, with extra lines now and again, and the capitalization of the users' handles is inconsistent. Tampering is evident, but will it bar admission of the log—

[*] The Heritage Foundation, Senior Writer; George Mason University School of Law, Juris Doctor Candidate, May 2008; Fels School of Government, University of Pennsylvania, Masters Candidate; Dartmouth College, B.A., Anthropology and Economics, May 2002. This Comment received the 2006 Adrian S. Fisher Award for best student article at George Mason University School of Law.

[1] *See* discussion *infra* Part III.A.

and the unjust prejudice it is certain to cause? Under present law, almost certainly not.

In an e-mail conversation, a party exchanges messages with a person who is likely known to him personally or whose identity is likely to be known to the owner or operator of his e-mail server, such as a school or business. In a telephone conversation, a party may be identified by his voice or locution, and there is the presumption that a party who picks up the phone and identifies himself as the person listed at that number in the phone book is indeed that person.[2] With instant messaging, the human sense of identification can be just as strong as with an e-mail or a telephone call, even when it is, in actuality, an illusion.[3] Parties use handles,[4] as is done on CB radio, and relatively few pay for instant messaging, meaning that there is no trail of billing data to establish identity. Anyone can create an instant messaging account, providing little or no personally identifying information in the process, and people conversing by instant message frequently meet online in chat rooms or on message boards.[5] Thus, connecting the identity of an online friend to that of a prosecutable human being can be difficult.

With the rising popularity of instant messaging, along with the feeling of anonymity that it provides those who would use it for criminal purposes and its concomitant use in law-enforcement stings and by online vigilantes,[6] courts will increasingly face the issue of the admissibility of instant message evidence. Of the 225 or so federal and state cases that have involved instant messaging (and related technologies) evidence, 167 were decided within the last three years.[7]

Even though the Federal Rules of Evidence, and the state evidence codes modeled on it, were drafted long before popular use of instant messaging, the codified authentication and Best Evidence rules provide a reasonable framework for assessing the reliability of proffered instant message evidence. Judges no doubt have a strong working knowledge of the Rules, but they may know less about instant messaging and therefore may make unwarranted assumptions when applying the Rules to proffered instant messaging evidence, as has already happened in several cases. This Comment is an attempt to remedy that problem.

2 FED. R. EVID. 901(b)(6).

3 *See infra* Part I.B.

4 *See infra* Part I.B.

5 *See infra* Part I.B.

6 *See, e.g.,* Perverted-Justice.com—The Largest and Best Anti-Predator Organization Online, http://www.perverted-justice.com (last visited May 1, 2006).

7 Search performed on Westlaw's ALLCASES database on April 23, 2006.

Both the nature of the technology in question and the law of evidence are relevant to this effort. Section I of this Comment outlines the use and technology of instant messaging, which turns out to be very heterogeneous though not especially complex. Section II looks at the traditional methods of satisfying the authentication and Best Evidence requirements. Section III analyzes the cases that have considered how the law applies to evidentiary issues raised by instant messaging. Finally, Section IV considers how judges may express the appropriate skepticism due instant messaging evidence within the framework of the Rules.

I. INSTANT MESSAGING

A. *Generally*

"Instant messaging" describes generally the class of services that allows users of computers, data-enabled cellular phones, and other electronic devices to send one another text messages (and sometimes audio and video messages) instantaneously.[8] Initially popular among children and teens, instant messaging usage has spread in recent years to include more adults, most large businesses, and many government agencies.[9] Where proficiency at e-mail was once a sign of computer literacy, adeptness at instant messaging is now the new threshold.[10]

Today, the top five instant messaging services have nearly 170 million active users among them, and many more users are scattered among smaller and in-house services.[11] Over 50% of workers use instant messaging software;[12] among companies that do not provide instant messaging software, employees of 70% of them will use it anyway, without official sanction or support.[13] According to a recent survey, U.S. Internet users between twelve

---

8 *See generally* Instant Messaging, http://en.wikipedia.org/w/index.php?title=Instant_messaging&oldid=28227880 (last visited May 1, 2006) [hereinafter Instant Messaging].

9 *See US Teens Prefer IM to E-mail*, INTERNET BUSINESS NEWS, July 28, 2005, http://findarticles.com/p/articles/mi_m0BNG/is_2005_July_28/ai_n14838097; Press Release, Followap Telecommunications, Instant Messaging—Useful, Convenient, Faster Decision Making (Nov. 3, 2005), http://www.followap.com/Index.asp?CategoryID=107&ArticleID=60 [hereinafter Followap Press Release].

10 *See* Debra D'Agostino, *Instant Messaging: IM Here to Stay*, CIO INSIGHT, Apr. 2004, http://www.cioinsight.com/article2/0,1397,1570390,00.asp.

11 *See* Instant Messaging, *supra* note 8.

12 Followap Press Release, *supra* note 9.

13 *The Numbers: April 2003*, CIO INSIGHT, Apr. 2003, at 18.

and seventeen years of age prefer instant messaging to e-mail;[14] 75% admitted to using instant messaging software for at least two hours per day.[15] According to the survey, teenagers "[feel] that e-mail is for older people."[16] Meanwhile, 42% of older people use instant messaging software regularly.[17]

As services from different periods in the evolution of instant messaging coexist today, some discussion of the medium's history is warranted.[18] As early as the late 1960s, users of time-shared computers were often able to converse with one another,[19] and by the late 1970s, users of UNIX and VAX servers could converse with one another using programs like the UNIX operating system's "talk" command.[20] By the late 1980s, the spread of the Internet had connected more and more sites.[21] Internet Relay Chat ("IRC"), which allows group chat and personal messaging, was developed in 1988 and quickly became popular.[22] It is still in use today.

In 1996, Mirabilis introduced its ICQ (phonetically, "I seek you") service and software,[23] generally regarded as the first modern instant messaging client.[24] ICQ racked up 850,000 users in its first six months, and the service was purchased by America Online ("AOL") in 1998 for $287 million.[25]

What ICQ brought to messaging has a special relevance to those concerned about evidentiary matters. First, it worked on the general Internet rather than on a closed, easier to monitor network, broadening the number of people with whom one could converse. Second, ICQ integrated a simple system for allowing users to establish "virtual presence" based on nick-

14 *US Teens Prefer IM to E-mail*, *supra* note 9.

15 *Id*.

16 *Id*.

17 *Id*.

18 *See generally* Instant Messaging, *supra* note 8.

19 *See* David Woolley, PLATO: The Emergence of Online Community (1994), http://thinkofit.com/plato/dwplato.htm ("A few such programs existed on PLATO before 1973, but they did not get much use, probably because the user community was quite small and most terminals were still in a single building.").

20 *See* talkd Source Code, http://www.tmk.com/ftp/multinet-contributed-software/ntalk/talkd/talkd.c (last visited May 1, 2006) (noting that a non-original version is "Copyright (c) 1983 Regents of the University of California").

21 *See* Robert Zakon, Hobbes' Internet Timeline v8.1, http://www.zakon.org/robert/internet/timeline/ (last visited May 1, 2006).

22 Robin Hamman, History of the Internet, WWW, IRC, and MUDs, http://www.socio.demon.co.uk/history.html (last visited May 1, 2006).

23 ICQ Inc., The ICQ Story, http://www.icq.com/info/icqstory.html (last visited May 1, 2006).

24 Instant Messaging, *supra* note 8 ("ICQ was the first general instant messenger combining presence . . . with the ability to send messages.").

25 The ICQ Story, *supra* note 23; ICQ, http://en.wikipedia.org/wiki/ICQ (last visited May 1, 2006).

names rather than on their computers' IP addresses or their e-mail addresses.[26] With just a simple nickname, a user could add a friend or acquaintance to a "contact list" and then keep track of that contact's availability for conversation. Starting a conversation with a contact required only clicking their name in the list and typing a message. Pseudonymity has likely played a large role in ICQ's success; users can maintain a persistent handle—which they can give to friends and strangers alike—without revealing any personally identifying information at all.[27] One commentator writes that users experience e-mail "[a]s a medium allowing spontaneous and instantaneous communication without directly sensing the presence of one's interlocutor in the seeming privacy of one's own workstation" and that this aloofness "encourage[s] people to let their guard down and communicate things they would otherwise never communicate."[28] The same is true of instant messaging, which can afford greater anonymity and even more spontaneity than e-mail.

Many instant messaging services employ a client-server architecture—that is, messages are transmitted from the user's client software to a centralized server operated by the service and then retransmitted to the recipient.[29] In theory, these services could log all messages that pass through them; in practice, they do not. Several services use their servers only for addressing purposes: a user's client software contacts the server once per conversation to obtain the Internet address of the recipient's computer but then sends the actual message directly to the recipient.[30] A few experimental instant messaging platforms dispense with the need for servers altogether, relying on peer-to-peer communication techniques to spread addressing information.[31]

---

26 Instant Messaging, *supra* note 8.

27 Pseudonymity is persistent but anonymous identity. On AOL Instant Messenger, for example, a handle is likely to always identify the same person; tying that handle to identity is more difficult. *See infra* Part I.B.

28 Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation*, 29 RUTGERS COMPUTER & TECH. L.J. 219, 223 (2003).

29 *See, e.g.,* Overview of MSN Messenger Protocol, http://www.hypothetic.org/docs/msn/general/overview.php (last visited May 1, 2006) ("Directly connected conversations between principals are not used in MSN Messenger, and the switchboard [server] acts as a proxy between you and those you are chatting with.").

30 *See, e.g.,* Microsoft Online Privacy Statement, Messenger Supplement, http://privacy.microsoft.com/en-us/messenger.aspx (last visited May 1, 2006) (explaining that a user's IP address "will be shared" with other users "in cases involving a peer-to-peer communication"); *see also* ICQ Inc., Protect Your IP Address From Unnecessary Exposure, http://www.icq.com/support/security/ipprivacy.html (last visited May 1, 2006) ("Some of the communications on ICQ are conducted by Direct Connections (peer-to-peer), thus exposing IP addresses.").

31 Skype uses this mechanism. *See* Salman A. Baset & Henning Schulzrinne, An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, http://arxiv.org/pdf/cs.NI/0412017 (last visited May 1, 2006) (describing the results of a series of experiments to reverse engineer the Skype addressing and

While textual communication seems to remain dominant, many instant messaging services allow users to communicate by voice and video and to send one another arbitrary files. For at least one popular instant messaging service—Skype—voice communication is the norm.[32]

B. *Identifying Users*

How does an instant message service keep track of its users' handles? Practice varies considerably, with only one constant: all services prevent two different people from using the same handle at once. Most services prevent collisions over an extended period of time (e.g., a handle-user link persists until the user cancels his account, at which point another user could take over that handle), whereas others do not allow extended registration of handles (i.e., when a user disconnects from the service, the handle he was using becomes available to others).

Authentication practices that link a handle to information that identifies a user run the gamut. At one end of the spectrum, IRC, which allows group chat and person-to-person messaging, requires only that a user choose a handle—no other information is required. At the other, the highly secure and auditable instant messaging systems employed by financial services firms may link a handle to other employment records that definitively identify a specific individual.

The most popular instant messaging services require little in the way of authentication, though they do request information. Neither Yahoo! Messenger nor MSN Messenger requires a user to submit any information that cannot be easily falsified. Still, when an account on one of these services is created for legitimate purposes, this information may have some value. AOL Instant Messenger requires a user to submit an e-mail address to create an account but does not confirm that address in any way.[33] To create a Google Talk account requires a mobile phone, to which the service will send an SMS message containing a required invitation code, though the phone need not belong to the person creating the account. ICQ requires a user to submit an e-mail address and access a Web URL sent in an e-mail

communications protocols).

32 Skype is primarily used for one-on-one voice communication, both over the Internet and through the regular telephone system. The service also offers textual instant messaging and, just recently, videoconferencing. Like other services' client software, while the Skype client can save a transcript of textual instant messages, it cannot record audio or video messages.

33 It will accept, for example, an e-mail address that was created as part of the sign-up process for MSN Messenger or Yahoo! Messenger.

to that address, thus verifying that e-mail address if not the identity of the person behind it.[34]

A few services require stronger authentication. Many users access AOL Instant Messenger using America Online's dial-up and broadband services. Linked to their handles, then, is their billing information, including name, billing address, and telephone number. Businesses that deploy instant messaging systems can assign handles and passwords just as they assign access to other network services, providing a strong link between an instant messaging account and a particular person.[35]

With the exception of IRC and other services, many of them Web-based,[36] that do not maintain persistent user accounts, instant messaging services require their users to log in with a handle and password. Accounts can be compromised when, for example, a user shares his password with others, when a password is intercepted as it travels through an insecure medium like e-mail, or when an imposter has direct access to a user's computer. As with other forms of communication, efficient use of the medium requires a strong presumption that accounts are rarely compromised and that account holders and their guests are the ones using their accounts. The log-in processes employed by some businesses, such as requiring strong passwords or biometric information like fingerprints,[37] further strengthen this presumption when they are present.

Despite the weak authentication processes that most instant messaging services have employed, nearly all have access to their users' network addresses when those users are connected,[38] and they tend to archive this information.[39] A computer connected to the Internet is assigned an IP address,

---

34 Again, an e-mail address obtained with falsified personal information may be used.

35 *See, e.g.*, Microsoft® Office Live Communications Server 2005 with Service Pack 1 Feature Guide 5, http://download.microsoft.com/download/e/f/3/ef30c672-fe79-4096-a7ae-45a933e6f266/Live CommGuide.doc (last visited May 1, 2006) (Microsoft's Live Communications Server 2005 can provide "Kerberos, NT LAN Manager (NTML) authentication.").

36 *See* List of Web Chat Services, http://dir.yahoo.com/Computers_and_Internet/Internet/World_Wide_Web/Chat/ (last visited May 1, 2006).

37 Jessica Pallay, *A Brave New World*, FIN. TECH, July 17, 2003, http://www.financetech.com/featured/showArticle.jhtml?articleID=14702284 ("Bloomberg terminals will soon require a fingerprint for access . . . .").

38 The exceptions are those services that use peer-to-peer techniques to keep track of addressing—which for now is just Skype. Skype claims not to store users' IP addresses. Skype Privacy Statement, http://www.skype.com/company/legal/privacy/privacy_general.html (last visited May 1, 2006) ("Passive Information is automatically generated and is not stored centrally.").

39 *See* Yahoo! Privacy Policy: IP Addresses, http://privacy.yahoo.com/privacy/us/ip/details.html (last visited May 1, 2006) [hereinafter Yahoo! Privacy Policy] (stating that Yahoo! stores users' IP addresses); America Online, AIM Privacy Policy, http://www.aim.com/tos/privacy_policy.adp (last visited May 1, 2006) (stating that AOL Instant Messenger service will gather users' IP addresses); Microsoft Online Privacy Statement, http://privacy2.msn.com/en-us/fullnotice.aspx (last visited May 1,

which can uniquely identify that computer at least for the time that it is connected.[40] Entities that provide Internet access, such as Internet Service Providers ("ISPs") and universities, typically keep records of their users' Internet connections that allow an IP address to be matched with a user's ISP account and the account information, such as billing data, that goes along with it.[41] Users of instant messaging services that allow computers to exchange information directly can determine the IP addresses of their conversation partners directly,[42] though actually accomplishing this may require technical skills that average users are unlikely to have.[43]

IP addresses and the like are not infallible. First, many computers access the Internet from behind proxy servers,[44] which conduct network transactions on a computer's behalf. In this case, an instant messaging service would log only the proxy's address and not that of the computer on which the instant messaging client software is actually running. While proxy operators may maintain logs themselves or the proxies may allow sufficient authentication (such as when a proxy is located in a user's own home, as is common with wireless Internet connections), proxies can also facilitate strong anonymity. Operators of "open proxies"[45] and "anonymous

2006) ("We also collect certain standard information . . . such as your IP address.").

40 Rus Shuler, How Does the Internet Work? § 2, http://www.theshulers.com/whitepapers/internet_whitepaper.html (last visited May 1, 2006).

41 *See, e.g.,* United States v. Campos, 221 F.3d 1143, 1146 (10th Cir. 2000) ("Alissa Simon, an employee with AOL, testified that the credit card on the AOL account belonged to Mr. Campos . . . ."); United States v. Lamb, 945 F. Supp. 441, 446 (N.D.N.Y. 1996) (describing subpoena to America Online to obtain billing information of child pornography distributor; also, the first mention of instant messaging in reported U.S. case); State v. Bell, No. 2004-CA-5, 2005 WL 388174, ¶ 68 (Ohio Ct. App. Feb. 18, 2005).

42 *See, e.g.*, Yahoo! Privacy Policy, *supra* note 39 ("Messenger sometimes uses a peer-to-peer connection during its operation . . . . Peer-to-peer means that your computer connects directly to the other user's computer in the conversation without needing to go through Yahoo! servers. As such, your IP address is available to users you share a peer-to-peer connection with.").

43 One exception to this general rule is ICQ's client software. ICQ Inc., The ICQ Privacy Policy, http://www.icq.com/legal/privacy_previous.html (last visited May 1, 2006) (A version of the privacy policy in effect for six years helpfully advised, "[Y]ou can try to find the last IP address (including dynamic IP address) of any [abusive] user on your contact list by 'right clicking' the user's name field . . . ."). While the current ICQ privacy policy does not contain this hint, the software continues to offer this functionality.

44 Many computers also access the Internet through Network Address Translation (NAT) boxes, which, for the purposes of this article, function as proxies. *See* Grenville J. Armitage, Inferring the Extent of Network Address Port Translation at Public/Private Internet Boundaries 1 (2002), http://www.caia.swin.edu.au/reports/020712A/CAIA-TR-020712A.pdf (estimating that NAT may account for 17 to 25 percent of the computers on the Internet).

45 Free Proxy vpn Socks and Anonymity Browsing, http://sockss.blogspot.com/2005_06_01_sockss_archive.html (June 9, 2005) ("An open Proxy generally exists because a System Administrator

proxies" make a point of not maintaining connection records and sometimes even route network traffic through several proxies to obscure the source of communications further and filter out possibly identifying information, such as network headers and e-mail addresses.[46] Other proxies, such as those connected to publicly accessible wireless networks, afford inherent anonymity—computers that connect to them are generally unidentifiable.[47] Finally, as has been widely reported, some recent computer viruses turn infected computers into proxies that can be used by those behind the viruses.[48] Only with laborious investigation and luck can traffic sent from such compromised computers be traced back to a source computer.[49]

C. *Logging*

Outside of the corporate environment, where servers may log all conversations,[50] instant message logging is dependent on a user's client software rather than the instant messaging service. Some clients log all conversations, while others require a user to activate logging. While many will record timestamps for messages, few record other metadata that may be available, such as participants' IP addresses; non-text data, such as images, audio, video, and file transfers, are usually not recorded either. All instant message clients, even those without logging features, allow a text conversation to be copied and then pasted into another application, such as a word

---

or home user has incorrectly setup a Proxy Server on their computer . . . . The reason it is desirable to use an Anonymous Proxy . . . is that you can garauntee (sic) the Proxies are infact (sic) Anonymous, which means less rechecking for you. An Anonymous Proxy itself is of great advantage since it stops the target computer from knowing what your IP is, and therefore in the larger scheme of things, hides you online.").

46 *See, e.g.*, Anonymizer Service, http://anonymizer.com/ (last visited May 1, 2006).

47 *See* Seth Schiesel, *Growth of Wireless Internet Opens New Path for Thieves*, N.Y. TIMES, Mar. 19, 2005, at A10. ("The No.1 challenge is that people are committing all sorts of criminal activity over the Internet using wireless, and it could trace back to somebody else.").

48 GFI Inc., The Corporate Threat Posed by E-mail Trojans: Proxy Trojans 4, www.gfi.com/whitepapers/network-protection-against-trojans.pdf (last visited May 1, 2006) ("These Trojans turn the victim's computer into a proxy server . . . . This gives the attacker complete anonymity and the opportunity to do everything from YOUR computer . . . however, the trail leads back to you not to the attacker . . . .").

49 *See, e.g.*, Evan Ratliff, *The Zombie Hunters*, NEW YORKER, Oct. 10, 2005, at 44 (describing the difficulty in hunting down "cyberextortionists" who used open proxies to flood businesses' sites with disabling traffic).

50 National Association of Securities Dealers, Notice to Members: Instant Messaging 345, July 2003, http://www.nasd.com/stellent/groups/rules_regs/documents/notice_to_members/nasdw_003249.pdf ("Members must also ensure that their use of instant messaging complies with applicable SEC and NASD recordkeeping requirements.").

processor, text editor, or e-mail program. This latter capability has been used to record evidence in several court cases.[51]

Typically, instant message logs are stored as plain text files or "marked-up" text files (text files interspersed with formatting commands). "[S]uch logs," according to one court's summary of testimony by an expert from America Online, "are stored on the user's computer (not an America Online computer) in basic text documents that anyone with a modicum of computer experience can modify at will."[52] Such modification, if it does not disturb the basic formatting or continuity of the log, is extremely difficult or impossible to detect.[53] Log files may be time-stamped by the operating system at the time of creation and the time of the most recent modification. These stamps are also easily modified and may have little probative value even if unchanged by a user (e.g., some backup software will update a file's timestamp automatically).[54]

Some client software stores logs as binary files that are more difficult to modify and may include information ignored by other log formats, such as images.[55]

Beyond instant messaging clients, a variety of add-on software can be used to create, search, and sometimes modify instant messaging logs. In addition, one commentator has suggested that those creating logs for use in subsequent prosecution or litigation should videotape the computer's screen.[56] Video recording of this sort would certainly be more difficult to modify than most log files and could also give the finder of fact a better sense of the conversation's flow. Thinking along similar lines, at least one police department has used screen-capture software to record, in video

51 *See, e.g.*, People v. Von Gunten, No. C035261, 2002 WL 501612, at *4 (Cal. Ct. App. Apr. 4, 2002); Adams v. State, 117 P.3d 1210, 1218 (Wyo. 2005).

52 Slattery v. United States, No. 2:98CR125-B, 2005 WL 2416339, at *6 (N.D. Miss. Sept. 30, 2005).

53 Depending on how a modified file is recorded to disk, the modification may be possible to detect. Using computer forensic analysis tools, a technician could search out previous versions of the file, if the editor used did not modify old versions directly, and compare these to the version proffered. This process is time consuming and difficult. *See* David Dittrich, Basic Steps in Forensic Analysis of Unix Systems, http://staff.washington.edu/dittrich/misc/forensics/ (last visited May 1, 2006).

54 *But see* People v. Hawkins, 121 Cal. Rptr. 2d 627, 641-43 (Cal. Ct. App. 2002).

55 The software "PowerTools Professional for AOL," which is capable of such recording, was mentioned in one case. *See* United States v. Weisser, 417 F.3d 336, 343 n.3 (2d Cir. 2005), *cert. denied*, 126 S. Ct. 505 (2005); PowerTools Professional for AOL Product Information Page, http://www.bpssoft.com/PowerTools/index.htm (last visited May 1, 2006).

56 J. Allan Cobb, *Evidentiary Issues Concerning Online "Sting" Operations: A Hypothetical-Based Analysis Regarding Authentication, Identification, and Admissibility of Online Conversations- A Novel Test for the Application of Old Rules to New Crimes*, 39 BRANDEIS L. J. 785, 832 (2001).

form, the conversation in an instant message window.[57] This evidence, however, was excluded for other policy reasons.[58]

II. BUILDING A FOUNDATION FOR ADMISSION

Before any evidence can be admitted or any non-collateral matter testified to, the proponent of that evidence must build a foundation for its admission. Under the Federal Rules of Evidence, this consists of making a prima facie showing of authenticity—that is, that the evidence is what it purports to be—and perhaps also showing that the evidence satisfies the "Best Evidence" rule, which is applicable to "writings and recordings." The proponent must also show that the evidence is relevant, subject to the balancing test against undue prejudicial effect in Rule 403.

A. *Authentication*

Authentication concerns the relationship of proffered evidence to an actual person, often a party in the case. Authenticity must be addressed for all "matters" raised and is said to speak directly to relevance: evidence that is not arguably relevant has no weight and is therefore irrelevant.[59] Issues of authentication turn on the standard of proof necessary to prove the relationship. For example, if a party seeks to admit a document that it claims is a contract, it must offer more than that bare assertion but far less than proof that the document is indeed authentic, which is ultimately a question for the finder of fact that goes to the weight of the evidence.[60] Rather, it must present to the judge, under the Federal Rules, "evidence sufficient to support a finding that the matter in question is what [the party] claims."[61] This procedure, then, is governed by Rule 104(b), which authorizes the judge to make "a preliminary determination whether the foundation evidence is sufficient to support a finding of fulfillment of the condition." If the judge believes this standard has not been met, the evidence is withdrawn.

---

57 State v. MacMillan, 872 A.2d 1031, 1034 (N.H. 2005) (noting that the officer used "Camtasia" software, which records a computer's screen display into a video file).

58 The lower court held that the recording violated New Hampshire's wiretapping statute, and the State did not appeal the issue. 872 A.2d at 1035-36.

59 FED. R. EVID. 901(a) advisory committee's note ("Authentication and identification represent a special aspect of relevancy.").

60 As Wigmore puts it, "[A] writing purporting to be of a certain authorship cannot go to the jury as possibly genuine, merely on the strength of this purport; *there must be some evidence of the genuineness* (or execution) of it . . . ." 7 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2130 (Chadbourn rev. 1978).

61 FED. R. EVID. 901(a).

The trial court has a great degree of discretion in deciding authenticity, being subject only to abuse of discretion review.[62] For documents, "an abuse of discretion will be found only where there is no competent evidence in the record to support a court's ruling; and then the trial court's decision will be reversed."[63] Even when questionable, then, authenticity decisions are unlikely to be reversed.

The purpose of requiring a prima facie showing of authenticity is to break the inevitable mental inference that a writing bearing a person's name or otherwise attributed to a person was necessarily written by that person. For non-inscribed chattels, "all can appreciate that this element is missing and must be supplied by evidence."[64] However, for documents purporting authorship in one way or another, "[t]here is a natural tendency to forget it,"[65] which could cause the finder of fact to give a document undue probative weight. Additionally, the rule may be justified by the weight given to tangible, written evidence over other forms[66] and by the desire to check fraud[67] and guard against innocent misidentification.[68]

Under Rule 902, certain types of documents are capable of "self-authentication." One commentator has suggested, relying on paragraph 7 of the Rule, that e-mail messages bearing a business's domain name as part of the alleged sender's e-mail address may qualify as self-authenticating "trade inscriptions."[69] Paragraphs 11 and 12, enacted in 2000, import the business-records exemption from the hearsay rules into the realm of authentication, allowing self-authentication of any document covered by Rule 803(6).[70]

If a piece of evidence is not self-authenticating, a party may make the required prima facie showing of authenticity with direct or circumstantial evidence. Rule 901(b) is a laundry list, "[b]y way of illustration only," of the means that parties may employ to meet this standard. Most directly, the author of a writing may admit to authorship, or a witness to the authoring may attest to it. For written or signed documents, a comparison of hand-

62 *See* Blain v. Commonwealth, 371 S.E.2d 838, 842 (Va. Ct. App. 1998) (explaining that "[t]he admissibility of evidence is within the broad discretion of the trial court, and a ruling will not be disturbed on appeal in the absence of an abuse of discretion").

63 Cobb, *supra* note 56, at 829.

64 7 WIGMORE, *supra* note 60, § 2130.

65 *Id*.

66 *Id*.

67 This impulse may be heightened in criminal cases. 2 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, EVIDENCE § 9.1 (3d ed. 2003).

68 *See* 2 MCCORMICK ON EVIDENCE § 218 (John W. Strong ed., practitioner ed. 1999).

69 Robins, *supra* note 28, at 240 & n.79.

70 FED. R. EVID. 902(11), (12).

writing may also serve as direct evidence. For recordings, similarly, voice identification may be employed.

Rule 901(b)(4) suggests that "distinctive characteristics," including a writing's contents and "circumstance," may provide authentication. "The content of a writing may reveal knowledge that is sufficiently distinctive to support a finding that it was authored by a particular individual who had such knowledge."[71] Wigmore suggests that this knowledge must be "peculiarly referable to a single person,"[72] but more recent commentators argue that it should be sufficient to show that "of the small group of persons having such knowledge[,] the person claimed to be the author is the one most likely to have prepared the writing in question."[73] This disagreement bears heavily on the authentication of evidentiary media that resist direct proof of authorship.

Rule 901(b)(4) incorporates a specific instance of the "distinctive characteristics" doctrine: the common-law "reply doctrine," under which a writing in response to a communication is authenticated if it is responsive to the earlier communication and is received without unusual delay.[74] No mere technical rule, the reply doctrine depends upon the reliability of the mails; the assumption, usually warranted, that mail addressed to an individual is likely to reach that individual only; and the responsiveness of the reply. [75]

The judge will admit evidence that is self-authenticating or that for which prima facie evidence of authentication has been presented. The opposing party may then present additional evidence rebutting the authenticity of the admitted evidence, and the ultimate question of authenticity, as it bears on the weight accorded a piece of evidence in proving an ultimate fact, is determined by the trier of fact.

B. *Best Evidence*

The "Best Evidence" rule, implemented in Rules 1002 through 1008 of the Federal Code, expresses a preference for original writings and recordings over lesser evidence of the contents of those writings and recordings, such as testimony. This rule is arguably intended to prevent fraud[76] and to ensure the accuracy of written documents, which nowadays "is of

71 MUELLER & KIRKPATRICK, *supra* note 67, § 9.8.

72 7 WIGMORE, *supra* note 60, § 2148.

73 MUELLER & KIRKPATRICK, *supra* note 67, § 9.8.

74 *See* MCCORMICK, *supra* note 68, § 225.

75 *Id*.

76 *Id*. § 231. *But see* 4 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW §1180 (Chadbourn rev. 1978).

more than average importance."[77] Some have questioned the need for the rule in recent years, given the capabilities of modern duplicative technologies[78] and expanded discovery processes,[79] while others have suggested that the expanding capabilities of computers, particularly their ability to modify evidence, may lead to a renaissance for the rule,[80] if not necessarily in its current codified form.

To prove the content of an original, "the original writing, recording, or photograph is required,"[81] but there are numerous exceptions.[82] Duplicates, for example, are admissible so long as no "genuine question is raised as to the authenticity of the original."[83] If the original has been destroyed (but not by the proponent of the evidence acting in bad faith) or is unobtainable, other evidence of the contents of the original may be admitted.[84] Thus, the "rule" of Best Evidence really is one of preference that will rarely, if ever, bar a party acting in good faith from admitting evidence.[85]

It can be difficult to discern an "original," though, when a document is created on a computer and consists physically of an ephemeral pattern of electrons and photons. Rule 1001(3) defines "any printout or other output readable by sight, shown to reflect the data accurately," to be an "original." The Advisory Committee's comment on this section, however, allows that "in some instances particularized definition is required," which may be based upon "practicality and common usage."[86] One commentator, writing on the admissibility of e-mail messages, concluded that the Best Evidence rule would never bar the admission of e-mail messages.[87] "Since electronic mail is technically data stored on a computer, courts will deem a printout of a message to be an 'original,' assuming it accurately reflects the information stored on a computer."[88] Whether that information accurately reflects

77 MCCORMICK, *supra* note 68, § 231.

78 *Id*. ("[T]here would appear little reason to apply the rule . . . to copies produced by modern copying techniques which virtually eliminate any possibility of mistransmission.").

79 MUELLER & KIRKPATRICK, *supra* note 67, § 10.1.

80 Jeffrey Parker, Professor of Law, Lecture on Best Evidence Rule (Nov. 8, 2005). *But see* CALIFORNIA LAW REVISION COMMISSION, RECOMMENDATION: BEST EVIDENCE RULE 373 (1996) (Recommending that the best evidence rule be scrapped due to recent "technological developments.").

81 FED. R. EVID. 1002.

82 *Id*.

83 FED. R. EVID. 1003.

84 FED. R. EVID. 1004.

85 *See* FED. R. EVID. 1004 advisory committee's note (The Best Evidence rule "has developed as a rule of preference: if failure to produce the original is satisfactorily explained, secondary evidence is admissible.").

86 FED. R. EVID. 1001(3) advisory committee's note.

87 Andrew Jablon, *God Mail: Authentication and Admissibility of Electronic Mail in Federal Courts*, 34 AM. CRIM. L. REV. 1387, 1401 (1997).

88 *Id*.

the information transmitted by the sender is, under this formulation, irrelevant.

That glib conclusion, however, overlooks the interaction of substantive law with the Best Evidence rule.[89] The creation of certain kinds of writings entails the creation of a second writing that may not be a duplicate. For example, when the contents of a writing sent by telegraph are sought to be proved, either the dispatch sent or the dispatch received could be the original writing. This is an issue of substantive law.[90] If the sender's intent to commit a crime, for example, is the ultimate fact to be proved, then the dispatch sent is the original; if the recipient's notice is the fact to be proved, then the dispatch received is the original.[91] Rule 1003, which concerns alleged duplicates, seems to allow this distinction.[92]

III. THE CASE LAW TO DATE

Though greatly simplified by the Federal Rules and the state evidence codes that parallel the Federal Rules, the law of authentication and Best Evidence in practice can be quite murky. There are several reasons for this. First, as Wigmore observes, a court's decision as to whether an adequate foundation has been laid can be so fact-specific that it "ordinarily does not result in abstract rules; each ruling stands by itself, and can form no precedent."[93] Second, the issues that arise from electronically transmitted documents can give rise to circumstances in which a literal reading of the Rules, combined with mistaken assumptions about technology, conflicts with the stated purposes of the Rules.[94] Thus, there are conflicting precedents with respect to instant message admissibility, as well as some troubling analyses and decisions. Many courts, confronted with electronic evidence, "[bypass] authentication requirements altogether" and focus solely on hearsay exceptions.[95]

---

89 MCCORMICK, *supra* note 68, § 235.

90 *Id*.; WIGMORE, *supra* note 60, § 1236(3)(a); MUELLER & KIRKPATRICK, *supra* note 67, at 1073-74. These sources provide numerous citations to the case law.

91 WIGMORE, *supra* note 60, § 1236(3)(a).

92 FED. R. EVID. 1003 ("A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original . . . .").

93 WIGMORE, *supra* note 60, § 2128.

94 For a discussion of the Best Evidence rule and its interaction with substantive law, *see supra* Part II.B.

95 J. Shane Givens, *The Admissibility of Electronic Evidence at Trial*, 34 CUMB. L. REV. 95, 106 (2003).

A. *Authentication*

The most clear-cut cases are those that rely upon direct evidence to satisfy the requirement of authentication. In *State v. Bell*, the defendant was convicted of importuning a 14-year-old girl (actually Detective Alonzo Wilson of the Xenia, Ohio, Police Department).[96] Importuning, as defined by a state statute, consists merely of enticing or urging an underage victim to engage in sexual activities, so the instant message conversation itself was the crime.[97] "WT309FD" and the victim engaged in conversation until "WT309FD," doubting that "Molly14Ohio" was indeed a 14-year-old girl, asked that she call his cellular phone and leave a message.[98] Detective Wilson enlisted a female colleague for this task.[99] When their conversation resumed, "WT309FD," pleased at his good fortune, exclaimed, "you are a female" and then proceeded to importune "Molly14Ohio."[100] Rather than determine the ownership of the cellular phone number to identify "WT309FD," which would have led to a reasonable application of the reply doctrine given the timing of the conversations, the police contacted America Online and requested billing information for the account.[101] Additionally, "WT309FD's" profile identified him by his first name and stated that he was a firefighter in Centerville, Ohio, and that town's fire department supplied the full name and address of the firefighter matching the statements made online.[102] The two addresses—from America Online and the fire department—matched.[103] The defendant argued that this evidence did not provide sufficient authentication, but the appeals court concluded that the evidence was sufficient to "permit reasonable minds to conclude that it was [the defendant] who had solicited sex from 'Molly14Ohio'" and therefore did not meet the abuse of discretion standard.[104]

Circumstantial evidence can also be used to similar effect in cases involving disputed instant message conversations. In *United States v. Simpson*, the defendant was convicted of receiving child pornography and appealed, citing as error that an Internet chat room conversation (essentially, instant messaging with multiple participants) that had been infiltrated and logged by a law-enforcement agent was not adequately authenticated.[105]

96 State v. Bell, No. 2004-CA-5, 2005 WL 388174, ¶¶ 1-2 (Ohio Ct. App. Feb. 18, 2005).

97 *Id.* ¶ 80.

98 *Id.* ¶¶ 51-60.

99 *Id.* ¶ 67.

100 *Id.*

101 *Id.* ¶ 68.

102 State v. Bell, 2005 WL 388174, ¶ 68.

103 *Id.*

104 *Id.* ¶¶ 89, 93.

105 United States v. Simpson, 152 F.3d 1241, 1244, 1249 (10th Cir. 1998).

The defendant's contention, based on a very literal reading of the Federal Rules, was that the government "could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice" and were thus not sufficiently authenticated.[106] The agent had exchanged names and addresses with a chat room participant, "Stavron," so that they could exchange child pornography by mail.[107] Police confirmed that the name "Stavron" had provided matched records for the residence at that street address.[108] Searching the premises, police seized a paper on which was written the agent's chat room identity and the name and address that he had provided to "Stavron."[109] The appeals court ruled that this was sufficient evidence to authenticate the chat room logs.[110] The circumstantial evidence in this case does narrow down the group of possible authors of a writing to a single individual.

The court in *People v. Von Gunten*, conversely, had to address circumstantial evidence reflecting knowledge that was not sufficiently limiting.[111] The defendant had been convicted of assaulting two young men with a baseball bat outside of a party.[112] On appeal, the defendant argued that the trial court had erred in excluding the testimony of a friend concerning instant messages she had received from a handle that she believed was held by one of the victims.[113] This friend had received the victim's handle, "BukaRoo20," from a mutual friend and added it to her instant messaging client's contact list.[114] Some time after the party and the assaults, she engaged in an instant message conversation with "BukaRoo20" in which he admitted to starting the fight, and she pasted the text of the conversation into a word processing program.[115] While the friend did state her belief, based on numerous instant message conversations over a period of weeks, that the account belonged to the victim, she was unable to offer any facts uniquely shared between her and the victim that would prove identification.[116] The appeals court cited several factors in affirming the lower court's finding of insufficient authentication. First, the prosecution presented no evidence, such as information from the instant messaging service, connecting the

106 *Id*. at 1249.
107 *Id*. at 1250.
108 *Id*.
109 *Id*.
110 *Id*.
111 People v. Von Gunten, No. C035261, 2002 WL 501612, at *6 (Cal. Ct. App. Apr. 4, 2002).
112 *Id*. at *1.
113 *Id*. at *1, *4.
114 *Id*. at *4.
115 *Id*. at *4, *5.
116 *Id*. at *5.

victim to the account.[117] Second, the witness did not obtain the account name from the victim directly;[118] whether, if she had, that would have been dispositive is unclear. Third, the account could have been created by anyone.[119] Fourth, the matters discussed in the instant message transcript were known within the circle of friends.[120] Thus, there was no direct evidence of authorship, and the circumstantial evidence connecting the victim to the "BukaRoo20" account name was insufficiently specific. The court explained that, despite the witness's belief of identity and some weak circumstantial evidence, "[i]nferences must be the probable outcome of logic applied to direct evidence; mere speculative possibilities or conjecture" do not suffice.[121] As the court implies, the often-anonymous nature of instant messaging, combined with its social familiarity, has the potential to obscure the "infirm" nature of evidence derived from it.

Thus, special knowledge present in a communication, only if sufficiently limiting, may prove that the communication was authored by a particular person who uniquely had such knowledge. As the debate between Wigmore and more recent commentators on this point[122] reveals, there is disagreement on the degree of uniqueness in identification required, and the modern trend seems to be that special knowledge known to a small group of people, of which the alleged author is one, is sufficient. However, special knowledge seems less than adequately authenticating when the sender and the recipient of a communication are among that small group and especially when the recipient, who is proffering the evidence or is otherwise adverse to the alleged sender, may have a motive to falsify the communication.

This was the issue in *In re F.P.*[123] A student, Z.G., received instant messages from one "Icp4Life30"[124] threatening a fight over a DVD that "Icp4Life30" claimed Z.G. stole from him.[125] "Icp4Life30" identified himself using the first name of the defendant, F.P.[126] Z.G. presented these mes-

117 2002 WL 501612, at *6.

118 *Id.*

119 *Id.*

120 *Id.*

121 *Id.*

122 *See supra* Part II.A.

123 In re F.P., 878 A.2d 91 (Pa. Super. Ct. 2005).

124 The name apparently refers to the "horrorcore" rap group Insane Clown Posse, which has been "voted the worst band of any genre of music [by] *Spin* and *Rolling Stone*," among other music magazines. *See* Insane Clown Posse, http://en.wikipedia.org/wiki/Insane_Clown_Posse (last visited May 1, 2006). The handles that instant messaging users choose to identify themselves are frequently sexually suggestive, boastful, otherwise tasteless, or just cryptic. Linking a party in court to his handle may thus result in some prejudice, perhaps due.

125 878 A.2d at 94.

126 *Id.*

sages to school authorities, who conducted a "mediation" during which, the court notes, Z.G. "did not deny sending the instant messages."[127] Whether he admitted to sending them is not mentioned. Subsequently, Z.G. received an instant message from "Icp4Life30" complaining "u gotta tell tha school shit and stuff like a little bitch" and threatening, "ima beat ur aSS."[128] Following the last message quoted, F.P. did assault Z.G., the messages were admitted into evidence at his trial, and F.P. was convicted of aggravated assault.[129] F.P. appealed, contesting admission of the instant message logs and arguing that they should have been authenticated by direct evidence, such as computer forensics or records from his ISP.[130]

The court of appeals affirmed the trial court's finding of sufficient authentication, explaining that the logs were "properly authenticated through the use of circumstantial evidence."[131] The court was convinced by four pieces of circumstantial evidence: "Icp4Life30's" use of F.P.'s first name, F.P.'s failure to deny authorship during the school's mediation session, the similarity of "Icp4Life30's" complaints about a stolen DVD and those F.P. had made to a friend of Z.G., and "Icp4Life30's" reference to the mediation session (though not to details of the session).[132] This analysis is troubling in two respects. First, it is not clear that this evidence limits the group of possible writers to a small group, much less a single individual. The court refers to no specific knowledge in Icp4Life30's writings that singles out F.P. Second, to the extent that the writings do evince some specific knowledge that could identify a small group, both F.P. and Z.G., who logged the conversations, are included in that group. The facts of the case, which allowed the trial court to find intent independent of the instant message evidence, make the outcome less objectionable,[133] but authenticating instant message conversations by such a loose standard runs the risk of heaping undue prejudice upon a falsely accused defendant.

---

127 *Id*.

128 *Id*. at 94-95. Different communities of instant message users have their own styles of communication. Misspelling, strange capitalization, slang, and lack of punctuation are often the norm. *See* Microsoft Corp., Leetspeak: A Parent's Primer to Computer Slang, (Mar. 7, 2006), http://www. microsoft.com/athome/security/children/leetspeak.mspx. Again, admission of instant message transcripts containing such dialects may thus result in some prejudice, perhaps due.

129 878 A.2d at 95.

130 *Id*. at 93. *See supra* Part I.B (instant message accounts can be linked to ISP records and thereby to identity); *supra* Part II.C (the log files created by most instant message software can be easily modified); *supra* note 53 and accompanying text (detecting such modifications with forensic techniques is extremely difficult or impossible).

131 878 A.2d at 93.

132 *Id*. at 94-95.

133 Several eyewitnesses testified to F.P.'s aggression and the fight, and F.P. admitted to the fight. *Id*. at 95 n.7.

The court in *People v. Downin*, involving e-mail communications, took a similar approach in admitting e-mail evidence.[134] In *Downin*, the defendant had been convicted of aggravated criminal sexual abuse for engaging in a sexual relationship with a fifteen-year-old girl.[135] At the instigation of a police officer, the victim sent a message to the defendant's e-mail address, which was provided by the victim, stating that she was considering revealing their sexual relationship to her mother.[136] The defendant's alleged response, which the victim forwarded to the police,[137] "contained admissions of a sexual relationship."[138] The prosecution sought to introduce this message but presented no evidence linking the message's e-mail address to the defendant, though the victim did testify that she had used it before.[139] The defendant also testified that she had accessed the defendant's e-mail account in the past and possessed his username and password.[140] Two friends of the victim testified that the victim had discussed with them the movie *Crush*, which concerns "a girl who plotted revenge against a man because she was jealous of another girl,"[141] and one testified that the victim had suggested that she create trouble for her own boyfriend by falsifying e-mails.[142]

On appeal, the defendant argued that the e-mail was not properly authenticated.[143] The court disagreed, holding that the victim's testimony was sufficient.[144] This is troubling because, in this case, the witness and the proffering party had strong shared interests, so the foundational evidence offered—that the victim had sent e-mail to the defendant at that address in the past—amounts to little more than a conclusive assertion that the message is indeed authentic. Though arguable, it is not apparent that this established a prima facie showing of authenticity, especially given the broad range of possible authenticating evidence—from ISP records to computer records[145] to, at the least, evidence of prior communications with that address. While the defendant did challenge the authenticity of the message after it was admitted, it may be that its prejudicial effect had already

134 People v. Downin, 828 N.E.2d 341 (Ill. App. Ct. 2005).

135 *Id*. at 347.

136 *Id*. at 344-45.

137 Forwarding an e-mail, of course, may raise other issues with respect to the Best Evidence rule and the rule of hearsay.

138 828 N.E.2d at 345.

139 *Id*. at 351.

140 *Id*. at 345.

141 *Id*. at 346.

142 *Id*.

143 *Id*. at 350.

144 828 N.E.2d at 350-51.

145 Neither the victim's nor the defendant's computer was examined by investigators. *Id*. at 345.

damned him. The court's mistake here is simple: a message apparently written in reply to an earlier message does not necessarily authenticate the reply when the identity of the original message's recipient has not been established. The court's authentication process confirmed only that a message admitting a sexual relationship was sent in reply to a message threatening to disclose that relationship.

Can an instant message conversation that is not a business record be self-identifying? One case implies that this is possible. In *Bloom v. Commonwealth*, the defendant was convicted of attempting to coerce a thirteen-year-old girl into sexual relations.[146] The prosecution proffered an instant message log between the victim and "Philter425," recorded by a police detective, and the victim testified to earlier instant message conversations, which had not been logged.[147] In these earlier conversations, the victim had noted her age, the defendant's knowledge of which was an essential element of the crime, and that she had been grounded by her mother.[148] The defendant admitted his participation in the later, recorded conversation but maintained that he was not the "Philter425" who took part in the earlier conversations and thus, when he had ventured to meet the victim at a local Burger King and take her home for "wild monkey sex," was unaware of the victim's age.[149]

The courts could have authenticated the earlier conversation in two ways. First, "Philter425" asked the victim in the recorded and admitted instant message conversation, "are you ungrounded now[?]"[150] Applying the reply doctrine in reverse (that is, to authenticate an earlier communication based on an authenticated later one), a court could find this question sufficient to authenticate the earlier conversations.[151] Second, the prosecution might have presented evidence that the instant message account "Philter425" was registered to the defendant, had been used by the defendant and not by others, or at least was protected by a password and had not been transferred during the period during which the conversations took place. There is no evidence in the record that the prosecution sought out this evidence or presented it to the court in response to the defendant's motion in limine to exclude the evidence.

On the defendant's appeal to Virginia's Court of Appeals,[152] the court employed the reply doctrine based on the victim's grounding but also fo-

146 Bloom v. Commonwealth, 542 S.E.2d 18, 19 (Va. Ct. App. 2001), *aff'd*, 554 S.E.2d 84, 88 (Va. 2001).

147 *Id*. at 20.

148 *Id*.

149 *Id*.

150 *Id*.

151 On the reply doctrine, *see supra* Part II.A.

152 After the Court of Appeals affirmed, the case was appealed to the Virginia Supreme Court,

cused on statements made by "Philter425" in the earlier conversations: that he was male, was named Greg, was twenty-eight years old, and had a daughter.[153] The problem with this is that these statements have probative value as to authentication only with the *assumption* that the defendant made them and that his motive in that conversation was to importune. Had the defendant not admitted to being "Philter425" in the later conversation, the court would seemingly have had to require additional evidence, such as from the instant message service or the defendant's ISP, to admit the conversations. As one discussion of *Bloom* explains, under the Virginia Supreme Court's standard, an instant message user who is using the handle "Prez2001" and admits to living on Pennsylvania Avenue in Washington with his wife Laura would be sufficiently identified for the purpose of authentication.[154]

Moreover, the court considered the identifying statements to have probative value without any independent verification of their connection to the alleged "Philter425"—that is, the defendant.[155] This practice "allows for the possibility that prosecutorial proffers, rather than hard evidence, will convict those accused of using the Internet for illegal purposes."[156]

The court's willingness to accept challenged proffers as proof and, more basically, to give "Philter425's" vaguely identifying statements much weight may stem from an analogy employed by the Court of Appeals. The court believed that "[c]onversations over the internet are analogous to telephone conversations. Conversations overheard on a telephone are admissible if direct or circumstantial evidence establishes the identity of the parties to the conversation."[157] While useful in some respects, that analogy carries only so far. The same lack of identifying characteristics and voice that makes textual instant messaging so attractive to practicing and would-be pedophiles also undercuts the ability to identify participants in instant message conversations by many direct means, such as voice, age, sex, and perhaps even writing style.[158] As well, the relative anonymity afforded by the medium facilitates and perhaps encourages deception.[159] In several instances at least, instant message users have met online acquaintances in real

which repeated the basic reasoning of the Court of Appeals decision. Bloom v. Commonwealth, 554 S.E.2d 84 (Va. 2001).

153 542 S.E.2d at 20.

154 Jessica C. Cobaugh, *Bloom v. Commonwealth: Identifying the Face Behind the Instant Message*, 8 RICH. J.L. & TECH. 17, ¶ 57 (2002), http://www.law.richmond.edu/jolt/v8i3/article17.pdf.

155 *See* 554 S.E.2d at 87-88.

156 Cobaugh, *supra* note 152, ¶ 56.

157 542 S.E.2d at 20.

158 On writing style, *see supra* note 126.

159 On pseudonymity, *see supra* note 27.

life who were not as described online.[160] Accepting at face value instant message conversations that purport to identify the author would be to give them undue weight.

As it is rarely challenged,[161] the authentication requirement may from time to time escape the court's notice. This seems to have happened in *Everett v. State*.[162] The prosecution's key evidence was a collection of instant messages that, despite being authored by a juvenile on her parent's computer and pasted into an e-mail (subsequently discovered by the father), was admitted as a business record by the trial court.[163] The appeals court found another way to escape the rule of hearsay[164] but overlooked the initial authentication of the messages, which was similarly in error.[165] Hedging its bets, the court declared the error not reversible anyway because there was other incriminating evidence.[166] That the error was insignificant is debatable, given the persuasive nature of writings and the graphic and explicit nature of the sex acts described in the instant messages.[167] Had the trial court not erroneously admitted the e-mail message, the appellate court would have faced a difficult question of authenticity. Though it patched up the hearsay problem, the appeals court ignored authentication, which might have kept the e-mail out to begin with.

B. *Best Evidence*

Perhaps surprisingly, given the ease with which instant message logs can be manipulated and counterfeited,[168] few parties have challenged evidence of instant message conversations using the Best Evidence rule. With the Best Evidence rule frequently relegated to the status of a "preference" rather than a bar, perhaps this reluctance to employ it is understandable. While the question has been raised, no courts have seriously entertained a Best Evidence challenge to instant message evidence.

---

160 *See, e.g.*, State v. Bell, No. 2004-CA-5, 2005 WL 388174, ¶ 80 (Ohio Ct. App. Feb. 18, 2005) (following receipt of a voice-mail message from the victim, defendant exclaims in instant message conversation, "you are a female").

161 MCCORMICK, *supra* note 68, § 218.

162 Everett v. State, No. 14-01-00588-CR, 2002 WL 534124 (Tex. Ct. App. Apr. 11, 2002).

163 *Id*. at *1.

164 *Id*. at *2.

165 As under the Federal Rules since the enactment of Rule 902(11) in 2000, business records are self-authenticating under the Texas Rules. TEX. R. EVID. 902(10).

166 Everett, 2002 WL 534124 at *2.

167 *Id*. at *3.

168 For a discussion of log falsification, *see supra* Part I.C. *See also* discussion of Slattery v. United States, No. 2:98CR125-B, 2005 WL 2416339, at *6 (N.D. Miss. Sept. 30, 2005), see *infra* text accompanying notes 180-87.

In most cases, the Best Evidence rule will present no bar to admission. In *Adams v. State*, for example, the defendant argued on appeal that printouts of the police department's instant message logs from an online sting did not satisfy the Best Evidence rule.[169] The electronic files, not the printouts, were "originals," he contended, and the printouts were thus inadmissible.[170] The appeals court answered this argument with ease: the Wyoming Rules of Evidence, which parallel the Federal Rules, consider printouts that accurately reflect data in a computer to be originals themselves.[171]

In *United States v. Tank*—cited in several cases as to the reliability and admissibility of instant communications[172]—the defendant challenged on appeal the trial court's admission of a log of conversations held in the "Orchid Club," a members-only chat room where participants "discussed, traded, and produced child pornography."[173] After one member of the club was arrested on molestation charges, police found on his computer automatically recorded log files of conversations that took place in the chat room.[174] Prior to his arrest, this member had removed "extraneous material," such as non-sexual conversations and timestamps, from the log files "to decrease the size of the text files and save space on his hard drive."[175] These logs implicated the defendant.[176] On appeal, the defendant argued that the government should have attempted recovery of the originals of the altered chat logs.[177] The court disagreed, explaining that the logs had been created as part of a regular and reliable process; thus, the logs that had been admitted, it concluded, "appeared to be an accurate representation of the chat room conversations."[178] Because the party offering the evidence—the government—did not undertake the alterations and deletions itself, there was no bad faith, and the Best Evidence rule was therefore not violated.[179] That the government's source of the evidence may share in the government's interest and has in fact destroyed the original writing is thus immaterial.

169 Adams v. State, 117 P.3d 1210, 1218 (Wyo. 2005).

170 *Id*. at 1218. For a discussion of the Federal Rules' approach to electronic evidence, *see supra* text accompanying notes 86-92.

171 117 P.3d at 1218. Wyoming Rule of Evidence 1001(3) is identical to Federal Rule 1001(3).

172 *See, e.g.*, U.S. v. Grant, 218 F.3d 72, 79 n.2 (1st Cir. 2000); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002).

173 United States v. Tank, 200 F.3d 627, 629 (9th Cir. 2000).

174 *Id*.

175 *Id*. With the low cost of spacious hard drives and the little space that text logs consume, this explanation strains credulity.

176 *Id*.

177 *Id*. at 631 n.5.

178 *Id*. at 630.

179 *See Tank,* 200 F.3d at 631 n.5. Secondary evidence can be used when the original was destroyed, unless the destruction was due to proffering party's bad faith. *See supra* Part II.B.

The court in *Slattery v. U.S.* faced a similar issue.[180] In the defendant's jury trial, the prosecution relied on two sets of instant message logs, one of which was not at issue in the defendant's subsequent habeas corpus petition, to prove that the defendant crossed state lines with the intent to engage in sex with a minor.[181] The other set was compiled by a would-be online vigilante named Shepherd who claimed that he stumbled by accident upon a chat room devoted to incestuous relations and sex with minors and, after interacting with the participants, began to log the conversation as an aid to law enforcement.[182] As the appeals court pointed out, "Shepherd was obviously lying" about much of his story, as evidenced by the fact that he was subsequently arrested and convicted for sexual acts with his underage daughter.[183]

The chat log supplied by Shepherd was "questionable at best," the appeals court noted.[184] A witness from America Online testified that "such logs are stored on the user's computer (not an America Online computer) in basic text documents that anyone with a modicum of computer experience can modify at will."[185] Moreover, the log files did show evidence of tampering: account names had been excised, the formatting was inconsistent, and it appeared that the log file contained several instant message conversations that had been blended into one, leading to internal inconsistencies in the text.[186] The appeals court does not actually reach the Best Evidence rule here, for the reason that so much other evidence not suffering from such faults was presented; in any case, as in *Tank*, discussed *supra*, the government did not undertake the alterations itself, allowing it to use secondary sources freely, whatever their relationship to the original.[187]

IV. A SKEPTICAL APPROACH

With much instant message evidence, skepticism is warranted. Especially in cases involving sexual offenses and children, the contents of instant message conversations can carry great weight and be extremely prejudicial and damaging to the accused, containing vulgarities, crude descriptions of sexual activities, and poor spelling and grammar.[188] This prejudice

180 Slattery v. United States, No. 2:98CR125-B, 2005 WL 2416339 (N.D. Miss. Sept. 30, 2005).
181 *Id*. at *1-*3.
182 *Id*. at *2.
183 *Id*. at *6.
184 *Id*.
185 *Id*.
186 *Slattery*, 2005 WL 2416339, at *6.
187 *See supra* Part II.B.
188 *See supra* notes 124, 128.

is warranted—indeed, it is laudable—when there is some evidence that the accused is actually the author of the written statements presented against him and that those statements are presented in court accurately. Other kinds of writings, to be sure, may carry just as much weight and be just as prejudicial, but instant messaging affords a great deal of anonymity that may stymie reasonable identification of authorship without collateral investigation.[189] Moreover, instant message evidence is easily and undetectably altered and fabricated.[190] The existing rules of evidence, applied with some justified skepticism toward this kind of evidence, permit a more thoughtful approach than has been employed so far.

This section addresses popular, as opposed to corporate, instant messaging services for the reason that regularly maintained logs of instant message conversations are less likely to be contested and, for authentication, seem to fit within Rule 902(11) and (12) and the similar rules and practices used in state courts.[191]

A. *Authentication*

The issues that arise when a party seeks to authenticate instant message evidence are the same as those that arise with any other kind of evidence. The only difference is that some courts, perhaps blinded by the technology, have generally declined to look beyond proffering parties' assertions and the text of proffered writings.

As illustrated by *People v. Von Gunten*[192]—in which the accused was the most likely author of instant messages that his witness believed came from the victim—the pseudonymous and conversational nature of instant messaging lends itself well to convincing impersonation. Cutting through all the inconclusive circumstantial evidence, the court determined that there was no actual basis for concluding that the alleged author of the messages was whom the accused claimed.[193] The court's skepticism here was admirable.

In contrast, the admission of instant messaging evidence in *In Re F.P.* demonstrates an overreach.[194] As in *Von Gunten*, no direct evidence connected the alleged sender to the instant message conversation, and the circumstantial evidence was perhaps even weaker: In *Von Gunten*, the witness

189 *See supra* Part I.B.

190 *See supra* Part I.C.

191 On corporate messaging, *see supra* notes 35, 37 and accompanying text. On self-authentication of business records, *see supra* note 69 and accompanying text.

192 *See supra* notes 111-21 and accompanying text.

193 *See supra* note 117 and accompanying text.

194 *See supra* notes 127-33 and accompanying text.

had conversed with an instant message sender for at least one month[195] rather than just a few days, as in *In re F.P.*[196]

Courts need not wade into these perilous waters because direct evidence is likely available. As several commentators have noted, a "genius . . . appears in one of every thousand cases,"[197] and while criminals may have the opportunity to cover their online tracks,[198] few will have the ability or the foresight to do so. In many cases, instant messaging technology can be made to yield a user's IP address,[199] and in most cases, that address can be tied to a means of accessing the Internet and thus a person, just as a telephone number can be connected to the person paying for it.[200] That the owner of an IP address actually is the author of the messages is a strong and logical presumption, though one that can be rebutted in some cases. It is surely enough, though, for a prima facie showing of authentication. Courts should be wary, then, when this foundational evidence, easily had, is not provided—though its absence, particularly in the case of that one-in-a-thousand genius criminal, is not dispositive.

As in *Simpson*, circumstantial evidence may suffice to authenticate instant message evidence.[201] In moving away from the standard set in that case, there is the risk that circumstantial evidence that is merely consistent with the proffering party's theory of authentication may appear actually to show authentication. This was the mistake in *In Re F.P.* and, even more egregiously, in *Downin*.[202] Courts that follow more recent precedent in holding that circumstantial evidence, usually knowledge, need not be uniquely identifying[203] run into a special problem when such knowledge is known to two people, the alleged author and an adverse proffering party or adverse witness. This use of circumstantial evidence, especially when the evidence would have a strong prejudicial effect or the finder of fact is likely to accord it undue weight, is dangerous.

195 People v. Von Gunten, No. C035261, 2002 WL 501612, at *6 (Cal. Ct. App. Apr. 4, 2002).

196 In re F.P., 878 A.2d 91, 94 (Pa. Super. Ct. 2005).

197 Jablon, *supra* note 87, at 1391 (quoting BUCK BLOOMBECKER, SPECTACULAR COMPUTER CRIMES 37 (1990)).

198 They may, for example, use proxy servers. *See supra* Part I.B.

199 *See supra* Part I.B.

200 *See supra* Part I.B.

201 *See supra* notes 105-110 and accompanying text.

202 For a discussion of Downin, *see supra* notes 134-45 and accompanying text.

203 *See supra* notes 73, 122 and accompanying text.

B. *Best Evidence*

The cases to date that have applied the Best Evidence rule to instant message evidence have engaged in little analysis and have barred no evidence, even when evidence was obviously altered and therefore not necessarily the best evidence. In most cases involving instant message logs, the Best Evidence rule is not reached. By the text of the rule and given the reliability of this kind of evidence, this may be a mistake.

To begin with, courts have given little thought as to whether an instant message log that was recorded by a victim or by police and is being used as evidence of intent is actually an "original" document. While instant messaging is a reliable medium, logs, if they exist, could vary between different participants in a conversation for a variety of reasons, such as Internet congestion that blocks messages or delays their delivery, the capabilities of the client software being used to create the log, participants' online status affecting message delivery, and falsification.[204] For these same reasons, different parties' logs may not be duplicates as defined by Rule 1001(4) and made admissible by Rule 1003.[205] The relevant document, when intent is to be proved, is not the victim's log but the log of the accused.[206] Rule 1004 provides only three substantive exceptions when the original writing or recording is not required: when an original is lost or destroyed, is not obtainable by judicial procedure, or is in the possession of the opponent.[207] Putting these rules together, the Best Evidence rule would seem to require proponents of instant message logs, if they have seized or copied the accused's computer disks, to apply appropriate forensic techniques to alleged perpetrator's computers to determine whether a truly "original" log exists. When law enforcement agencies have not gone to this trouble, as in *Tank*,[208] evidence of the instant message conversation should be barred from the court because it is not necessarily the "best evidence."

In addition, it is debatable whether any log file, at least among those that have been described in the case law to date,[209] truly meets the definition of "original" in Rule 1001(3). The rule speaks of the "writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it." The language applies most readily, of course, to matters of contracts, wills, deeds, and the like, but it may also have some relevance to other evidentiary matters. An instant message, unlike an e-mail

204 *See supra* Part I.C.

205 *See supra* Part II.B.

206 *See supra* notes 89-92 and accompanying text.

207 FED. R. EVID. 1004.

208 *See supra* note 177 and accompanying text.

209 There is one exception, which was excluded on other grounds. *See supra* note 58.

or a letter, is practically incapable of standing alone. Rather, an instant message is more akin in form to a single sentence in a telephone conversation.[210] A partial log of an instant message conversation may or may not have the same "effect" as the original whole. Moreover, instant messaging clients may not log audio and video, timestamps, colors and text decorations, images and URLs, and other trappings of the conversation.[211] Thus, the full "effect" of such a conversation is unlikely to be captured in a log file; in logging, then, much of the "original" writing is lost. A reasonable duplicate of this original would be a video of the entire screen coupled with an audio recording, which would include all contextual information that may have some bearing on the conversation.[212] With current technologies, such videos are easy and very inexpensive to record and do not require a camera or any equipment beyond the computer itself.[213] Crucially, such videos are difficult to alter and falsify.

What should happen when this standard is not met? A police detective, other law-enforcement agent, or vigilante who is recording an instant message conversation has no good excuse for not capturing the complete original. Except in the case of computer malfunction or the like, falling short of this standard would mean that the original has been deliberately "lost," as that word is used in Rule 1004(1), presumably in bad faith. When the recording party is not engaging in actual or contemplated law enforcement, this presumption would generally not apply; perhaps, however, it should when such logs are recorded with litigation or prosecution in mind—especially if the party has contacted counsel or a law-enforcement agent. The category of "testimonial" evidence established in *Crawford v. Washington*[214] may be applicable to this determination.

C. *Using Rule 403*

A Note concerning the admissibility of e-mail evidence recommends that "judges . . . use their discretionary powers under Rule 403" to exclude e-mail evidence that is authenticated by a literal reading of the rules but still appears to be unreliable in a way for which the finder of fact may not ac-

210 *See generally supra* Part I.A.

211 *See generally supra* Part I.C.

212 For an example of such use, *see supra* note 57.

213 *See, e.g.*, TechSmith Corp., Camtasia Studio Screen Recorder Product Information Page, http://www.techsmith.com/products/studio/default.asp (last visited May 1, 2006) ("Easily record activity on your computer screen, audio and webcam video." The software costs $300 and will run on nearly all Windows-based computers purchased within the past 5 years.).

214 Crawford v. Washington, 541 U.S. 36, 68 (2004).

count fully.[215] Under this Rule, "evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice…." A sensitivity to the ways in which instant message evidence can be fabricated and falsified would no doubt influence a judge's application of this Rule. As the Note explains, "[d]ue to the difficulty in proving that a piece of electronic mail is a forgery, it does not appear to be an abuse of a judge's discretion to exclude electronic mail because of unfair prejudice."[216] As e-mail evidence is, in some ways, easier to authenticate than instant message evidence, this conclusion should hold.

CONCLUSION

For nearly twenty years, lawyers have counseled that e-mail technology is insecure and should be replaced by a system that uses encryption and digital signatures and creates a better record of e-mail communications.[217] For as long as these technologies have existed, however, consumers have ignored them.[218] The same is likely to happen with instant messaging, which means that the insecure, unauthenticated networks that we have today are likely to be the norm for years. Regular users may favor this current technology specifically for these shortcomings.

In many ways, an instant message is like an e-mail or a letter; a textual instant message log appears more like the transcript of a telephone call. In reality, however, neither consumer-grade instant messaging nor its log files carry any of the direct markers of authentication of these other media of communication. Even jurors who are familiar with instant messaging and use it regularly to converse with friends and family may not be aware of its inherent evidentiary unreliability—especially when identity is not evidenced directly and given the ease with which records of conversations can be falsified. In other words, jurors' own familiarity with the medium may

215 Jablon, *supra* note 87, at 1407.

216 *Id*.

217 *See, e.g.*, Jablon, *supra* note 87, at 1405-07; Chris Reed, *Authenticating Electronic Mail Messages - Some Evidential Problems*, 52 MOD. L. REV. 649, 656-59, 660 (1989) ("[T]he best method of authentication is undoubtedly some form of digital signature."); Andew Grosso, *The National Information Infrastructure*, 41 FED. B. NEWS & J. 481 (1994); Peter N. Weiss, *Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy*, 12 J. MARSHALL J. COMPUTER & INFO L. 425, 437 (1993). *But see* Robert W. McKeon, Jr., *Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena*, 12 J. MARSHALL J. COMPUTER & INFO. L. 511, 519 (1994) ("Digital signatures are not likely to be widely implemented in the near future . . . .").

218 For example, none of the major free and commercial e-mail services provide encryption and digital signatures. Digital signatures are not enabled by default in Microsoft's popular Outlook messaging application or Apple's Mail application.

cause them to inflate the relevancy of evidence from it. Judges and defense attorneys, however, should not suffer from such misconceptions.