View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Campbell University Law School

Campbell Law Review

Volume 43
Issue 3 *Symposium Issue*

Article 7

2021

It Was Here a Second Ago: North Carolina Discovery andEphemeral Messaging Apps

Joshua Walthall

Follow this and additional works at: https://scholarship.law.campbell.edu/clr

Recommended Citation

Joshua Walthall, *It Was Here a Second Ago: North Carolina Discovery andEphemeral Messaging Apps*, 43 CAMPBELL L. REV. 477 (2021).

This Article is brought to you for free and open access by Scholarly Repository @ Campbell University School of Law. It has been accepted for inclusion in Campbell Law Review by an authorized editor of Scholarly Repository @ Campbell University School of Law.

It Was Here a Second Ago: North Carolina Discovery and Ephemeral Messaging Apps

BY: JOSHUA WALTHALL*

ABSTRACT

Ephemeral messaging apps allow users to send and receive text messages that disappear after being read. How might such technology impact the practice of law, especially as it concerns discovery? This Article defines ephemeral messaging apps, reviews recent discovery litigation in North Carolina for possible points of application with ephemeral messaging apps, and analyzes the North Carolina Rules of Civil Procedure and the North Carolina Rules of Professional Conduct in light of ephemeral messaging apps. This Article also examines how other, out-of-state courts have dealt with ephemeral messaging apps in the context of discovery and makes some practical suggestions on what North Carolina courts might or should do when faced with ephemeral messaging apps and their use by attorneys or litigants in North Carolina.

*Walthall is a lawyer and adjunct professor in Raleigh, N.C. He is particularly grateful to Jeff Kelly, as fine a civil litigator as you're likely to meet, for guidance on this topic. He is also deeply indebted to the exceptional research and writing assistance of Laurel Christmas and Lauren Johnson in the drafting of this article. All mistakes and boring portions are the author's.

Published by Scholarly Repository @ Campbell University School of Law, 2021

BOTH FRIEND AND ENEMY: AN INTRODUCTION

Neil Postman describes technology as "both friend and enemy,"[1] "both a burden and a blessing."[2] Objectively, this rings true. Anyone who attempted to drive a car to an unfamiliar location before the advent of global positioning systems and downloadable celebrity voices instructing us when to "take a left in half a mile" can attest to the blessings of technology. And anyone who has attempted to have a meaningful or cogent conversation with a teenager holding a smart phone can likely swear to technology's burden—as could any attorney forced to respond to a client's text message at 11:37 p.m. on a Tuesday.

What is undeniable, though, is that technology is here to stay, demanding we use it and taking captive our time and attention, for better or worse. "Copious studies show a reduced amount of leisure time experienced by modern families, more time in front of the TV and the computer, and growing obesity among adults and children because of diet and sedentary lifestyles."[3] For old dogs and Luddites, the proliferation of technology presents more burden than boon. But digital natives likely see only blessings or friends in the ever-present screens in their offices, bedrooms, cars, kitchens, and pockets.

> Today's students – K through college – represent the first generations to grow up with this new technology. They have spent their entire lives surrounded by and using computers, videogames, digital music players, video cams, cell phones, and all the other toys and tools of the digital age. Today's average college grads have spent less than 5,000 hours of their lives reading, but over 10,000 hours playing video games (not to mention 20,000 hours watching TV). Computer games, email, the Internet, cell phones and instant messaging are integral parts of their lives.[4]

In the world of law, the blessing-and-curse nature of technology—and the dichotomy with which its users respond to it—evidences itself not just in how digital natives and digital immigrants use their time, interact with each other, and bill hours, but it rears its head in more formalized communications as well. For a significant portion of lawyers in the United States, emails seem to have largely replaced hardcopy letters, even in formal

1. NEIL POSTMAN, TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY, at xii (Vintage Books 1993) (1992).

2. *Id.* at 5.

3. RICHARD LOUV, LAST CHILD IN THE WOODS 31–32 (rev. and updated ed. 2008).

4. Marc Prensky, *Digital Natives*, *Digital Immigrants*, 9 ON HORIZON, no. 5, Oct. 2001, at 1.

legal communications; others, though, still swear by the thick and oily cardstock of a hardcopy letter, signed in majestic hand.

Notable differences in discovery approaches also exist in the profession; in just the last few years "e-discovery" became, if not a household word, one regularly on the lips of all but the luckiest civil litigators.[5] And as any first-year law student can attest, the Rules governing discovery are legion[6]—and often confusing.

To complicate matters even more, technology, as we all know, is not static. Inventors, engineers, and entrepreneurs create new platforms, websites, and "apps," common vernacular for "applications," every day; and the world of law—specifically, the world of discovery—enjoys no immunity from this constant evolution. What happens when these inevitable and relentless advances in technology outrun the rules governing lawyers, be they the North Carolina Rules of Civil Procedure or the North Carolina Rules of Professional Conduct? Well, overlong law review articles that get written by dodgy law school professors perhaps provide as honest an answer as any. This is the situation before us at present: ephemeral messaging apps have arrived on the scene, so lawyers and litigants must figure out how the legal and ethical standards govern the apps, their use, and the attorneys and litigants who utilize them. "For it is inescapable that every culture must negotiate with technology, whether it does so intelligently or not."[7]

This Article will (I) introduce the blissfully uninitiated—be you digital native or digital immigrant—to ephemeral messaging apps; (II) review recent discovery litigation in North Carolina, paying particular attention to discovery violations, document preservation, spoliation, and sanctions, with an eye toward how North Carolina courts might handle ephemeral messaging apps; (III) analyze the North Carolina Rules of Civil Procedure and the North Carolina Rules of Professional Conduct for possible points of intersection with this new technology; (IV) examine how other, out-of-state courts have dealt with ephemeral messaging apps in the context of discovery; and finally, (V) make some practical suggestions on what North Carolina courts might or should do when faced with ephemeral messaging apps and their use by attorneys or litigants in this state.

---

5. *See* Lucas Newcomer & Johnny Lee, *E-Discovery Challenges and Information Governance Solutions*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/litigation/committees/pretrial-practice-discovery/articles/2019/winter2019-e-discovery-challenges-and-information-governance-solutions/ [https://perma.cc/V3C3-S7JW] ("Over 90 percent of the data in the world today has been created within the past two years, and the number and variety of data sources that an organization must manage continues to grow.").

6. *See generally* FED. R. CIV. P.; N.C. R. CIV. P.

7. POSTMAN, *supra* note 1, at 5.

I. NEWFANGLED TECHNOBABBLE: WHAT ARE EPHEMERAL MESSAGING APPS?

What are ephemeral messaging apps and how are they used? Perhaps only a fool risks summarizing new technology in a medium such as this. Undoubtedly it risks information technology professionals—or perhaps just any digital native—finding it overly simplistic and wanting, while at the same time threatening to be too confusing for digital immigrants. In an effort to strike a balance somewhere in between, the below summary is by no means exhaustive, but merely an effort at a brief explanation that most folks, be they digital natives or digital immigrants, can hopefully understand.

An ephemeral messaging app is a communication platform that allows one user to send to another user an electronic message, similar to an email or text message, that will automatically disappear directly after the recipient views it. Ephemeral messaging apps "are now widely available on a host of platforms, including enterprise software such as Slack or DingTalk. Although each application is slightly different, they all incorporate some type of trigger that automatically deletes messages shortly after viewing and prevents users from editing, copying, forwarding or printing the messages."[8] Such apps are lauded by "privacy advocates"[9] and are becoming increasingly available, especially in the context of litigants and those subject to discovery:

> Time-limited messaging, after all, can stifle the best laid e-discovery plans or the most thoroughly conducted investigation. And they're not going away anytime soon. Once only the focus of a handful of messaging apps, ephemeral messages are now being offered by widely used services like Gmail and Facebook.[10]

Typically, messages sent through ephemeral messaging apps are not even captured or saved on a server. Messages sent and received via an ephemeral messaging app "create the digital facsimile of an in-person

8. William Semins et al., *The Compliance Risks Facing Companies That Use Chat Apps*, LAW360 (June 16, 2020, 4:38 PM), https://www.law360.com/articles/1282305/the-compliance-risks-facing-companies-that-use-chat-apps [https://perma.cc/4QW2-T376].

9. Rhys Dipshan, *This Article Will Self-Destruct: Behind Ephemeral Messaging's In-House Rise*, LAW.COM: LEGALTECH NEWS (June 13, 2019, 11:30 AM), https://www.law.com/legaltechnews/2019/06/13/this-article-will-self-destruct-behind-ephemeral-messagings-in-house-rise/ [https://perma.cc/RFZ4-4FD9] (follow "Go to Lexis Advance®" or "Go to Bloomberg Law" hyperlink to access archived content).

10. *Id.*

meeting or a telephone call by deleting or otherwise destroying a message shortly after it has been read or opened by its recipient(s)."[11] The apps themselves "are often peer-to-peer, which eliminates servers in between the sender and recipient that could potentially be used to capture the communication. These layers of security make retrieval or reproduction of such messages nearly impossible."[12]

For digital natives, the preceding paragraph, what with its references to servers and digital facsimiles, is probably as easy to read as a bowling alley lunch menu and requires no further explanation. Digital immigrants like the undersigned author, though, require some expert help. A server is essentially a central storage system through which a company's emails travel before being sent to the recipient: "Generally, in a business organization, email systems use a central computer (sometimes the server) to store messages and data and to send them to the appropriate destination. All that is needed to send messages is a PC, modem, and email connection."[13] Emails sent through a regular channel are often captured on a server and, even when deleted from the email recipient's inbox, can be retrieved by someone searching or accessing the server. "Deleted emails are, in most cases, not irretrievably lost. Deleted emails may remain on a computer hard drive, servers or retained on back-up tapes."[14]

Think of it this way: if an email is a hardcopy letter, the email recipient's inbox is her hands, and the server is the waste bin in which she tosses the note after she has read it. Even if she throws the note away, into the bin, the note still exists and can be accessed and read later. To completely eradicate the note, the recipient would need to remove it from the bin and burn it. In much the same way, the recipient of an email cannot eradicate it simply by deleting the email from his inbox; it will still exist on a server and can be searched for, found, and produced in discovery later. Messages sent via ephemeral messaging apps, however, are not kept on a server, so when they disappear, they cannot be accessed again, even by the sender or the recipient.[15]

The interface, methods, and use of ephemeral messaging apps vary from platform to platform, but many are akin to instant messaging applications popularized in the early dawn of the internet and known even amongst some digital immigrants: America Online Instant Messenger and

11. Semins et al., *supra* note 8.

12. *Id.*

13. MICHAEL R. ARKFELD, *Structure and Type of Electronic Information*, *in* ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE § 3.9 (2020).

14. *Id.*

15. *See* Semins et al., *supra* note 8.

Google Chat. Once again, an example may help illustrate how ephemeral messaging apps are used. An ephemeral messaging app user, Woodrow, pulls out his mobile phone and initiates a "chat" with another user, Augustus. Woodrow types text into the app and sends it to Augustus in the platform, not unlike a text message. Augustus reads the message on his mobile phone and then it disappears, never touching a server or being stored in any way and thus not saved or accessible anywhere. Augustus can then send a text message back to Woodrow in the app, and vice versa, the process of typing, sending, receiving, and disappearing repeated as many times as the parties wish.

That, in short form, is what ephemeral messaging apps are: disappearing text messages that vanish shortly after they are read by the recipient. As mentioned, this summary does not plumb the depths of the technology; certain aspects of the various applications are not explained in absolute detail, but for our purposes, they need not be. Let us now set aside these strange new apps and consider, non-exhaustively and only by way of example, recent discovery litigation in North Carolina so that we can thereafter look at how courts might examine ephemeral messaging apps and their use by attorneys and litigants in The Old North State.

II. WHAT HAD HAPPENED WAS: RECENT DISCOVERY LITIGATION IN NORTH CAROLINA

Once again, the recent cases listed below are not intended to be exhaustive of all discovery litigation in North Carolina, nor is the summary an opus on the North Carolina Rules of Civil Procedure; such a tome already exists and cannot be improved upon.[16] The below exists here only to provide us with a framework through which we can consider ephemeral messaging apps in light of the laws of North Carolina.

A. Crosmun v. Trustees of Fayetteville Technical Community College

In *Crosmun*, the North Carolina Court of Appeals faced its "first opportunity to address the contours of eDiscovery within the context of North Carolina common and statutory law regarding the attorney-client privilege and work-product doctrine."[17] In *Crosmun*, former employees of Fayetteville Technical Community College sued the school, "alleging retaliatory dismissals . . . in violation of the North Carolina Whistleblower

16. *See* G. GRAY WILSON, NORTH CAROLINA CIVIL PROCEDURE (3rd ed. 2007).

17. Crosmun v. Trs. of Fayetteville Tech. Cmty. Coll., 832 S.E.2d 223, 228 (N.C. Ct. App. 2019).

Protection Act."[18] The plaintiffs served the defendants with three sets of interrogatories and requests for production, seeking electronically stored information retained in the school's computers and servers.[19] The trial court entered both an order compelling discovery and an order providing that a computer forensic expert would conduct a forensic examination of the defendants' computer files.[20] The defendants appealed from this order and contended that the order amounted to an involuntary waiver of their attorney–client privilege and the work-product doctrine.[21]

On appeal, the court acknowledged the necessity of the forensic examination order but identified two reasons for vacating the discovery order.[22] The court then advised, first, that an independent expert needed to perform the forensic examination to protect confidentiality, and, second, that the responding party should have an opportunity to review the keyword search used in the forensic examination prior to production of responsive electronically stored information to the opposing party.[23]

In analyzing the broader contours of e-discovery, the court "consider[ed] decisions of courts in other jurisdictions."[24] The court stated that forensic examinations of electronically stored information "may be warranted when there exists some factual basis to conclude that the responding party has not met its duties in the production of discoverable information."[25] But even when a forensic examination is appropriate, "any protocol ordered must take into account privileges from production that have not been waived or otherwise lost."[26] The court noted that, in ordering forensic examinations, courts should be mindful of: a) disclosing trade secrets; b) disclosing confidential or private information; c) disclosing "confidential attorney–client or work-product communications"; d) "unreasonably disrupting the ongoing business"; e) "endangering the

18. *Id.*

19. *Id.*

20. *Id.* at 229.

21. *Id.* at 228.

22. *Id.* at 236–37 (identifying error in allowing plaintiffs' expert, "rather than an independent third party, the authority to directly access and image the entirety of Defendants' computer systems absent regard for Defendants' privilege," and in "the delivery of responsive documents to Plaintiffs without allowing Defendants an opportunity to review them for privilege").

23. *Id.* at 240.

24. *Id.* at 233.

25. *Id.* at 234 (citing Feeassco, LLC v. Steel Network, Inc., 826 S.E.2d 202, 209 (N.C. Ct. App. 2019)).

26. *Id.*

stability of operating systems" or files; and f) "placing a responding party's computing systems at risk of a data security breach."[27]

B. Tumlin v. Tuggle Duggins P.A.

In *Tumlin*, a North Carolina Business Court case, the plaintiff moved for discovery sanctions against the defendant, asserting that the defendant violated Rules 26(g) and 37(b)(2) of the North Carolina Rules of Civil Procedure.[28] The plaintiff asked the court to order a forensic examination of the defendant's email server, at the defendant's expense, "to determine if potentially relevant e-mails were lost because of [the defendant's] failure to adequately preserve documents."[29] The document request at issue sought the production of "emails . . . in [the defendant's] possession or control . . . regarding or pertaining to plaintiff's departure from the defendant [law firm] and/or relating to plaintiff's compensation."[30] The defendant law firm diligently searched its email server numerous times and produced responsive, non-privileged emails when appropriate.[31]

The plaintiff's motion asserted four separate contentions: (1) the defendant violated Rule 26(g) of the North Carolina Rules of Civil Procedure; (2) the defendant "failed to conduct reasonable searches and effectively manage e-discovery"; (3) the defendant "failed to provide [the plaintiff] with all responsive emails"; and (4) the defendant "did not take reasonable steps to preserve electronic records."[32]

The court rejected each of these arguments.[33] First, the court found that by conducting multiple searches to locate relevant documents, the defendant made sufficient efforts to produce all reasonably accessible documents and, as such, there was no factual basis to conclude that the defendant "signed the discovery responses with knowledge that a potentially relevant email had been lost" or deleted.[34] Next, based on the number of searches conducted—four—and the documents produced compared to the purported value of any further production, the court found that the defendant neither purposely withheld responsive documents nor

27. *Id.*

28. Tumlin v. Tuggle Duggins P.A., 15 CVS 9887, 2018 NCBC LEXIS 51, at *1 (N.C. Super. Ct. May 22, 2018).

29. *Id.* at *1–2.

30. *Id.* at *7.

31. *Id.* at *8–11.

32. *Id.* at *16.

33. *Id.* at *18–41.

34. *Id.* at *20–21.

conducted insufficient searches.[35] Lastly, the court concluded that sanctions were not appropriate, reasoning that the defendant did not intentionally "deprive [the plaintiff] of potentially relevant information, nor was there a general abuse of discovery obligations sufficient to support the Court's imposing sanctions."[36] Additionally, the court noted that "all parties should create a detailed [electronically stored information] protocol at the outset of discovery and should strive to be transparent as to how documents will be preserved and what searches will be conducted."[37]

C. Kixsports, LLC v. Munn

In *Kixsports*, another North Carolina Business Court action, the court held that "[t]he deletion of evidence during the pendency of litigation and the continuing failure to preserve evidence in the face of a court order [were] sanctionable under Rule 37" of the North Carolina Rules of Civil Procedure.[38] The trial court ordered the plaintiffs in *Kixsports* to produce its electronic devices for inspection by a forensic expert.[39] The expert "was also authorized to retrieve content associated with various software applications, such as WhatsApp, Slack, Gmail, and similar applications."[40] Soon thereafter, the defendants moved for sanctions on three grounds.[41] First, the defendants contended that the plaintiffs "had repeatedly refused [the expert's] requests for the login credentials for some of the software applications."[42] Second, the plaintiffs' counsel had received potentially privileged documents from the forensic expert but failed to provide a privilege log to the defendants' counsel.[43] Lastly, the defendants "submitted an affidavit from [the expert] opining that [the plaintiffs] had deleted relevant evidence."[44] This sanctions motion was eventually withdrawn, and the defendants reserved their right to refile it later, which they did.[45] When refiling the sanctions motion, the defendants also requested that the plaintiffs be held in contempt.[46]

---

35. *Id.* at *22–25.

36. *Id.* at *45.

37. *Id.* at *44–45.

38. Kixsports, LLC v. Munn, 17 CVS 16373, 2019 NCBC LEXIS 62, at *1, *24–25 (N.C. Super. Ct. Sept. 30, 2019).

39. *Id.* at 5–6.

40. *Id.* at *6.

41. *Id.*

42. *Id.* at *6–7.

43. *Id.* at *7.

44. *Id.*

45. *Id.* at *7–9.

46. *Id.* at *9.

The court in *Kixsports* concluded that it was "more likely than not that [one of the plaintiffs] intentionally deleted backup files for his mobile device during the pendency of the lawsuit."[47] Given the lack of denial or explanation of the deletion by the plaintiffs and the absence of a rebuttal, the court found that the evidence presented by the defendants was consistent with intentional deletion.[48] Additionally, the court concluded that the plaintiffs "either caused or allowed their smartphones to delete messages after the complaint was filed . . . , after [the defendants] requested the communications . . . , [and] after [the defendants] filed their motion to compel.[49] The North Carolina Business Court concluded that it would not be appropriate to strike the plaintiff's pleadings, but given the totality of the circumstances, lesser sanctions were sufficient.[50] The lesser sanctions included: (1) at trial, the court was to "advise the jury regarding [the plaintiffs'] misconduct and to instruct the jury on spoliation of evidence"; (2) "additional discovery [was] needed to ameliorate the loss of evidence"; and (3) the court determined that monetary sanctions were needed "to compensate the defendants for their costs, including reasonable attorneys' fees, incurred in connection with filing" the motion to compel.[51]

D. Out of the Box Developers, LLC v. Logicbit Corp.

This North Carolina Business Court action initially arose when the plaintiff alleged that the defendants stole customizations from the plaintiff's software and incorporated those customizations into a competing case management software.[52] In *Out of the Box Developers*, the parties entered into a "Preservation Agreement" to preserve "any documents, files, program, or other computer-related instrumentalities" that were related to the business at issue.[53] The court ordered that the defendants provide the plaintiff with access to (1) the customized version of the competing program as it was used by a law firm in the past, (2) the customized version of the competing version that the law firm currently used, and (3) the current off-the-shelf version of the competing program.[54]

47. *Id.* at *15.

48. *Id.* at *15–17.

49. *Id.* at *18.

50. *Id.* at *26–27.

51. *Id.* at *27–29.

52. Out of the Box Devs., LLC v. Logicbit Corp., No. 10 CVS 8327, 2013 NCBC LEXIS 32, at *6 (N.C. Super. Ct. June 5, 2013).

53. *Id.*

54. *Id.* at *21.

The plaintiff alleged that the defendants failed to comply with the court order requiring the defendants to provide two of the customized versions and, in response, the plaintiff filed a motion for discovery sanctions and for contempt.[55] The defendants countered that there was never a request for the three versions of the software, and therefore, the defendants did "not have a duty to respond."[56] The court found that there was no justifiable reason why the defendants did not make an adequate effort to comply with the discovery requests; thus, in the absence of demonstrating substantial justifications, the defendants were subject to sanctions under Rule 37 of the North Carolina Rules of Civil Procedure.[57] The court elected to impose "the lesser sanction of taxing costs" but indicated that it would be revisiting the issue should the defendants further fail to comply with the court's directives.[58]

E. OSI Restaurant Partners, LLC v. Oscoda Plastics, Inc.

In *Oscoda Plastics*, the North Carolina Court of Appeals reversed the trial court's imposition of discovery sanctions because the defendant was not given notice that sanctions might be imposed.[59] In discovery, the plaintiffs requested that the defendant produce all documents that were related to the defendant's knowledge of the alleged defects in its flooring.[60] "Following [the plaintiffs'] first motion to compel, [the defendant] indicated that it had certain 'backup tapes' that might potentially contain responsive emails and documents."[61] The trial court subsequently ordered the defendant "to produce 'all responsive, non-privileged documents contained on the backup tapes.'"[62] Next, the defendant filed a motion for reconsideration, in which it contended that recovery of the backup tapes would be too "expensive and time consuming."[63] Following "two orders extending [the defendant's] deadline to produce the backup tapes," the defendant represented that "it was unable to access the documents due to the fact that the backup tapes were encrypted."[64]

---

55. *Id.* at *24.

56. *Id.* at *25.

57. *Id.* at *42–43.

58. *Id.* at *44–45.

59. OSI Rest. Partners, LLC v. Oscoda Plastics, Inc., 831 S.E.2d 386, 387 (N.C. Ct. App. 2019).

60. *Id.* at 388.

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

The trial court entered a spoliation order, "concluding that [the defendant] had 'intentionally encrypted emails and . . . intentionally failed to retain the electronic ability to retrieve the subject emails, with knowledge of their relevance and materiality for this case.'"[65] Shortly thereafter, the defendant produced more than 5,000 pages of documents from its backup tapes, but the plaintiffs filed a second motion to compel, requesting that the defendant "further supplement its document production."[66] Eventually, the defendant produced over 1,000 additional documents, including "highly relevant emails that . . . were not included within the [initial] 5,000 pages that [the defendant] produced."[67] "Based upon its findings of misrepresentations and 'other acts of misconduct,' the trial court concluded that it would 'impose additional sanctions against [the defendant] pursuant to North Carolina Rules of Civil Procedure 37(b)(2) and [the court's] inherent powers.'"[68] The sanctions included striking the defendant's answer and entering default against the defendant as to liability on the plaintiffs' various claims.[69]

On appeal, the defendant argued "that the trial court's order striking its answer as a discovery sanction violated [the defendant's] due process rights."[70] The court of appeals agreed and found that the trial court failed to allow the defendant appropriate notice of the alleged grounds for the imposition of sanctions or the fact that sanctions might be imposed.[71] The court held that "the fact that [the defendant] attempted to defend against [the plaintiff's] request for additional sanctions at the hearing [was] not evidence that" the defendant received proper notice.[72] Thus, due to the lack of notice, "the trial court's order sanctioning [the defendant] by striking its answer" was reversed.[73]

F. Stathum-Ward v. Wal-Mart Stores, Inc.

In *Stathum-Ward*, the North Carolina Court of Appeals considered a situation in which the plaintiff requested a spoliation instruction at the jury

65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.* at 389.
69. *Id.*
70. *Id.*
71. *Id.* at 390.
72. *Id.* at 391.
73. *Id.*

charge conference.[74] Ultimately, the trial court struck the spoliation instruction, but on appeal, the plaintiff asserted "the trial court erred by refusing to give the spoliation instruction because [the] defendants failed to preserve video evidence from [the defendant's] surveillance system."[75] The plaintiff contended that the instruction was justified "because [the] defendants had exclusive control over the video evidence and were put on notice of plaintiff's injury and the potential for litigation."[76] The court in *Stathum-Ward* held that the plaintiff did not provide sufficient evidence "to determine [that] the trial court abused its discretion in denying [the] plaintiff's request for the spoliation jury instruction."[77]

Additionally, the court noted that the video evidence at issue was retained on an in-house server with limited storage capacity.[78] The video stored on this server was "never deleted by anyone, but [was] automatically overwritten as space [was] needed to store new video."[79] At the time of the incident in question, video was retained on the server for forty-five to sixty days. "Thus, video recorded from other parts of the store on the date of the incident was automatically recorded over by later surveillance video."[80]

G. Chesson v. Rives

In this North Carolina Business Court case, the plaintiffs contended that the defendants should have been sanctioned because: "(1) they altered certain documents in connection with an audit; (2) they failed to take appropriate steps to have e-mails that [were] stored on a remote server preserved; and (3) they destroyed a laptop containing potentially relevant information."[81]

As to the first allegation, the plaintiffs "presented evidence detailing that documents kept in the course of an audit . . . were altered after . . . [the defendants] were put on notice of [the] litigation."[82] However, the documents were not irretrievably lost because the track-changes in the relevant documents showed the content before they were altered; thus, the

74. Stathum-Ward v. Wal-Mart Stores, Inc., No. COA18-738, 2019 N.C. App. LEXIS 416, *7 (N.C. Ct. App. May 7, 2019).

75. *Id.* at *8.

76. *Id.*

77. *Id.* at *9.

78. *Id.*

79. *Id.* at *11.

80. *Id.*

81. Chesson v. Rives, No. 12 CVS 3382, 2017 NCBC LEXIS 218, *1 (N.C. Super. Ct. Jan. 18, 2017).

82. *Id.*

court determined, sanctions based on these alterations were not appropriate.[83]

As to the second allegation, the plaintiffs complained that the defendants "maintain[ed] their electronic business records on a server maintained by Thomas Reuters but failed to request that Thomas Reuters preserve relevant e-mails," and as a result, the e-mails were erased by Thomas Reuters after one year.[84] The parties did not dispute that neither the defendants nor plaintiffs "contacted Thomas Reuter to request that documents be preserved"; thus, the court concluded that "neither party should be sanctioned on that basis."[85]

Lastly, as to the third allegation, the plaintiffs claimed that the defendants "did not maintain the laptop used by [the defendant] in the course of conducting the audit and failed to acknowledge that they did not preserve the laptop until four months after the Court ordered its production."[86] The court concluded that the defendants "were not justified in failing to maintain [the laptop]."[87] The court concluded that, "even if [the laptop] or the information stored on it was destroyed through no fault of [the defendants], . . . [the defendants] should have preserved [the laptop] to allow [the plaintiffs] to conduct a forensic examination."[88] Thus, the failure to preserve the laptop entitled the plaintiffs "to a jury instruction for a permissive adverse inference that [the laptop] contained information unfavorable to [the defendants]."[89]

H. Primary Takeaways from These Cases

In sum, we may reasonably conclude the following from just this small survey of North Carolina case law:

1. Forensic examinations of electronically stored information may be warranted when there exists some factual basis to conclude that the responding party has not produced discoverable documents, though such

83. *Id.* at *5.
84. *Id.* at *1–2.
85. *Id.* at *3, *6.
86. *Id.* at *2.
87. *Id.* at *6.
88. *Id.* at *6–7.
89. *Id.* at *7.

examinations must not disclose trade secrets or confidential communications or privileged information.[90]

2. A litigant's "diligent" search of its email servers numerous times and production of responsive, non-privileged emails when appropriate is sufficient to satisfy a party's duties of discovery production under Rules 26(g) and 37(b)(2) of the North Carolina Rules of Civil Procedure.[91]

3. The deletion of discoverable evidence, specifically including electronic communications that a party allows to be deleted from a smartphone, during the pendency of litigation and the continuing failure to preserve evidence in the face of a court order are sanctionable under Rule 37 of the North Carolina Rules of Civil Procedure.[92]

4. Upon receiving a preservation notice or entering into a preservation agreement, a party's failure to preserve all documents, files, or "other computer-related instrumentalities" may be grounds for sanctions under Rule 37 of the North Carolina Rules of Civil Procedure.[93]

5. While the striking of a party's answer without notice may be an excessive sanction, a litigant can be guilty of spoliation of evidence for intentionally encrypting electronic emails and intentionally failing to retain the ability to electronically retrieve the subject communications and produce them in discovery, particularly when the litigant knows the documents may be relevant and material to the case at hand.[94]

6. A party allowing but not intentionally causing evidence to be automatically deleted from an in-house server with limited storage capacity after being retained for forty-five to sixty days is not necessarily guilty of intentional spoliation.[95]

---

90. Crosmun v. Trs. of Fayetteville Tech. Cmty. Coll., 832 S.E.2d 223, 234 (N.C. Ct. App. 2019).

91. Tumlin v. Tuggle Duggins P.A., 15 CVS 9887, 2018 NCBC LEXIS 51, at *21 (N.C. Super. Ct. May 22, 2018); *see also* N.C. R. CIV. P. 26(g), 37(b)(2).

92. Kixsports, LLC v. Munn, 17 CVS 16373, 2019 NCBC LEXIS 62, at *1 (N.C. Super. Ct. Sept. 30, 2019); *see also* N.C. R. CIV. P. 37.

93. Out of the Box Devs., LLC v. Logicbit Corp., No. 10 CVS 8327, 2013 NCBC LEXIS 32, at *4 (N.C. Super. Ct. June 5, 2013); *see also* N.C. R. CIV. P. 37.

94. OSI Rest. Partners, LLC v. Oscoda Plastics, Inc., 831 S.E.2d 386, 387 (N.C. Ct. App. 2019).

95. Stathum-Ward v. Wal-Mart Stores, Inc., No. COA18-738, 2019 N.C. App. LEXIS 416, *10–12 (N.C. Ct. App. May 7, 2019).

7. A litigant who does not take steps to preserve discoverable evidence, including electronically stored information, when on notice of pending or current litigation may be penalized by an instruction for a permissive adverse inference.[96]

III. BOUNDARIES AND SIGNPOSTS: THE NORTH CAROLINA RULES OF PROFESSIONAL CONDUCT AND THE NORTH CAROLINA RULES OF CIVIL PROCEDURE

The Rules of Professional Conduct govern the standards with which lawyers must comport themselves. And the Rules of Civil Procedure provide the standards governing all civil litigation. What—if anything—do these Rules have to say about ephemeral messaging apps? In truth: not much, at least specifically. This is not surprising—as mentioned, this technology is relatively new; the aforementioned Rules are older than those practicing under them, which, for some senior members of this noble profession, is very old indeed. But if we take a closer look at the North Carolina Rules of Professional Conduct and the North Carolina Rules of Civil Procedure, various points of possible intersection with ephemeral messaging apps reveal themselves. Let us now examine these possible points of application and, as above, note the key parameters the Rules might provide to litigants and attorneys using ephemeral messaging apps in this state. Our first source of knowledge in this respect rests in the North Carolina Rules of Professional Conduct and the formal ethics opinions interpreting the same.

Rule 3.4 of the North Carolina Rules of Professional Conduct indicates that, out of "fairness to opposing party and counsel," a "lawyer shall not . . . unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act."[97] Rule 3.4 goes on to note that a lawyer shall not "knowingly disobey or advise a client or any other person to disobey an obligation under the rules of a tribunal, except a lawyer acting in good faith may take appropriate steps to test the validity of such an obligation."[98] Finally, the Rule notes that, "in pretrial procedure," a lawyer is prohibited from "fail[ing] to make a reasonably diligent effort to comply with a legally

96. Chesson v. Rives, No. 12 CVS 3382, 2017 NCBC LEXIS 218, at *7 (N.C. Super. Ct. Jan. 18, 2017).

97. N.C. R. OF PRO. CONDUCT r. 3.4(a) (2020).

98. N.C. R. OF PRO. CONDUCT r. 3.4(c).

proper discovery request by an opposing party," or from "fail[ing] to disclose evidence or information that the lawyer knew, or reasonably should have known, was subject to disclosure under applicable law, rules of procedure or evidence, or court opinions."[99]

The second official comment to this Rule of Professional Conduct elaborates on the discovery implications of this requirement:

> Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for the purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense. Paragraph (a) applies to evidentiary material generally, including computerized information. Applicable law may permit a lawyer to take temporary possession of physical evidence of client crimes for the purpose of conducting a limited examination that will not alter or destroy material characteristics of the evidence. In such a case, applicable law may require the lawyer to turn the evidence over to the police or other prosecuting authority, depending on the circumstances.[100]

The fifth comment to the Rule highlights "that a lawyer must be reasonably diligent in making inquiry of the client, or third party, about information or documents responsive to discovery requests or disclosure requirements arising from statutory law, rules of procedure, or caselaw."[101] The comment then goes on to note that "[r]easonably" generally means acting as "a reasonably prudent and competent lawyer," and that, "[w]hen responding to a discovery request or disclosure requirement, a lawyer must act in good faith."[102] The fifth comment concludes by noting,

> [A] lawyer should impress upon the client the importance of making a thorough search of the client's records and responding honestly. If the lawyer has reason to believe that a client has not been forthcoming, the lawyer may not rely solely upon the client's assertion that the response is truthful or complete.[103]

---

99. N.C. R. OF PRO. CONDUCT r. 3.4(d)(2)–(3).
100. N.C. R. OF PRO. CONDUCT r. 3.4 cmt. 2.
101. N.C. R. OF PRO. CONDUCT r. 3.4 cmt. 5.
102. *Id.*
103. *Id.*

Thus, in summation, the following principles drawn from Rule 3.4 of the Rules of Professional Conduct may implicate the use of ephemeral messaging apps in litigation in North Carolina:

1. Lawyers cannot obstruct an opposing party's access to documents by obfuscating the evidence directly or advising a client to do so.

2. The Rules of Professional Conduct require lawyers to make diligent efforts to obtain and preserve discoverable information and evidence and to comply with discovery directives issued by the courts.

3. It is wrongful for a lawyer to destroy evidence or documents for the purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen.

4. Lawyers have a duty to impress upon clients the importance of being honest, thorough, and forthcoming in producing and preserving records in discovery.

The Ethics Committee of the North Carolina State Bar issued 2014 Formal Ethics Opinion 5 in 2015, and it, too, may provide some possible points of application to the present analysis.[104] The opinion's second hypothetical raises a relevant situation: A "client's legal matter will probably be litigated, although a lawsuit has not been filed. May the lawyer instruct the client to remove postings on social media?"[105] While ephemeral messaging apps are not necessarily "social media," the answer to the inquiry is nonetheless instructive:

> A lawyer may not counsel a client or assist a client to engage in conduct the lawyer knows is criminal or fraudulent. Rule 1.2(d). In addition, a lawyer may not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value. Rule 3.4(a). The lawyer, therefore, should examine the law on preservation of information, spoliation of evidence, and obstruction of justice to determine whether removing existing postings would be a violation of the law.[106]

104. N.C. State Bar, 2014 Formal Ethics Op. 5 (2015) (advising a civil litigation client about social media).

105. *Id.*

106. *Id.*

The opinion notes that, provided various criteria are satisfied, advising a client to remove or delete postings is not necessarily a violation of the North Carolina Rules of Professional Conduct: "If removing postings does not constitute spoliation and is not otherwise illegal, or the removal is done in compliance with the rules and law on preservation and spoliation of evidence, the lawyer may instruct the client to remove existing postings on social media."[107] It is also permissible for the lawyer to "take possession of printed or digital images of the client's postings made for purposes of preservation."[108]

The third hypothetical, in its delightful brevity, provides further points of interest to the present discussion: "May the lawyer instruct the client to change the security and privacy settings on social media pages to the highest level of restricted access? . . . Yes, if doing so is not a violation of law or court order."[109]

Thus, we may conclude the following principles from the advice for 2014 Formal Ethics Opinion 5:

1. A lawyer may be guilty of violating Rule 3.4 of the North Carolina Rules of Professional Conduct if she advises a client to remove or destroy social media posts or other communications that might have evidentiary value in pending or expected litigation.

2. A lawyer may not be guilty of violating Rule 3.4 of the North Carolina Rules of Professional Conduct if she advises a client to restrict access to or increase security features governing certain posts or other communications, provided it is not in violation of law or court order.

But the North Carolina Rules of Professional Conduct do not serve as our only guiding lights in this analysis; the North Carolina Rules of Civil Procedure provide us with, if not the most authoritative guidance, at least the most verbose. Rule 26 of the North Carolina Rules of Civil Procedure provides the "[g]eneral provisions governing discovery."[110]

First, Rule 26 establishes the scope and limits of discovery; pay particular attention to the breadth and depth of permissible discovery and the language regarding electronically stored information:

107. *Id.*
108. *Id.*
109. *Id.*
110. N.C. R. CIV. P. 26.

> 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, electronically stored information, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. It is not ground for objection that the information sought will be inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence nor is it grounds for objection that the examining party has knowledge of the information as to which discovery is sought. For the purposes of these rules regarding discovery, the phrase "electronically stored information" includes reasonably accessible metadata that will enable the discovering party to have the ability to access such information as the date sent, date received, author, and recipients. The phrase does not include other metadata unless the parties agree otherwise or the court orders otherwise upon motion of a party and a showing of good cause for the production of certain metadata.[111]

Furthermore, "metadata" is defined as follows:

> [E]lectronic information that underlies and describes the e-record with which it is associated. Stripped of metadata, an e-record loses vital identifiers and descriptors, resulting in diminished functionality and searchability. With metadata, "vast storehouses" of otherwise unintelligible electronic data can be readily searched, organized, and, in many cases, verified for authenticity and integrity.[112]

The leading expert on the North Carolina Rules of Civil Procedure, G. Gray Wilson, notes:

> [T]he onset of notice pleading, the discovery rules were designed to enable a party to find out what his opponent's case was about. The discovery rules should be liberally construed to accomplish these purposes, and the emphasis of the discovery process should not be on gamesmanship but rather the orderly disclosure of factual information. However valid complaints about the excessive use of discovery may be, the expansive treatment afforded the discoverability of information has not suffered. The spirit of the discovery rules is in harmony with the general philosophy of

111. N.C. R. CIV. P. 26(b)(1).

112. Ben Minegar, *Forging a Balanced Presumption in Favor of Metadata Disclosure Under the Freedom of Information Act*, 16 J. TECH. L. & POL'Y 23, 24 (2015).

> the civil rules that litigation be addressed expeditiously and on the merits rather than by a sporting competition of technicalities.[113]

Moreover, Wilson notes that "Rule 26 [of the North Carolina Rules of Civil Procedure] is essentially the same as its federal counterpart, and federal decisions interpreting this rule are instructive."[114] Rule 26 of the North Carolina Rules of Civil Procedure also indicates "[s]pecific limitations" regarding electronically stored information: "discovery of electronically stored information is subject to the limitations set forth in Rule 34(b)."[115] This limitation thus provides us with a natural segue to the second of the two Rules of Civil Procedure in North Carolina that likely impact litigants' use of ephemeral messaging apps.

Rule 34 of the North Carolina Rules of Civil Procedure governs, among other things, the production of documents and electronically stored information.[116] The statute notes first that

> Any party may serve on any other party a request . . . to produce and permit the party making the request, or someone acting on that party's behalf, to inspect and copy, test, or sample any designated documents, electronically stored information, or tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served[.][117]

The Rule goes on to explain the procedures that apply to producing documents or electronically stored information, noting that parties "must produce documents as they are kept in the usual course of business" and that, if "a request does not specify a form for producing the electronically stored information, a party must produce it in a reasonably usable form or forms."[118]

Once again, for completion, our analysis necessitates consideration of Wilson's editorializations:

> Rule 34 regulates the procedure for the production and inspection of documents and tangible things in all civil actions and proceedings, except where otherwise provided by statute. . . . With one exception, Rule 45 may

113. WILSON, *supra* note 16, at § 26-1 (citations omitted).
114. *Id.*
115. N.C. R. CIV. P. 26(b)(1).
116. N.C. R. CIV. P. 34.
117. N.C. R. CIV. P. 34(a).
118. N.C. R. CIV. P. 34(b)(1)–(2).

> also be used to procure the production of documents from nonparty witnesses or anyone else at a hearing or trial.[119]

Wilson also notes that the Rules:

> [R]equire[] that the documents sought be within the "possession, custody or control" of the party served with the request. Obviously this requires that the documents be in existence, and a party may apply to the court for a document retention order if there is any concern that over the course of the litigation materials may be destroyed by another party either deliberately or in the ordinary course of business. A party may not limit production solely to documents within his physical possession. Any documents to which a party has access and the right to inspect and copy are covered by this rule.[120]

Accordingly, we may faithfully adopt the following key principles from the above North Carolina Rules of Civil Procedure that may impact litigants' uses of ephemeral messaging apps:

1. Parties may seek, through discovery, the production of electronically stored information, including metadata.

2. Parties must produce documents as they are kept in the usual course of business.

IV. WHEN THE RUBBER MEETS THE ROAD: COURTS THAT HAVE CONSIDERED EPHEMERAL MESSAGING APPS

As of the date of publication, the undersigned author knows of no instance wherein a court in North Carolina has considered or ruled on a party's use of ephemeral messaging apps. In fact, it appears very few courts anywhere have dealt with the subject. Thus, the three cases below, taken from various jurisdictions, showcase what may be the only—or at least a large portion—of the instances wherein courts have considered and ruled upon litigants' use of this new technology.

A. Columbia Pictures Industries v. Bunnell

In *Columbia Pictures Industries v. Bunnell*, a case out of the Central District of California, plaintiffs filed a copyright infringement claim against

119. WILSON, *supra* note 16, at § 34-1.

120. *Id.* at § 34-2.

the defendants on February 23, 2006, alleging that the "defendants knowingly enable[d], encourage[d], induce[d], and profit[ed] from massive online piracy of plaintiffs' copyrighted works through the operation of their internet website."[121] The defendants "operate[d] a website known as 'TorrentSpy,' which offer[ed] dot-torrent files for download by users."[122] The defendants' webserver was located in the Netherlands in an attempt to attract users who did not want their identities known.[123]

When a user clicked on a webpage, "the website's web server program receive[d] from the user a request for the page or the file."[124] This "request include[d] the IP address of the user's computer, and the name of the requested page or file, among other things"; that information was copied and stored in RAM, "a form of temporary computer storage."[125] "If the website's logging function [was] enabled, the web server copie[d] the request into a log file, as well as the fact that the requested file was delivered."[126] On the other hand, "[i]f the logging function [was] not enabled, the request [was] not retained."[127] The defendants' web server, Microsoft Internet Information Services, possessed logging functionality, but the defendants' "website's logging function ha[d] not been enabled to retain the Server Log Data."[128] "Although defendants did not affirmatively retain the Server Log Data through logging or other means, the data went through and was temporarily stored in the RAM of defendants' website server for approximately six hours."[129] On May 15, 2006, the plaintiffs sent their one and only preservation request to the defendants that specifically addressed data temporarily stored in RAM.[130] This notice reminded the defendants "of their obligation to preserve all potentially discoverable evidence in their possession, custody or control related to the litigation, including all logs for the TorrentSpy website, and records of all communications between the defendants and users of the website, including instant-messaging and other chat logs," but "[t]his notice did not

121. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at *4 (C.D. Cal. 2007).

122. *Id.* at *9.

123. *Id.* at *11–13.

124. *Id.* at *10.

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.* at *11–12.

129. *Id.* at *13.

130. *Id.* at *16–18.

specifically request that defendants preserve Server Log Data temporarily stored only in RAM."[131]

On March 12, 2007, the plaintiffs filed a motion requesting "that the court issue an order requiring defendants to preserve and produce certain data responsive to plaintiffs' First Request for Production of Documents."[132] The plaintiffs sought production and preservation of "(a) the IP addresses of users of defendants' website who request 'dot-torrent' files; (b) the requests for 'dot-torrent files'; and (c) the dates and times of such requests (collectively 'Server Log Data')" and "evidentiary sanctions against defendants for their alleged spoliation of the Server Log Data."[133] The defendants requested "that the court require plaintiffs to pay reasonable expenses incurred in opposing Plaintiffs' Motion, including attorneys' fees, pursuant to [Federal Rule of Civil Procedure] 37(a)(4)(B)."[134]

Subsequent to the filing of the plaintiffs' motion, the defendants entered into a contract with a third-party entity, Panther.[135] According to the court, after the defendants entered into this contract with Panther, "[r]equests from users who visit[ed] defendants' website for a dot-torrent file on defendants' server [were then] routed from a location not hosted on defendants' server to a Panther server geographically proximate to the users making the requests."[136] As a result, "Panther [then] receive[d] the Server Log Data in issue in its RAM."[137] The defendants argued

> that the Server Log Data [did not] constitute electronically stored information under [Federal Rule of Civil Procedure] 34(a) because the data [had] never been electronically stored on their website or in any medium from which the data [could] be retrieved or examined, or fixed in any tangible form, such as a hard drive.[138]

Importantly, the court held that because the Server Log Data, in this case, was transmitted through and temporarily stored in RAM while the requests of users for dot-torrent files were processed, data in RAM *did* constitute electronically stored information under Rule 34.[139]

131. *Id.*
132. *Id.* at *5.
133. *Id.*
134. *Id.* at *5–6.
135. *Id.* at *14.
136. *Id.* at *14–15.
137. *Id.* at *15.
138. *Id.* at *21–22.
139. *Id.* at *23.

The court noted that, as "Rule 34(a) is limited in its scope to documents and electronically stored information which are in the possession, custody or control of the party upon whom the request is served," the court had to consider whether the Server Log Data was within the scope of Rule 34(a) because the Server Log Data was directed to Panther's RAM, as opposed to the RAM on the defendants' website.[140] The court held that because the defendants had "the ability to manipulate at will how the Server Log Data [was] routed," the data was in defendants' possession, custody, or control.[141] As Rule 34 requires a party to produce only documents that are already in existence, the defendants argued that "because their website ha[d] never recorded or stored Server Log Data since the commencement of the website's operations, requiring defendants to retain such data would be tantamount to requiring them to create a record of the Server Log Data for its production."[142] However, the court held that "because the Server Log Data already exist[ed], [was] temporarily stored in RAM, and [was] controlled by defendants, an order requiring defendants to preserve and produce such data [was] not tantamount to ordering the creation of new data."[143]

In the plaintiffs' motion, the plaintiffs requested that the court issue an order that required the "defendants to preserve the Server Log Data."[144] The defendants objected "on the grounds that the Server Log Data is not subject to any preservation obligation and that requiring such preservation would be unduly burdensome."[145] The court noted:

> In determining whether to issue a preservation order, courts undertake to balance at least three factors: (1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in the absence of an order directing preservation; (2) any irreparable harm likely to result to the party seeking the preservation of the evidence absent an order directing preservation; and (3) the capability of the party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation.[146]

140. *Id.* at *23–25.
141. *Id.* at *25–26.
142. *Id.* at *26.
143. *Id.* at *27.
144. *Id.* at *28.
145. *Id.*
146. *Id.* at *28–29 (citation omitted).

The court held that because the defendants did not "retain and affirmatively object to retention of the Server Log Data, and in light of the key relevance of such data in this action, the first two factors clearly weigh in favor of requiring preservation of the Server Log Data."[147]

The court first considered the potential burden of employing a "technical mechanism through which retention of the Server Log Data in RAM [could] be enabled" and found that employing such a mechanism "would not be an undue burden on defendants."[148]

The court then considered the potential burden of actually retaining and producing the Server Log Data.[149] Addressing the defendants' argument that their server could not handle the volume of data that the Server Log Data would accumulate, the court found that requiring the defendants to preserve and produce solely the Server Log Data at issue would not be an undue burden.[150] The defendants also raised "issues concerning the privacy of their website users based upon defendants' privacy policy, the First Amendment and multiple federal statutes."[151] The court did not find the defendants' arguments persuasive due to the order that directed the defendants to mask users' IP addresses before producing the Server Log Data.[152] Ultimately, the court found that the factors weighed "in favor of requiring defendants to preserve and produce the Server Log Data."[153] The court relied upon

> the key relevance of the Server Log Data to th[e] action, the specificity of the data sought, the lack of alternative means to acquire such information, and the fact that defendants [were] United States individuals and entities who affirmatively chose to locate their server in the Netherlands at least in part to take advantage of the perceived protections afforded by that country's information security law.[154]

The defendants also argued that they should not be required to produce the Server Log Data for the same reasons they believed a preservation order should not be issued.[155] "On a motion to compel discovery, the party from

147. *Id.* at *29.
148. *Id.*
149. *Id.* at *30.
150. *Id.* at *31–32.
151. *Id.* at *32.
152. *Id.* at *36.
153. *Id.* at *50–51.
154. *Id.* at *51.
155. *Id.*

whom electronically stored information is sought must show that the information is not reasonably accessible because of undue burden or cost."[156] The court found:

> (1) [The] defendants . . . failed to demonstrate that the Server Log Data [was] not reasonably accessible because of undue burden or cost; (2) [the] plaintiffs . . . show[ed] good cause to order discovery of such data; (3) the discovery sought [was] not unreasonably cumulative or duplicative or obtainable from some other source that [was] more convenient, less burdensome, or less expensive; (4) [the] plaintiffs ha[d] not otherwise had the opportunity to obtain the data sought; and (5) the burden and expense of the proposed discovery [did] not outweigh its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.[157]

The plaintiffs also requested evidentiary sanctions against the defendants for spoliation of the Server Log Data.[158] However, the court found such sanctions were unnecessary and inappropriate, as the "defendants' failure to retain the Server Log Data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not legally required."[159]

In conclusion, the defendants were ordered to (1) "commence preservation of the Server Log Data" within seven days of the court order and "preserve the Server Log Data for the duration of [the] litigation," (2) produce the Server Log Data no more than two weeks from the court order date and update such production no less frequently than every two weeks, and (3) "preserve the IP addresses of the computers used to request dot-torrent files," but may mask, encrypt, or redact IP addresses.[160]

B. Waymo LLC v. Uber Technologies, Inc.

In this case from the Northern District of California, Waymo LLC commenced a lawsuit on February 23, 2017, against, among other defendants, "Uber Technologies, Inc., and Ottomotto LLC (collectively, "Uber") for misappropriation of eight alleged trade secrets" concerning

156. *Id.* at *51–52 (citing FED. R. CIV. P. 26(b)(2)(B)).
157. *Id.* at *52–53.
158. *Id.* at *53.
159. *Id.* at *55.
160. *Id.* at *56–57.

self-driving technology.[161] Among several other issues, the court considered Uber's use of ephemeral messaging and Waymo's motion for relief due to Uber's alleged spoliation.[162] "Waymo [moved] under both Federal Rule of Civil Procedure 37(e) and the Court's inherent authority for an adverse-inference instruction against Uber on the basis that Uber spoliated evidence."[163] However, because the relevant evidence consisted of electronically stored information, the court ruled that Rule 37(e) was the correct legal standard, not inherent authority, and that potential litigants have a duty to preserve evidence and relevant information when "a reasonable party in the same factual circumstances would have reasonably foreseen litigation."[164] The court noted that "[s]poliation is the destruction or material alteration of evidence or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[165]

The court found "the record clearly [showed] . . . not only that a reasonable party in Uber's circumstances would have reasonably foreseen this litigation in January 2016, but also that Uber *actually* foresaw this litigation in January 2016 when it commenced the process of acquiring Otto."[166] However, Uber claimed that it did not reasonably foresee the litigation in 2016 and therefore did not have a duty to preserve evidence.[167] As proof that Uber reasonably foresaw the litigation beginning in January 2016, the court found: (1) in January 2016, Uber retained litigation counsel for legal advice concerning "potential liability exposure arising out of its planned acquisition of Ottomoto . . . , including for potential claims that could be brought by Waymo specifically";[168] (2) in March 2016, Uber retained Stroz "to perform a due diligence investigation" to aid Uber's litigation counsel;[169] and (3) "the purported joint-defense and common-interest privileges among the parties to the Otto acquisition were an elaborate artifice carefully and meticulously constructed for the purpose

161. Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 U.S. Dist. LEXIS 16020, at *8 (N.D. Cal. Jan. 29, 2018).

162. *Id.* at *49, 69.

163. *Id.* at *49.

164. *Id.* at *49–51 (quoting Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1320 (Fed. Cir. 2011)).

165. *Id.* at *50 (citing Apple Inc. v. Samsung Elec. Co., 888 F. Supp. 2d 976, 989 (N.D. Cal. 2012)).

166. *Id.* at *51 (emphasis removed).

167. *Id.* at *52.

168. *Id.*

169. *Id.* at *53.

of shrouding the acquisition and 'due diligence' process in secrecy."[170] Although Uber argued that these pieces of evidence showed only that "Uber anticipated 'potential litigation,'"[171] the court held that "any reasonable party in Uber's position would have reasonably foreseen litigation from Waymo for trade secret misappropriation related to the defections of Levandowski and other Otto employees."[172] Therefore, Uber's duty to preserve evidence began, at least, in January 2016.[173]

Waymo argued that Uber failed to take reasonable steps to preserve five categories of evidence: (1) "hundreds of text messages among Levandowski, Ron, Kalanick, and Qi [were] deleted"; (2) "Levandowski and Ron also deleted their electronic communications, files, and Slack records"; (3) "Levandowski supposedly destroyed five discs"; (4) "emails and email archives from Tyto LIDAR, LLC, were apparently deleted after its acquisition by Ottomotto"; and (5) "Waymo . . . was denied access to Levandowski's personal laptops."[174] The court rejected Waymo's spoliation argument regarding Levandowski's laptops because Levandowski asserted his Fifth Amendment privilege.[175] With respect to the other four categories of evidence, Uber argued that it should not be sanctioned for spoliation of evidence because "(1) Waymo's motion came too late . . . , (2) the spoliated evidence was irrelevant . . . , and (3) Uber acted in good faith."[176]

First, the court found that "the spoliation issue continued to evolve even *after* Waymo filed its motion with the eleventh-hour discovery of" additional materials and evidence.[177] Second, the court stated that "Uber cannot now evade spoliation by speculating that all of the lost information was benign," and "Uber's unfounded insistence that the evidence it failed to preserve would have been irrelevant does not bar Waymo's request for relief."[178] Regarding spoliation, the court found that Waymo seemed "unwilling or unable to prove its case at trial with qualified witnesses and evidence and [sought] to have the Court fill in the gaps with adverse inferences instead."[179] Because of this, the court reserved the "decision on the question of whether or not Uber spoliated evidence with the intent to

170. *Id.* at *53–54.
171. *Id.* at *54.
172. *Id.* at *55.
173. *Id.*
174. *Id.* at *55–56.
175. *Id.* at *56.
176. *Id.* at *57.
177. *Id.* at *58.
178. *Id.* at *58–60.
179. *Id.* at *61.

deprive another party of its use in litigation, and further [reserved] decision as to whether or not the jury [would] be instructed that it may or must presume the lost information was unfavorable to Uber."[180]

Uber's use of ephemeral messaging apps requires some additional context. The court noted that "Richard Jacobs was a former Uber employee turned 'whistleblower' whose attorney sent Uber a 37-page demand letter dated May 5, 2017, filled with scandalous accusations that led to a jackpot settlement."[181] An "evidentiary hearing unearthed the existence of a resignation email that Jacobs had sent to Uber's leadership on April 14, 2017, further detailing his allegations against Uber, and a subsequent confidential settlement agreement between Jacobs and Uber."[182] "The demand letter, resignation email, and settlement agreement (collectively, 'the Jacobs materials') contained a barrage of scandalous allegations against Uber ranging from deliberate spoliation and systemic abuse of attorney-client privilege to hacking and corporate espionage."[183] The court made three primary conclusions regarding the Jacobs materials and Uber's response thereto.[184]

First, the court agreed that Uber should have produced the Jacobs letter in discovery and that Uber's failure to do so constituted "discovery misconduct."[185] The court ruled that Waymo could present certain instances of Uber's purported "discovery misconduct" to the jury; specifically, Waymo was permitted to inform the jury that Uber withheld the Jacobs letter and explain that the jury may, but need not, draw some adverse inference against Uber based on that withholding.[186] Second, the court ruled that Waymo could adduce certain facts before the jury to show that Uber sought information about the technical details of Waymo's self-driving technology, and, of particular note for our purposes, that "Uber sought to minimize its 'paper trail' by using ephemeral communications."[187] In relevant part, the court held that "Uber's use of ephemeral communications is also relevant as a possible explanation for why Waymo has failed to turn up more evidence of misappropriation in this case."[188] Further, the court held that Waymo would be allowed to "present evidence and argument on this subject at trial, provided that it [could] do so through qualified witnesses

180. *Id.*
181. *Id.* at *62.
182. *Id.* at *12.
183. *Id.*
184. *Id.* at *63.
185. *Id.*
186. *Id.* at *62–63.
187. *Id.* at *63.
188. *Id.* at *69.

and evidence."[189] The court also held that in response, Uber would be allowed to "present its own evidence and argument that its use of ephemeral communications shows no wrongdoing, including by pointing out Waymo's own use of ephemeral communications."[190] Third, the court ruled that the Jacobs materials themselves would be excluded at trial as hearsay unless used to impeach Jacobs.[191]

C. Herzig v. Arkansas Foundation for Medical Care, Inc.

In *Herzig v. Arkansas Foundation for Medical Care, Inc.*, a case out of the Western District of Arkansas, the plaintiffs Brian Herzig and Neal Martin filed age discrimination claims against their previous employer, Arkansas Foundation for Medical Care, Inc. (AFMC), after they were terminated "for repeated misrepresentations to AFMC that the Laserfiche Integration Program was secure and HIPAA-compliant."[192] Herzig was the Director of Information Technology and "was responsible for development, production, and maintenance of AFMC's IT systems and for ensuring compliance with data confidentiality and security policies."[193] Martin was the Assistant Director of Information Technology and "was responsible for application development projects and implementation of programs and applications."[194] In his position, "Martin reported directly to Herzig."[195]

In 2016, AFMC developed an in-house medical necessity review software, ReviewPoint.[196] "ReviewPoint was intended to integrate servers hosting protected health information through a software platform called 'Laserfiche' with customized and default features of a software program called 'Salesforce.'"[197] Herzig, Martin, and other employees of the IT Department were "responsible for the Laserfiche Integration Program, which would allow Salesforce to access the Laserfiche-based protected health information in a way that complied with AFMC's HIPAA obligations to limit and log personnel access to that information."[198] However, in March 2017, employees of AFMC's Business Intelligence Department

189. *Id.*
190. *Id.*
191. *Id.* at *63.
192. Herzig v. Ark. Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 U.S. Dist. LEXIS 111296, at *10–11 (W.D. Ark. July 3, 2019).
193. *Id.* at *4.
194. *Id.* at *5.
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.* at *5–6.

learned of an exploit that could allow "a ReviewPoint user to bypass . . . security and gain unauthorized access to protected health information."[199] During a subsequent review to determine whether any users had used the exploit, another security problem was identified: "Laserfiche was not logging access by users who actually accessed protected health information."[200] After an investigation, Herzig, Martin, and two other employees were terminated "for their contributions to the Laserfiche Integration Program's vulnerabilities and, in Herzig and Martin's case, for repeated misrepresentations to AFMC that the Laserfiche Integration Program was secure and HIPAA-compliant."[201] Herzig and Martin subsequently filed age discrimination claims with the Equal Employment Opportunity Commission against AFMC. [202]

"When the parties conferred pursuant to Federal Rule of Civil Procedure 26(f), they agreed that AFMC might request data from Herzig and Martin's mobile phones and that the parties had taken reasonable measures to preserve potentially discoverable data from alteration or destruction."[203] Herzig and Martin produced screenshots of messages between the two of them dated up to August 20, 2018; however, after litigation began, the two downloaded and communicated on an ephemeral messaging application called Signal.[204] "Signal allows users to send and receive encrypted text messages accessible only to sender and recipient, and to change settings to automatically delete these messages after a short period of time."[205] Herzig and Martin did not disclose these communications until near the end of the discovery period in Herzig's deposition.[206] AFMC filed a motion for dismissal or adverse inference on the basis of spoliation and a motion for summary judgment.[207]

> In its motion for dismissal or adverse inference on the basis of spoliation, AFMC argue[d] that despite Herzig and Martin's duty to impose litigation holds and to update responses to requests for production following their initial and reluctant production of text messages, Herzig and Martin instead

199. *Id.* at *6.
200. *Id.* at *7.
201. *Id.* at *10.
202. *Id.* at *11.
203. *Id.*
204. *Id.* at *12.
205. *Id.* at *12–13.
206. *Id.* at *13.
207. *Id.* at *1.

> intentionally acted to withhold and destroy discoverable evidence by installing and using the Signal application on their mobile devices.[208]

Based on the content of Herzig and Martin's previous communications, reluctance to produce responsive communications, familiarity with information technology, and initial misleading responses, the court agreed that, by downloading and using an ephemeral messaging app, Herzig and Martin withheld and destroyed their communications intentionally and in bad faith.[209] The court stated that this intentional, bad-faith spoliation of evidence warranted a sanction; however, because Herzig and Martin's case was dismissed on the merits, the court did not have to determine what sanction was appropriate.[210]

D. Primary Takeaways from These Cases

In sum, we may reasonably conclude the following from this limited number of cases addressing ephemeral messaging applications:

1. Data stored in RAM constitutes electronically stored information under Rule 34. If a party has the ability to manipulate at will how data is routed, then the court can find that the data is in that party's possession, custody, or control for purposes of Rule 34. If data already exists, is temporarily stored in RAM, and is controlled by a defendant, then an order requiring a defendant to preserve and produce such data is not tantamount to ordering the creation of new data.[211]

2. Courts may find a party's use of ephemeral communications as a possible explanation for why an opposing party lacks evidence. Courts or juries may also conclude that a party engaged in spoliation or made efforts to eliminate a "paper trail" if that party used ephemeral communications after learning about the possibility of litigation.[212]

3. Courts can conclude that, by downloading and using an ephemeral messaging app once litigation has begun, a party may be guilty of

208. *Id.* at *13.

209. *Id.* at *14–15.

210. *Id.* at *15.

211. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at *52–53 (C.D. Cal. 2007).

212. Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 U.S. Dist. LEXIS 16020, at *63, 69 (N.D. Cal. Jan. 29, 2018).

withholding and destroying discoverable communications intentionally and in bad faith.[213]

V. SO, WHAT DO WE DO NOW? PRACTICAL APPLICATION AND SUGGESTIONS

For purposes of symmetry, familiarity, and ease of reading, I had hoped to have only ten guiding principles at this point, but obviously that plan failed. From recent discovery litigation in North Carolina, the North Carolina Rules of Professional Conduct, the North Carolina Rules of Civil Procedure, and the rulings and decisions of other courts regarding ephemeral messaging apps, we may conclude that the following boundaries or signposts may govern the use of ephemeral messaging apps in North Carolina by litigants and attorneys:

1. Forensic examinations of electronically stored information may be warranted when there exists some factual basis to conclude that the responding party has not produced discoverable documents, though such examinations must not disclose trade secrets or confidential communications or privileged information.[214]

2. A litigant's "diligent" search of its email servers numerous times and production of responsive, non-privileged emails when appropriate is sufficient to satisfy a party's duties of discovery production under Rules 26(g) and 37(b)(2) of the North Carolina Rules of Civil Procedure.[215]

3. The deletion of discoverable evidence, specifically including electronic communications that a party allows to be deleted from a smartphone, during the pendency of litigation and the continuing failure to preserve evidence in the face of a court order are sanctionable under Rule 37 of the North Carolina Rules of Civil Procedure.[216]

4. Upon receiving a preservation notice or entering into a preservation agreement, a party's failure to preserve all documents, files, or "other

213. *Herzig*, 2019 U.S. Dist. LEXIS 111296, at *14–15.

214. Crosmun v. Trs. of Fayetteville Tech. Cmty. Coll., 832 S.E.2d 223, 234 (N.C. Ct. App. 2019).

215. Tumlin v. Tuggle Duggins P.A., 15 CVS 9887, 2018 NCBC LEXIS 51, at *1, *18–20 (N.C. Super. Ct. May 22 2018); *see also* N.C. R. CIV. P. 26(g), 37(b)(2).

216. Kixsports, LLC v. Munn, 17 CVS 16373, 2019 NCBC LEXIS 62, at *1, *39 (N.C. Super. Ct. Sept. 30, 2019); *see also* N.C. R. CIV. P. 37.

computer-related instrumentalities" may be grounds for sanctions under Rule 37 of the North Carolina Rules of Civil Procedure.[217]

5. While the striking of a party's answer without notice may be an excessive sanction, a litigant can be guilty of spoliation of evidence for intentionally encrypting electronic emails and intentionally failing to retain the ability to electronically retrieve the subject communications and produce them in discovery, particularly when the litigant knows the documents may be relevant and material to the case at hand.[218]

6. A party allowing but not intentionally causing evidence to be automatically deleted from an in-house server with limited storage capacity after being retained for forty-five to sixty days is not necessarily guilty of intentional spoliation.[219]

7. A litigant who does not take steps to preserve discoverable evidence, including electronically stored information, when on notice of pending or current litigation may be penalized by an instruction for a permissive adverse inference.[220]

8. Lawyers cannot obstruct an opposing party's access to documents by obfuscating the evidence directly or advising a client to do so.[221]

9. The Rules of Professional Conduct require lawyers to make diligent efforts to obtain and preserve discoverable information and evidence and to comply with discovery directives issued by the courts.[222]

10. It is wrongful for a lawyer to destroy evidence or documents for the purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen.[223]

---

217. Out of the Box Devs., LLC v. Logicbit Corp., No. 10 CVS 8327, 2013 NCBC LEXIS 32, at *6 (N.C. Super. Ct. June 5, 2013); *see also* N.C. R. CIV. P. 37.

218. OSI Rest. Partners, LLC v. Oscoda Plastics, Inc., 831 S.E.2d 386, 388 (N.C. App. 2019).

219. Stathum-Ward v. Wal-Mart Stores, Inc., No. COA18-738, 2019 N.C. App. LEXIS 416, *10–12 (N.C. Ct. App. May 7, 2019).

220. Chesson v. Rives, No. 12 CVS 3382, 2017 NCBC LEXIS 218, at *1, *5 (N.C. Super. Ct. Jan. 18, 2017).

221. N.C. R. OF PRO. CONDUCT r. 3.4 (2020).

222. *Id.*

223. *Id.*

11. Lawyers have a duty to impress upon clients the importance of being honest, thorough, and forthcoming in producing and preserving records in discovery.[224]

12. A lawyer may be guilty of violating Rule 3.4 of the North Carolina Rules of Professional Conduct if she advises a client to remove or destroy social media posts or other communications that might have evidentiary value in pending or expected litigation.[225]

13. A lawyer may not be guilty of violating Rule 3.4 of the North Carolina Rules of Professional Conduct if she advises a client to restrict access to or increase security features governing certain posts or other communications, provided it is not in violation of law or court order.[226]

14. Parties may seek, through discovery, the production of electronically stored information, including metadata.[227]

15. Parties must produce documents as they are kept in the usual course of business.[228]

16. Data stored in RAM constitutes electronically stored information under Rule 34. If a party has the ability to manipulate at will how data is routed, then the court can find that the data is in that party's possession, custody, or control for purposes of Rule 34. If data already exists, is temporarily stored in RAM, and is controlled by a defendant, then an order requiring a defendant to preserve and produce such data is not tantamount to ordering the creation of new data.[229]

17. Courts may find a party's use of ephemeral communications as a possible explanation for why an opposing party lacks evidence. Courts or juries may also conclude that a party engaged in spoliation or made efforts

224. *Id.*

225. N.C. State Bar, 2014 Formal Ethics Op. 5 (2015) (advising a civil litigation client about social media); N.C. R. OF PRO. CONDUCT r. 3.4.

226. N.C. State Bar, 2014 Formal Ethics Op. 5 (2015); N.C. R. OF PRO. CONDUCT r. 3.4.

227. N.C. R. CIV. P. 26, 34.

228. *Id.*

229. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at *52–53 (C.D. Cal. 2007).

to eliminate a "paper trail" if that party used ephemeral communications after learning about the possibility of litigation.[230]

18. Courts can conclude that, by downloading and using an ephemeral messaging app once litigation has begun, a party may be guilty of withholding and destroying discoverable communications intentionally and in bad faith.[231]

In light of this, what may we conclude regarding a party's use of ephemeral messaging apps in North Carolina? As with most legal inquiries, it likely depends on the situation, the litigants, the attorneys, the courts, or the facts of the individual case, including, particularly, how and when the apps are used and by whom. But as that answer makes for a poor conclusion—and even worse legal analysis—the more helpful method is likely to consider various hypotheticals and apply what we have learned to the individual situations, hopefully not only to predict how North Carolina courts *might* treat ephemeral messaging apps, but also to examine how North Carolina courts *should* treat them.

A. Hypothetical One

Mr. Johnson and his neighbor, Jake, often argue over Jake's interactions with Mr. Johnson's wife, Ellie. Mr. Johnson's jealousies are well-founded: Jake and Ellie regularly send each other private text messages regarding their ongoing romantic relationship. Upon discovering only a select few of the amorous text messages between his spouse and his neighbor, Mr. Johnson made plain to all his determination to hire an attorney and file suit against Jake for alienation of affection. Ellie, smarter than the lot of them, suggested to Jake that they download and begin using an ephemeral messaging app to discuss, among other things, their continued romantic feelings for each other and their determined efforts to defeat Mr. Johnson in court. Once litigation based on Mr. Johnson's alienation of affection claim began, Mr. Johnson's attorney sent Jake and Ellie a preservation notice. During their respective depositions, Jake and Ellie unsuccessfully hid the fact that they used an ephemeral messaging app to communicate with each other. Jake and Ellie claim, through counsel, however, that they started using the app well before suit was actually filed and thus cannot be guilty of spoliation and that it would be wrongful of the

230. Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 U.S. Dist. LEXIS 16020, at *63, 69 (N.C. Cal. Jan. 29, 2018).

231. Herzig v. Ark. Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 U.S. Dist. LEXIS 111296, at *10 (W.D. Ark. July 3, 2019).

court to instruct the jury to draw any negative inferences from their use of the app. Mr. Johnson's attorney claims that there are two sets of communications that Jake and Ellie have spoliated: (1) those exchanged after Mr. Johnson declared his intent to file suit but before Mr. Johnson had actually filed his suit and (2) those exchanged after suit was filed and a preservation notice was sent.

How should a North Carolina court rule? Based on what we know from recent discovery litigation in North Carolina, the North Carolina Rules of Professional Conduct, the North Carolina Rules of Civil Procedure, and the rulings and decisions of other courts regarding ephemeral messaging apps, a North Carolina court should rule that (a) a forensic examination of Jake and Ellie's phones would be appropriate to determine if, when, and to what extent they used an ephemeral messaging app; (b) Jake and Ellie spoliated both sets of communications and thus are subject to sanctions; and (c) an instruction to the jury that it be permitted to draw any negative inferences from Jake and Ellie's use of the app would be appropriate.

First, there is no doubt that the communications are discoverable: parties may seek, through discovery, the production of electronically stored information, including metadata.[232] Second, we know from the holding in *Crosmun v. Treasurers of Fayetteville Technical Community College*, that forensic examinations of electronically stored information, like the communications between Jake and Ellie—or the lack thereof—may be warranted when there exists some factual basis to conclude that the responding party has not produced or has destroyed discoverable documents.[233] Moreover, the deletion of evidence, specifically including electronic communications like the text exchanges between Jake and Ellie on the ephemeral messaging app, during the pendency of litigation is sanctionable under Rule 37 of the North Carolina Rules of Civil Procedure.[234]

Furthermore, since Jake and Ellie deleted communications by using the ephemeral messaging app both after they were aware of the likelihood of litigation and after receiving the preservation notice from Mr. Johnson, they are guilty of spoliation as it concerns both sets of communications. The holding in *Chesson v. Rives* makes it clear that a litigant who does not take steps to preserve discoverable evidence when on notice of pending litigation may be penalized by an instruction for a permissive adverse

232. N.C. R. CIV. P. 26, 34.

233. Crosmun v. Trs. of Fayetteville Tech. Cmty. Coll., 832 S.E.2d 223, 239 (N.C. Ct. App. 2019).

234. Kixsports, LLC v. Munn, 17 CVS 16373, 2019 NCBC LEXIS 62, at *23 (N.C. Super. Ct. Sept. 30, 2019).

inference.[235] Additionally, pursuant to the court's analysis in *Out of the Box Developers, LLC v. Logicbit Corp.*, upon receiving the preservation notice from Mr. Johnson, Jake and Ellie had a duty to preserve all documents, files, or "other computer-related instrumentalities"; their failure to do so is grounds for sanctions under Rule 37 of the North Carolina Rules of Civil Procedure. Moreover, if the court analyzes the facts of Jake and Ellie's situation like the court did in *Herzig v. Arkansas Foundation for Medical Care, Inc.*, the court could conclude that, by downloading and using an ephemeral messaging app once litigation had begun, Jake and Ellie were guilty of withholding and destroying discoverable communications intentionally and in bad faith.[236]

When considering what sanction might be appropriate, the court should find the holding in *OSI Restaurant Partners, LLC v. Oscoda Plastics, Inc.* instructive. While the striking of Jake or Ellie's answer without notice may be an excessive sanction, the court would have grounds to find that Jake and Ellie spoliated evidence by intentionally encrypting electronic communications between them, thereby intentionally failing to retain the ability to electronically retrieve the subject communications, particularly since Jake and Ellie knew the documents may be relevant and material to the case at hand and nonetheless chose to use an ephemeral messaging app anyway.[237] The court would also be justified in finding that Jake and Ellie's use of the ephemeral messaging app explains why Mr. Johnson lacks more evidence to support his alienation of affection claim and instruct the jury accordingly.[238]

B. Hypothetical Two

Janey, a college student, entered into a contract to purchase a horse from Clara, in exchange for Janey completing work on Clara's ranch. Janey completed the work as contracted, but Clara refused to provide her the horse. Janey sued Clara for breach of contract. Janey then began exchanging text messages and emails with Lorie, a disgruntled former employee of Clara's, in an effort to obtain inside information to use against Clara in the litigation. The text messages were exchanged first via normal

235. Chesson v. Rives, No. 12 CVS 3382, 2017 NCBC LEXIS 218, at *1 (N.C. Super. Ct. Jan. 18, 2017).

236. Herzig v. Ark. Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 U.S. Dist. LEXIS 111296, at *10 (W.D. Ark. July 3, 2019).

237. OSI Rest. Partners, LLC v. Oscoda Plastics, Inc., 831 S.E.2d 386, 387 (N.C. App. 2019).

238. Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 U.S. Dist. LEXIS 16020, at *8 (N.C. Cal. Jan. 29, 2018).

text messaging on Janey's and Lorie's phones, but then later via an ephemeral messaging app; the emails were exchanged via a student email service from Janey's college. Text messages sent through the normal channels on Janey's and Lorie's phones were originally saved on the phones' RAM, but once they downloaded and began using the ephemeral messaging app, the messages never made it to the phones' RAM storage and were, instead, immediately deleted after being read by the recipient. The emails, even deleted ones, were saved in the usual course of business on an in-house server at the college but were, unbeknownst to Janey and Lorie, only kept for sixty days before being automatically deleted by school administrators to save storage capacity.

In discovery, Janey admitted to communicating with Lorie via her student email and via an ephemeral messaging app. Upon Clara's request, Janey had the servers holding her student emails searched three times; several emails between Janey and Lorie were found, but none older than sixty days, as the emails older than sixty days had been deleted from the servers. Janey refused to produce any text messages, claiming that requiring her to produce those prior to her using the ephemeral messaging app would be a requirement that she create new data and that those exchanged via the ephemeral messaging app no longer existed. Janey produced the emails she found, but Clara claims, through counsel, that Janey is guilty of spoliation as it concerned the emails older than sixty days and the text messages exchanged via the ephemeral messaging app. Clara also claims that Janey's refusal to produce the text messages exchanged prior to her using the ephemeral messaging app is wrongful.

How should a North Carolina court rule? Once again, based on what we know from the rules and relevant case law, a North Carolina court should rule that (a) Janey is not guilty of spoliation as it concerns the emails automatically deleted after sixty days from the student-email server; (b) Janey was right to produce the emails kept on the email server that were still there, and her searches of the server for them were adequate; (c) Janey is guilty of spoliation as it concerns the text messages she exchanged with Lorie via the ephemeral messaging app once litigation began; and (d) Janey must produce the text messages exchanged prior to her using the ephemeral messaging app.

First, there is no doubt that the communications are discoverable: parties may seek, through discovery, the production of electronically stored information, including metadata.[239] Moreover, Janey's diligent searches of her student-email servers numerous times and production of the responsive, non-privileged emails are sufficient to satisfy Janey's duties of discovery

239. N.C. R. CIV. P. 26, 34.

production under Rules 26(g) and 37(b)(2) of the North Carolina Rules of Civil Procedure.[240] She had a duty to produce the emails, as they were kept in the usual course of business.[241] Janey is not guilty of intentional spoliation by passively and unknowingly allowing the emails older than sixty days to be automatically deleted from her college's in-house server due to limited storage capacity.[242]

However, by allowing her text messages with Lorie to be immediately deleted by using an ephemeral messaging app rather than stored on RAM on the phone, Janey is guilty of intentional spoliation; moreover, since the data stored in RAM constitutes electronically stored information under Rule 34, the court would be justified in finding that the data is in Janey's possession, custody, or control for purposes of Rule 34 and thus must be produced.[243] If data already exists, is temporarily stored in RAM, and is controlled by a defendant, then an order requiring a defendant to preserve and produce such data is not tantamount to ordering the creation of new data.[244]

C. Hypothetical Three

Mr. Deets and Newt entered into a business venture together to sell beef cattle to the United States military. Newt, being what folks call a "close trader," took what Mr. Deets believed was more than his fair share of the profits of a recent sale. Mr. Deets hired a locally renowned cattle attorney, Mr. Wilbarger, to represent him in a lawsuit against Newt. Mr. Deets informed Mr. Wilbarger that he was regularly texting with a member of the military regarding the sale and the pending lawsuit. Mr. Wilbarger suggested that Mr. Deets stop texting through normal channels and begin texting only through an ephemeral messaging app. Mr. Wilbarger also instructed Mr. Deets to delete a public social media post wherein Mr. Deets bragged about the money he made from the sale in question. Mr. Deets and Newt eventually settled their dispute to everyone's satisfaction and are now much better friends and cattle traders; Mr. Wilbarger's actions, however, drew the ire of the court. Eventually, the court issued an order to show

240. Tumlin v. Tuggle Duggins P.A., 15 CVS 9887, 2018 NCBC LEXIS 51, at *24 (N.C. Super. Ct. May 22 2018).

241. N.C. R. CIV. P. 26, 34.

242. Stathum-Ward v. Wal-Mart Stores, Inc., No. COA18-738, 2019 N.C. App. LEXIS 416, *10–12 (N.C. Ct. App. May 7, 2019).

243. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at *4 (C.D. Cal. 2007).

244. *Id.*

cause, requiring Mr. Wilbarger to show the court why he should not be disciplined for violating the North Carolina Rules of Professional Conduct.

How should a North Carolina court rule? Based on what we know from the aforementioned Rules and relevant case law, a North Carolina court should rule that by suggesting that Mr. Deets use an ephemeral messaging app and delete relevant social media posts, Mr. Wilbarger obstructed Newt's access to discoverable communications in violation of Rule 3.4 of the North Carolina Rules of Professional Conduct.

Rule 3.4 clearly prohibits lawyers from obstructing an opposing party's access to documents by directly obfuscating the evidence or advising a client to do so.[245] The Rule also requires that lawyers make diligent efforts to obtain and preserve discoverable information and evidence; by advising his client to use an ephemeral messaging app and thus cause his messages to be automatically deleted, Mr. Wilbarger did not make appropriate efforts to protect discoverable evidence and, in fact, took deliberate steps to obstruct Newt's access to those communications.[246] Finally, by advising Mr. Deets to remove or destroy social media posts that have evidentiary value in the pending litigation with Newt, Mr. Wilbarer further violated Rule 3.4.[247]

VANISHING ACTS AND A BRAVE NEW WORLD: A CONCLUSION

Neil Postman notes that cultures that use tools "may have many tools or few, may be enthusiastic about tools or contemptuous."[248] But the mere fact that we use tools sets us apart: it makes us a "tool-using culture." "The name 'tool-using culture' derives from the relationship in a given culture between tools and the belief system or ideology. The tools are not intruders. They are integrated into the culture in ways that do not pose significant contradictions to its world-view."[249] In other words, the tools our society creates are not divorced from our culture; they are extensions of it.

What then does this new tool—ephemeral messaging apps—say about our culture? We have spent far too many words to conclude simply that such tools are wrong and should not be used; indeed, there are many contexts, even in litigation, where their use would be far from wrong and are, in fact, beneficial. For example, an attorney communicating with his

245. N.C. R. OF PRO. CONDUCT r. 3.4 (2020).

246. *Id.*

247. N.C. State Bar, 2014 Formal Ethics Op. 5 (2015) (advising a civil litigation client about social media); *see also* N.C. R. OF PRO. CONDUCT r. 3.4.

248. POSTMAN, *supra* note 1, at 25.

249. *Id.*

client about a pending case may use an ephemeral messaging app with confidence, knowing that such privileged communications are not being recorded or saved in some way to be used against his client later. Or individuals not in litigation or even anticipating litigation may use an ephemeral messaging app to protect personal conversations, trade secrets, patented information, or simply mundane conversations they prefer not be heard or read later by anyone else. In short, the societal and cultural concerns of privacy and secrecy—the very concerns ephemeral messaging apps are designed to serve—are legitimate and worth protecting, and ephemeral messaging apps are a brilliant new tool to accomplish as much. But litigants and lawyers in North Carolina must use them, like any other arrow in the litigation quiver, appropriately and in accordance with the well-established words comprising the North Carolina Rules of Civil Procedure and the North Carolina Rules of Professional Conduct. Those words, at least, will not disappear anytime soon.