DISAPPEARING DATA

AGNIESZKA MCPEAK*

"Ephemeral" applications like Snapchat facilitate social interaction in a format that mimics the impermanence of face-to-face conversations. In the age of "big data" and the growing privacy concerns it raises, platforms offering ephemeral social media tools are meeting a market demand for smaller digital footprints. Additionally, these platforms are responding to regulatory pressure to embrace "privacy by design," the idea that new technology should be built with privacy as a goal from the ground up. Indeed, ephemeral platforms, though imperfect in their impermanence, mark a positive shift in the direction of data minimization.

But the Federal Rules of Civil Procedure provide for broad discovery of electronically stored information. And they mandate, along with other rules, preservation of potentially relevant data in anticipation of litigation. Preservation duties for this new brand of ephemeral data, however, have not been clearly defined.

This article urges for a fair and balanced approach to defining preservation duties for disappearing data. While ephemeral content may be discoverable, onerous preservation duties are unwarranted and will negatively impact both corporate and individual litigants alike. For corporate interests, overly broad preservation duties lead to risk-averse companies stockpiling all things digital, often at great cost. For individuals, the law should recognize that mobile technology has become ubiquitous and social media is a key tool for personal expression, free speech, and social interaction. But individuals also have become the unwitting stewards of vast amounts of data, some of which is dynamic and ever-changing. Deletion or revision of personal information is a normal occurrence on social media platforms—indeed, some are a product of privacy by design. Overly broad preservation duties for individual litigants thus impose unwarranted burdens and are out of step with technological change.

Introduction 18
I. The Shift to Disappearing Data..... 23
A. Privacy by Design as an Important Industry Goal 25
B. Dynamic Social Media Functionality and Ephemeral Content 29
1. Social Media as Non-Static Data 30

* Associate Professor, University of Toledo College of Law. Special thanks to the hosts and participants at Marquette University Law School's Fourth Annual Junior Faculty Works-in-Progress Conference, the Ohio Legal Scholarship Workshop, Chapman University Fowler School of Law's Junior Faculty Works-in-Progress Conference, and Duquesne University School of Law's Junior #FutureLaw Conference, and particularly to Chad Oldfather, Bruce Boyden, Marisa Cianciarulo, Ernesto Hernandez, Jacob Rooksby, and Seth Oranburg for their commentary. I appreciate early input on this project from the Ohio State University Moritz College of Law faculty at their Summer Workshop Series, the participants in the Junior Scholars Virtual Colloquium, and the University of Toledo College of Law faculty.

2. Self-Destructing and Ephemeral Applications 32
II. ESI Exceptionalism 39
A. Defining ESI 40
1. Accessible ESI 41
2. Inaccessible ESI 42
B. The Scope of ESI Discovery 44
1. Social Data Discovery 46
2. Discovery of Transitory, "Ephemeral" Content 48
III. Preservation and Spoliation 49
A. Preservation Duties Under Federal Rules of Civil Procedure 51
1. Evolution of Spoliation Safe Harbors 52
2. Examples of ESI Spoliation 55
B. Legal Ethics Rules 61
IV. Toward a Balanced Approach to Disappearing Data 64
A. Fairness for Individual Litigants 66
B. Balancing Concerns as to Corporate Litigants 68
Conclusion 71

INTRODUCTION

Civil discovery is struggling to cope with the new realities of how we use technology to create—or avoid creating—digital records. Currently, technology companies are shifting to offer products that minimize data creation and retention. The concept of "privacy by design,"[1] and the use of behavioral interventions,[2] in particular, have

1. The term "privacy by design" was first coined by Ann Cavoukian, the Ontario Privacy Commissioner. *See* Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391, 418 (2014) (describing the boom of "privacy by design" as a policymaking trend in the US and European Union); *see also* Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 390 (2013) (crediting Dr. Ann Cavoukian as the originator of the privacy by design movement); Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 264 (2017) (noting that Dr. Ann Cavoukian "first introduced the 'foundational principles' of [privacy by design] in the mid-1990s."); Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1411–12 (2011) (describing privacy by design as "a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture.").

2. Behavioral interventions are design cues that steer users to certain conduct and can be used to promote privacy-protecting activities within a platform. *See* Hartzog & Stutzman, *supra* note 1, at 411–12. Hartzog and Stutzman draw on the work of Richard Thaler and Cass Sunstein, which examined the idea of "nudging" people to make better choices through the way choices are presented. *Id.* (citing RICHARD H.

led to privacy safeguards being incorporated into the very design of new technology.[3] Privacy by design is a positive development and an important industry goal that is responding to consumer demands in the technology marketplace.[4] But as more technology products offer privacy through ephemeral content that is not archived in any meaningful way—what is effectively "disappearing data"—civil discovery rules have to grapple with the challenges created by shrinking digital footprints.

The proliferation of ephemeral apps, like Snapchat,[5] signals that disappearing data will become more common as a fundamental design feature of new platforms. And other social media platforms, like Facebook, already include user control settings that allow for changes and deletion of past content, so that editing older content has become a normal practice for users.[6] Quite simply, social media platforms and similar new technology no longer produce a static archive of data. Rather, social data is dynamic, ever-changing, and increasingly ephemeral.

But in the litigation context, vast retention has become the norm, resulting in dramatic cost increases and uncertainty as to preservation

THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008)). "Nudging" then encourages certain conduct without mandating it. *Id.*

3. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1284 (1998).

4. For example, the Federal Trade Commission has urged industry actors to embrace privacy by design and to move swiftly with its implementation of new features and products. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES & POLICYMAKERS vii (2012) [hereinafter FTC Final Report], [https://perma.cc/TK9B-X9BL]. The FTC Final Report describes privacy by design in the context of principles that call for "[c]ompanies [to] incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy." *Id.*

5. Snapchat is a leading social media application known for its self-destruct default for images, video, and messages sent via the platform. *See Our Approach to Privacy*, SNAP INC., [https://perma.cc/GC25-J5R8]. It is intentionally designed to offer more privacy and less of a permanent digital record than other social media platforms. *See* Larry Magid, *What Is Snapchat and Why Do Kids Love It and Parents Fear It? (Updated)*, FORBES (May 1, 2013, 4:14 PM), [https://perma.cc/NL64-8KCC] (author notes that CEO Evan Spiegel told him he designed Snapchat to offer more privacy than Facebook). Apps like Snapchat are growing in popularity: nearly a quarter of all adult Smartphone users use messaging apps that automatically delete messages. SHANNON GREENWOOD, ANDREW PERRIN & MAEVE DUGGAN, SOCIAL MEDIA UPDATE 2016 11 (2016), [https://perma.cc/QHM8-4F9B].

6. For example, Facebook users can go back and edit previously posted content. *See How Do I Edit a Post I've Shared?*, FACEBOOK, [https://perma.cc/FDM7-SAAZ].

duties.[7] Over-preservation of digital content, expansive litigation holds, and fear of sanctions fuel corporate hoarding of all things digital.[8] These practices occur as a risk-averse reaction to the discovery norms established through the Federal Rules of Civil Procedure, but are inconsistent with the realities of technological change. Thus, the Federal Rules, and the courts applying them, should take into account the reality of how we use technology and how future technological innovation will revolutionize data retention and storage.

Fortunately, recent amendments to the Federal Rules, particularly the new safe harbors for good-faith deletion of electronically stored information ("ESI") under Rule 37,[9] are moving in the right direction. And courts interpreting and applying discovery rules should strive to find fairness for litigants when examining spoliation concerns for ephemeral content. With a balanced approach that accepts the realities of reduced digital footprints, the law can be less onerous for corporate litigants who face the costs and challenges of over-preservation in uncertain technological times.[10] And this approach promotes fairness to the individual litigant,[11] who has become the unwitting steward of vast

7. *See, e.g.*, John H. Beisner, *Discovering a Better Way: The Need for Effective Civil Litigation Reform*, 60 DUKE L.J. 547, 550 (2010) (discussing the overwhelming cost and impact of electronic discovery in litigation).

8. *See* Kenneth J. Withers, *Risk Aversion, Risk Management, and the "Overpreservation" Problem in Electronic Discovery*, 64 S.C. L. REV. 537, 544 (2013) [hereinafter *Risk Aversion*].

9. Rule 37(e) addresses spoliation of electronically stored content. FED. R. CIV. P. 37(e). It was amended in 2015 and now provides two options for courts dealing with the spoliation of evidence. *See id.* First, if the party "acted with the *intent* to deprive another party of the information's use in the litigation," the court can make a presumption that the destroyed evidence was unfavorable to the party who caused the spoliation. *Id.* (emphasis added). The court then can instruct the jury to make such a presumption or dismiss the case altogether. *Id.* If the party did not act with intent, there must be a showing of prejudice made. *Id.* If prejudice exists, the court can take remedial measures that must be "no greater than necessary to cure the prejudice." *Id.* Rule 37(e) is often referred to as a safe harbor provision, protecting litigants from spoliation sanctions if its provisions are met. *See, e.g.*, Alexander Nourse Gross, Note, *A Safe Harbor from Spoliation Sanctions: Can an Amended Federal Rule of Civil Procedure 37(e) Protect Producing Parties?*, 2015 COLUM. BUS. L. REV. 705, 708.

10. *Risk Aversion*, *supra* note 8, at 578–81.

11. While corporate concerns are certainly relevant, some scholars note that recent amendments to the Federal Rules overwhelmingly take into account the needs of corporate litigants, which often overlook the unique issues affecting individual litigants. *See, e.g.*, Stephen B. Burbank, *Pleading and the Dilemmas of "General Rules,"* 2009 WIS. L. REV. 535, 562–63; Brooke D. Coleman, *One Percent Procedure*, 91 WASH. L. REV. 1005, 1008–09 (2016); *but see* Steven S. Gensler, *Judicial Case Management: Caught in the Crossfire*, 60 DUKE L.J. 669, 699 (2010) (describing how the rules can be flexible to address needs of smaller cases and analyzing different theories for customizing rules or their application).

archives of data through their personal use of technology like social media.

The need for a balanced approach to preservation of ephemeral content is supported by three distinct concerns. First, civil discovery rules should accept the industry trend towards privacy by design and behavioral interventions meant to increase user privacy. Not only is technology evolving to respond to consumer demands for more privacy, privacy by design and industry self-regulation are important aspects of how United States privacy law currently functions. Civil discovery rules should accept the fact that technology now facilitates new forms of communication that are essentially the equivalent of in-person or telephonic conversation—for which no traditional, physical record need be maintained in most cases.

Second, as to corporate litigants, the civil discovery rules already recognize that ESI is different in scope and character than traditional, physical records. Routine, good-faith deletion of ESI is a necessary business practice within companies. Additionally, the 2015 revisions to the Federal Rules shift towards proportionality and greater cooperation,[12] both of which seek to minimize overly intrusive discovery. Further, new safe harbors in the 2015 revisions to Rule 37 also seek to simplify and clarify spoliation. This trend of reducing the vastness of discovery and preservation should continue even further when dealing with disappearing data. In particular, courts should resist the urge to expect preservation where no record was created, or where a record existed in a transitory and ephemeral form only.[13] At the same time, however, preservation does require record retention in certain cases and for certain industries.[14] Use of ephemeral apps to transform business records into disappearing data should be scrutinized.

12. *See, e.g.*, FED. R. CIV. P. 26 (proportionality factors moved up in Rule 26 following 2015 revisions); Steven S. Gensler, *Some Thoughts on the Lawyer's E-volving Duties in Discovery*, 36 N. KY. L. REV. 521, 567 (2009) (noting the call for adding emphasis on cooperation and proportionality to the Federal Rules).

13. *See, e.g.*, *Quinby v. WestLB AG*, No. 04Civ. 7406(WBP)(HBP), 2005 WL 3453908, at *8 n.10 (S.D.N.Y. 2005) (companies have no duty to store electronically stored information in accessible formats).

14. *E.g.*, Home Mortgage Disclosure Act of 1975, 12 U.S.C. §§ 2801, 2803 (1976) (rules mandate five-year retention period for certain information about mortgage loans); Health Insurance Portability and Accountability Act, 45 C.F.R. pt. 164 (2017) ("security rule" mandates creation and retention of certain records); FDIC Record Retention Requirements, 12 C.F.R. § 380.14 (2017) (noting that companies need internal policies that conform to regulators' requirements for document retention); Records to Be Kept by Employers, 29 C.F.R. pt. 516 (1993) (outlining specific retention requirements for human resource records, payroll forms, tax records, and other employee file contents).

Nonetheless, corporate litigants as a general rule should not be forced to over-preserve, particularly in light of technological realities.

Third, individuals and their rights are best protected by a balanced approach that accepts the realities of disappearing data. Technology, such as social media apps, plays an important role in how individuals interact with the world and each other, and is a key avenue of self-expression.[15] Yet individuals rarely implement personal document retention policies or think of themselves as stewards of vast data archives. While preservation duties certainly apply to individuals on many levels, onerous application of rules to individuals is unwarranted and unfair.[16]

Thus, this Article urges courts to adopt a balanced and fair approach to preservation of disappearing data. Under this approach, disappearing data should fall within the scope of discovery, but it generally does not need to be preserved due to its fleeting nature. This approach is supported by the trend of privacy by design, the growth of ephemeral applications, the over-preservation problem for corporate litigants, and the realities of how individuals use technology in their personal lives. Part II of this article outlines the technological shift from vast data collection to disappearing data as a fundamental design principle. In Part III, it addresses the exceptionalism of ESI discovery and why this particular category of information must be treated differently than traditional documents in civil discovery. Part IV explores preservation duties and spoliation, including the evolution of the Federal Rules and preservation principles in legal ethics rules. Part V proposes a fair and balanced approach to defining preservation duties in the age of disappearing data.

15. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017) ("While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves; and define who we want to be.").

16. My prior work explores other aspects of social media in civil litigation, including how courts should handle the scope of social media discovery, see Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887 (2013) [hereinafter *The Facebook Digital Footprint*], the ethical constraints of informal social media discovery, see Agnieszka McPeak, *Social Media Snooping and its Ethical Bounds*, 46 ARIZ. ST. L.J. 845 (2014), and an analysis of how the proportionality factors should be applied to limit discovery of social media content, Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235 (2015) [hereinafter *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*].

I. THE SHIFT TO DISAPPEARING DATA

According to some scholars, the world is in the midst of a "big data revolution."[17] From the rise of the microprocessor in the 1970s to the internet boom in the 1990s, the second half of the twentieth century saw a sharp increase in the volume of information stored in electronic format.[18] Now, the volume of data created continues to increase at unfathomable rates, fueled by cheaper storage options and the ubiquity of electronic devices.[19] And in the last decade, social media[20] and smartphones[21] have caused an explosion in the amount of electronic

17. *See, e.g.*, Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 397 (2014). *See also* Gil Press, *A Very Short History of Big Data*, FORBES (May 9, 2013, 9:45 AM), [https://perma.cc/4ZPE-X8UJ]. *Cf.* Meg Leta Ambrose, *Lessons from the Avalanche of Numbers: Big Data in Historical Perspective*, 11 I/S: J.L. & POL'Y INFO. SOC'Y 201 (2015).

18. *See supra* note 17.

19. *See* Richards & King, *supra* note 17, at 398–401 (explaining how data quantity is increasing "at breakneck pace" and how smartphones, wearable technology, and cloud computing are facilitating big data growth). *See generally* Ambrose, *supra* note 17, at 222–24 (cataloguing big data and the evolution of the computer age from the early 1800s to today).

20. According to the 2016 Social Media Update by Pew Research Center, a vast majority of adults use social media: 79 percent of online adults, or 68 percent of all adults, use Facebook. GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 4. Even in the 2012 report, over 60 percent of online adults used Facebook. *Id.* at 2. The 2016 trends show that users turn to Facebook for more than mere socializing and use it for news and political campaign updates. Jeffrey Gottfried et al., *The 2016 Presidential Campaign – A News Event That's Hard to Miss*, PEW RES. CTR. (Feb. 4, 2016), [https://perma.cc/V69T-H5DX] (although cable news was cited as the "most helpful" source of news for all adults, about one-third of adults under age 30 cited social media as the most helpful source for political news). Additionally, older users seem to be joining social media sites. GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 4–5. When broken down by demographic, the results show the greatest increase in Facebook usage among those age 65 or older. *Compare id.*, *with* Maeve Duggan & Joanna Brenner, *Social Networking Site Users*, PEW RES. CTR. (Feb. 14, 2013), [https://perma.cc/6228-2XBA]. Of all adults who use Facebook, three quarters of them use it daily. GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 3. Social media users tend to use more than one platform. *Id.* at 10 (reporting that more than half of online adults who use social media use multiple sites). While Facebook remains the leading social network, about a quarter to one third of online adults use Twitter, Pinterest, Instagram, or LinkedIn. *Id.*

21. Smartphone use by adults is on the rise, with 72 percent using a smartphone in 2016. *Compare* GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 11, *with* LEE RAINIE, SMARTPHONE OWNERSHIP UPDATE: SEPTEMBER 2012 1–2 (2012), [https://perma.cc/U5QZ-8KU4]. With smartphones, users have access to popular messaging apps like WhatsApp. *See About WhatsApp*, WHATSAPP, [https://perma.cc/7HSJ-JV7W]. Additionally, a quarter of smartphone owners use self-destruct apps like Snapchat and Wickr. GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 11. Lastly, a small percentage of smartphone owners used anonymous chat apps like YikYak or Whisper in 2016. *Id.*; *see* Jefferson Graham, *Yik Yak, the Once Popular and*

information amassed by private companies, often for advertising purposes[22] (as some say, if a product is free, this means you are the product).[23] Businesses too have shifted to largely electronic forms of communication and document management.[24] Without a doubt, the modern digital age is an era in which everyone has a digital footprint, and the vastness of "big data" is unprecedented.

But as this new digital landscape continues to evolve, businesses and individuals are feeling the challenges of living in a digital world. Privacy has been a key issue as technology tracks physical movements, online activity, and personal lives.[25] Businesses also grapple with the

Controversial College Messaging App, Shuts Down, USA TODAY (April 28, 2017, 7:53 PM), [https://perma.cc/DC2E-CEF5] (noting that Yik Yak was a top-downloaded app in 2013 but was forced to close after declining use, mismanagement, and campus bans); *About Whisper*, WHISPER, [https://perma.cc/Y7NK-E73G] ("Whisper is a leading media company based in Venice, California. Whisper's mobile app is the largest online platform where people share real thoughts and feelings, forge relationships and engage in conversations on an endless variety of topics - without identities or profiles. Whisper content and stories reach hundreds of millions of people each month across platforms. Whisper is spearheading a movement that believes that happiness starts with being your real self.").

22. Brian Naylor, *Firms are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016, 4:51 PM), [https://web.archive.org/web/20180222191606/https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it].

23. The origins of this phrase are debatable, but in 1973 artist Richard Serra created a short film, "Television Delivers People," which contained the text: "The Product of Television, Commercial Television, is the Audience. Television delivers people to an advertiser. . . . You are consumed. You are the product of television. Television delivers people." Videotape: Richard Serra & Carlota Fay Schoolman, *Television Delivers People*, *in* PERSISTENCE OF VISION – VOLUME 1: MONITORING THE MEDIA (1987). A blogger named Andrew Lewis has been credited with coining the phrase "If you're not paying for it . . . you're the product . . . ." *See* Andrew Lewis, blue_beetle's profile, METAFILTER, [https://perma.cc/2F3D-47RL]; *see also* Andrew Lewis (@andlewis), TWITTER (Sept. 13, 2010, 6:01 AM), [https://perma.cc/VDT3-M433]; *see also* Scott Goodson, *If You're Not Paying for It, You Become the Product*, FORBES (Mar. 5, 2012, 12:34 PM), [https://perma.cc/5BNP-GCKG] (noting that the title quote is borrowed from a MetaFilter post); Jason Fitzpatrick, *If You're Not Paying for It; You're the Product*, LIFEHACKER (Nov. 23, 2010, 9:30 AM), [https://perma.cc/2LGC-B5LZ] (crediting Andrew Lewis' post on MetaFilter as the origin of the phrase).

24. *See generally Risk Aversion*, *supra* note 8, at 539, 541.

25. While debates continue about the degree to which consumers willingly abandon their own privacy by participating in social media, users at least tend to manage and prune their account contents to limit the scope of what they disclose. *See* MARY MADDEN, PRIVACY MANAGEMENT ON SOCIAL MEDIA SITES 2 (2012), [https://perma.cc/SC4P-W2H5]. As of 2012, the majority of social media users restricted access to their postings via platform privacy settings and unfriended people at some point. *Id.* at 2–3. Notably, half of social media users also noted "some difficulty in managing privacy controls . . . ." *Id.* at 3. Users also seem to be aware of the

sheer volume of records now created through word processing, email, and other electronic systems.[26] While technology has become commonplace,[27] the full scope of privacy concerns and data management challenges are becoming more pronounced.

As a result of big data challenges, some companies are evolving in the other direction: to create less long-lasting data. Indeed, data minimization and other privacy-by-design features are being encouraged as modes of industry self-regulation by the Federal Trade Commission (FTC) and other regulatory bodies. As companies adapt to new privacy norms, technology will continue to shift towards disappearing data.

This Section discusses the industry shift to: (A) privacy-by-design, including behavioral interventions, and (B) dynamic social media accounts and ephemeral apps. Both of these developments are valuable for allowing companies to manage data and empowering consumers to minimize their digital footprints, even though it means fewer records are created and stored.

A. Privacy by Design as an Important Industry Goal

Privacy by design is technology principles that allows companies to minimize privacy harm and security risks.[28] It requires companies to treat privacy as both a value and a foundational design goal, so that new systems are built with privacy protection in mind.[29] In essence, privacy by design is a way for companies to think proactively about privacy from the onset, rather than dealing with privacy as an afterthought.[30]

---

potential ramifications of social media posts, as eleven percent of all social media users claim to regret posting something in the past. *Id.*

26. *See Risk Aversion*, *supra* note 8, at 539.

27. Given the wide use of smart phones today among adults, more individuals now have access to the internet from their mobile devices. *See* GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 11 (noting that seventy-two percent of adults use a smartphone). And social media is now a major part of online activity, as one out of every five minutes online is spent on social media platforms. *See* COMSCORE, 2016 U.S. CROSS-PLATFORM FUTURE IN FOCUS 29 (2016), [https://perma.cc/Q7P3-BLSE] ("Social Networking leads all categories in engagement, account for 1 out of 5 minutes spent online. The strength of this category, along with Email and IM [instant messaging], highlights that one of digital's primary functions is for communication – now more so than ever with the rise of mobile.").

28. *See* Tene, *supra* note 1, at 418 and accompanying text.

29. *See* Hartzog & Stutzman, *supra* note 1, at 390–91; Rubinstein, *supra* note 1, at 1421.

30. *See* Hartzog & Stutzman, *supra* note 1, at 390.

Scholars have identified several principles that should guide technological design. These include companies recognizing privacy concerns early on, defining and applying "spheres of privacy protection" as a core principle, mitigating privacy concerns throughout the entire lifecycle of data, and respecting the privacy rights of users.[31]

Although privacy by design is a relatively new approach to handling information privacy in the digital age, it is an important facet of industry self-regulation in the United States. The FTC, the agency taking the lead on privacy enforcement in the United States, issued a report that emphasizes privacy by design as an important aspiration for technology companies that handle consumer data.[32] The report is intended to function as a framework for industry best practices in the collection and use of data.[33] It notes that the tech industry as a whole needs to improve its practices and move faster with implementing recommendations for privacy-by-design frameworks.[34] To facilitate industry action, the report focuses on five key items: (1) implementing an effective "Do Not Track" system; (2) improving disclosures and privacy with respect to mobile services; (3) increasing transparency and regulation of data brokers; (4) addressing privacy concerns relating to large platform providers (like social media and browsers); (5) and creating a code of conduct that is sector-specific.[35] Additionally, the report identifies simplified consumer choice and transparency in data practices as additional, important principles.[36]

Along with the FTC, the Department of Commerce also started a privacy initiative that resulted in a White Paper on consumer privacy.[37] That white paper also includes privacy by design as a goal. In Europe, the General Data Protection Regulation (GDPR) will mandate privacy by design as one of many consumer protection features, and United

31. *See id.* at 390–91; *see* Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles*, PRIVACY BY DESIGN (Aug. 2009), [https://perma.cc/582E-RSZD]. Dr. Covoukian lists seven Fair Information Principles which should guide companies' approach to designing new technologies. *See id.* Others have criticized privacy by design because of challenges with implementing comprehensive privacy protection measures across an organization and within all facets of technological design. Hartzog & Stutzman, *supra* note 1, at 392 (citing Rubinstein, *supra* note 1, at 1421 ("Privacy by design is an amorphous concept.")). Further, enforcement of privacy by design as a regulatory tool can be problematic. *See* Hartzog & Stutzman, *supra* note 1, at 392 (citing Rubinstein, *supra* note 1, at 1444–53).

32. *See* FTC Final Report, *supra* note 4 and accompanying text.

33. FTC Final Report, *supra* note 4, at iii.

34. *Id.* at iv–v.

35. *Id.* at v–vi.

36. *Id.* at vii–viii.

37. *Id.* at 3.

States companies will likely meet the higher standards of the GDPR in order to participate in the global marketplace.[38]

Notably, the FTC Final Report seeks to shift the burdens of protecting privacy from the consumers (and onerous—or perhaps dubious—consumer choice models) to the businesses that collect, store, and use consumer data.[39] Individual consumers should no longer be expected to weed through privacy policies and employ measures to block tracking and other privacy invasions.[40] Instead, companies should minimize the use of invasive technology.[41] Some techniques companies can use include minimizing the data collected in the first place, deleting data after a period of time, anonomyzing data, and promoting security through encryption.[42]

The framework of privacy by design is particularly important as a tool for designing better social media platforms. But privacy by design becomes difficult to implement in the social media context due to the core role personal information plays in social networking. Social interactions online necessarily require disclosure and transfer of personal information, which raises unique and broad privacy concerns.[43] Like with other technology innovations that deal with personal data, social media platforms should look to fundamental design-based solutions to privacy issues from the onset of a platform's creation, rather than as a reactive measure.[44] These designs, however, need to take into account "front end" privacy protections: ways to add privacy protection on the user-facing portion of the application.[45] Examples here include "privacy settings, search visibility, password protections, and the ability to use pseudonyms."[46]

38. *See* European Parliament & Council Regulations 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 25, 2016 O.J. (L 119) 48.

39. FTC Final Report, *supra* note 4, at 23.

40. *Id.* at 23–24.

41. *Id.* at 23.

42. *Id.*; *see also* Hartzog & Stutzman, *supra* note 1, at 387–88 (noting that some of these privacy technologies are tools on the "back end" that enable better data practices by technologies); *see also* Rubinstein, *supra* note 1, at 1411–12 (noting that Privacy Enhancing Technologies [PETs], like anonymity, are narrow, singular tools often added as an afterthought by designers. Privacy by design, by contrast, includes a systematic, proactive approach to embedding privacy protection into the very architecture of the system).

43. Hartzog & Stutzman, *supra* note 1, at 387.

44. *Id.* at 387, 389.

45. *Id.* at 387–88.

46. *Id.* at 388.

Some scholars suggest thinking of privacy by design in social networks as "obscurity by design."[47] "Privacy" is a complicated concept that seemingly contradicts the "social" element of social networking, and the concept of obscurity can be more informative for designing data-minimizing social media platforms.[48] Thus, companies should focus on obscurity (and not just privacy) principles such as restricting front-end access to content, reducing the ability to identify users, and reducing the clarity of information.[49] These obscurity principles can be implemented on the front end of design through technologies that hide or restrict content,[50] policies that enable users to choose obscurity,[51] and behavioral interventions that "encourage obscurity-friendly practices" by users.[52]

Behavioral interventions, in particular, focus on influencing user behavior through design. Subtle aspects of a platform's design can influence users to make choices that increase their privacy.[53] Thus, if privacy is a foundational value, designers can build features that steer users to choosing privacy over disclosure.[54] In this way, social media platforms can include features that promote privacy, and design them in a way that makes users more likely to utilize them.

Default settings, feedback mechanisms, and signal or language choices are important design decisions that influence user behavior.[55] The default settings send a message to users about the expected use of the platform; they "can even be seen as an implicit endorsement from the default setter that the settings are desirable."[56] Additionally, users may not bother changing default settings, due to inertia or what some call "status quo bias."[57] Choices as to feedback given to the user also

47. *Id.*

48. *See id.*

49. *Id.* at 397–401.

50. *See id.* at 403–07. Examples here include access walls and smart hyperlinks that limit who can view content, privacy settings that enable users to self-select limited audiences for content, search blockers that prevent indexing for search engines, de-identification tools like face-blurring to counter facial recognition technology, and password and encryption tools to "restrict outsider access and thus raise the transactional cost of finding information." *Id.* at 407.

51. *See id.* at 407–11. Examples here include using policies that allow pseudonyms, preventing scraping by other sites, restricting user behavior, and setting community guidelines of user behavior. *Id.*

52. *Id.* at 411–12.

53. *See supra* note 2 and accompanying text.

54. *See* Hartzog & Stutzman, *supra* note 1, at 412.

55. *Id.* at 412–18.

56. *Id.* at 412.

57. *Id.* at 412–13 (citing William Samuelson & Richard Zeckhauser, *Status Quo Bias in Decision Making*, 1 J. RISK & UNCERTAINTY 7 (1988)).

influence user behavior.[58] Feedback includes notice and other information a user gets while interacting on the platform.[59] It can mean showing a reminder about the audience size before a user posts something or letting a user see a report of what data is collected or who looked at it.[60] Other language and signal choices matter as well. For example, privacy policy pop-up reminders at the moment before a disclosure of personal information can be more effective than merely burying privacy information in a hard-to-locate policy.[61] And the language used to frame a privacy choice also influences user decisions. Framing a user choice as one that reminds them of the privacy they are losing may inspire them to choose greater privacy protection.[62]

Privacy by design is an important development in self-regulation of technology and in protecting user privacy. By proactively addressing privacy concerns from the beginning—in the very design of the system itself—platforms can function in ways that promote privacy. And through design decisions, platforms can enable, or even influence, users to act in ways that minimize disclosure of personal information. New designs are seeking to reduce data collection, storage, and use, which will result in less personal information being revealed and stored on both the back end and front end of platform design. In the context of social media, privacy by design and user preference have inevitably led to platforms that archive little, if any, personal information. For other social media platforms, accounts may still store personal information, but they take on a dynamic character that enables changes, edits, or deletions to pieces of older data. These unique features of social media are important to understand before analyzing preservation, spoliation, and discoverability of content.

B. Dynamic Social Media Functionality and Ephemeral Content

Social media, in general, is not designed to function primarily as an archive or cloud storage tool. Rather, social media accounts are live, dynamic programs that exist to facilitate ongoing interactions with others. And the newest social media platforms demonstrate a market and consumer shift to less data retention. But these features and trends have a profound effect on the discovery of content. This Section

58. Hartzog & Stutzman, *supra* note 1, at 413.

59. *Id.*

60. *Id.* at 413–14 (citing M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012)). Examples include a web browser showing users a report of web history it collected under its privacy policy or a social network displaying a list of who clicked on a profile. *Id.*

61. *Id.* at 415–16.

62. *Id.* at 417.

explains (1) how social media produces a non-static data set and (2) the ways ephemeral applications reduce digital footprints.

1. SOCIAL MEDIA AS NON-STATIC DATA

Most social media accounts enable, or even encourage, users to add, edit, and take away content regularly. When Facebook users create personal Timelines or Pages, they can continue to add new posts,[63] comment on other posts,[64] change privacy settings that affect the visibility of posts,[65] and edit their contacts and associations.[66] While some features of social media function more like email, such as Facebook's Messenger,[67] other aspects such as account settings and personal updates continue to change and morph over time.

Much of the ongoing activity on a social media account stem from the "social" nature of social media itself. A picture on Facebook may continually get new comments, have new tags added to it,[68] be visible to a different audience,[69] or become visible to only the account-holder.[70] That particular Facebook photo becomes more like a real-time conversation than an archived photograph due to the very nature and purpose of social media. Notably, past posts remain live and can be altered.[71] A user can edit the text or content of a past post.[72] Privacy

63. *See How Do I Post to my Timeline?*, FACEBOOK, [https://perma.cc/WXP2-GGKA] ("Your timeline is where you can see your own posts or posts you've been tagged in displayed by date . . . [y]ou can post to your timeline either from the top of your timeline or from News Feed . . .").

64. *See How Do I Comment on Something I See on Facebook?*, FACEBOOK, [https://perma.cc/37Q5-FC4T].

65. *See Profile & Timeline Privacy*, FACEBOOK, [https://perma.cc/35PT-CPB7] (describing user privacy settings for Facebook Timeline).

66. *See How Do I Unfriend or Remove a Friend?*, [https://perma.cc/52GT-U2NA].

67. *See Sending a Message*, FACEBOOK, [https://perma.cc/6FVE-NT9W].

68. *See Tagging*, [https://perma.cc/9KQ6-5XAH].

69. *See What Audiences Can I Choose From When I Share?*, FACEBOOK, [https://perma.cc/54JQ-WYL6].

70. *Id.*

71. Notably, the Pew Research Center found in 2012 that more and more users engage in "profile pruning" in which they delete friends, comments, posts, and tags: "[a]ll users have become more likely to delete comments on their profiles over time, but this is especially true of young adults. It is now the case that 56% of all social media users ages 18-29 say they have deleted comments that others have made on their profile . . ." *See* MADDEN, *supra* note 25, at 9.

72. Facebook users can edit posts even after they have been shared. *See How do I Edit a Post I've Shared?*, FACEBOOK, [https://perma.cc/7444-M665].

settings for an individual post can be edited after posting, as well.[73] The location of a post can be removed or altered.[74] The user who commented on a post can edit or delete that comment later.[75] Users can even backdate a post to make it appear in the past on a Page.[76]

Social media content is created in large part by the user intentionally. But a social media account also contains "back-end" data that goes beyond that which the user affirmatively posts.[77] Facebook, for example, tracks IP addresses used to log into an account, dates and times of active sessions, facial recognition software data, and targeted ad topics that are assigned to the account.[78] These categories of information are also stored as part of the account data.[79] Back-end data may be more static in some ways, but it is also being added to continuously.[80]

Account deactivation and total deletion are also possible in social media accounts. In Facebook, users can deactivate their accounts, an option that may preserve the account contents while making the account no longer live.[81] Users can even delete the entire account altogether, an affirmative act that effectively deletes the entire account.[82] Facebook does offer a "download" feature that enables users to receive a file of all of their account contents.[83]

All of these features give the user a degree of control over some aspect of the account and enables changes and deletions. In this way, social media accounts do not remain fixed in time as a static data set. Rather, they are dynamic and ever-changing. At the same time,

73. *See Can I Limit Who Can See My Past Posts*, FACEBOOK, [https://perma.cc/6CPD-KDH4]. Facebook even has special tips for dealing with a breakup and seeing less of someone in your past posts. *See How Do I Take a Break from Someone on Facebook?*, FACEBOOK, [https://perma.cc/DVA2-WC5F].

74. *See How Do I Edit or Remove My Location on a Post?*, FACEBOOK, [https://perma.cc/2LBY-NSL2].

75. *See How do I Delete or Edit my Comment Below a Post?*, FACEBOOK, [https://perma.cc/FYP9-SPWL].

76. *See How Do I Change a Post's Date or Backdate a Post so that it Appears in the Past on my Page?*, FACEBOOK, [https://perma.cc/NRN9-RYQL] (notably, the back-dating feature only works in Facebook Pages and not on Timelines).

77. *See Accessing Your Facebook Data*, FACEBOOK, [https://perma.cc/933N-JYQ6].

78. *See id*. (listing what is included within a user's downloadable Facebook account).

79. *See id*.

80. *See id*. Ad topics, for example, may change or expand over time based on users' activities. *Id.*

81. *What's the Difference Between Deactivating and Deleting My Account?*, FACEBOOK, [https://perma.cc/76Y8-4UZS].

82. *Id*.

83. *See Downloading Your Info*, FACEBOOK, [https://perma.cc/9HW7-4XNA].

however, the back-end data collection and front-end permanence of social media posts have spawned a new type of social media platform: the ephemeral application.

2. SELF-DESTRUCTING AND EPHEMERAL APPLICATIONS

The latest trend in social media is self-destruct or "ephemeral" apps like Snapchat and Confide. Unlike Facebook, Snapchat was designed with user privacy as a key feature.[84] It is similar to other social media platforms in that it permits users to send texts (called "Chats"),[85] and images or video (collectively known as "Snaps")[86] within the app to a self-selected audience.[87] But Snapchat is unique because users can set the front-end lifespan for their content,[88] enabling the recipient to see a message from a few seconds to "infinity."[89] But once the allotted time runs out or the recipient closes the message, it disappears from view.[90] Snapchat also allows Stories that are visible to all Snap Friends for twenty-four hours.[91]

According to its privacy policy, Snapchat appears to embody privacy by design as a core value.[92] Its emphasis on disappearing content is meant to set it apart from other social media platforms:

> From the beginning, the way we treat your information has been very different from other technology companies. We don't stockpile your private communication, and we don't show your friends an ongoing history of everything you've ever posted. We believe that this approach makes the

84. Magid, *supra* note 5 (noting that CEO Evan Spiegel told him he designed Snapchat to offer more privacy than Facebook).

85. *About Chat*, SNAPCHAT, [https://perma.cc/N2MG-9QYD]. (explaining how a one-on-one Chat disappears once both parties leave the Chat and explaining how voice and video Chats are also possible).

86. *Create a Snap*, SNAPCHAT, [https://perma.cc/ESB7-N3ZW] (explaining what a Snap is).

87. Magid, *supra* note 5.

88. *Id.*

89. Snapchat recently added "infinity" as a setting for Snaps. *See Limitless Snaps*, SNAP INC. (May 9, 2017), [https://perma.cc/XS37-J8G9]. Infinity means the Snap does not disappear until the recipient closes it. Thus, the message still self-destructs, but can be viewed for a longer duration when first opened. *Id.*

90. *Id.*

91. *Add to My Story*, SNAPCHAT, [https://perma.cc/R3H4-QULW]. The default audience for Stories is the user's entire Friend list. *Change Your Privacy Settings*, SNAPCHAT, [https://perma.cc/48QD-SKCU].

92. *Your Privacy Matters*, SNAP INC., [https://perma.cc/XXL8-TMK8].

> Snapchat app feel less like a permanent record, and more like a conversation with friends.[93]

Through its policies and design, Snapchat attempts to provide the benefits of live social interaction without the detriments of a digital record. It represents a shift away from social media that archives and collects personal information to one that encourages a smaller digital footprint.

Notably, however, Snapchat allows for some storing of content by users and incentivizes frequent sharing.[94] For a front-end way for users to save their own content, Snapchat added its "Memories" feature, which lets users store Snaps they created in the app[95] and on the phone's camera roll.[96] In the Memories feature, users also can save their own Snaps as "My Eyes Only."[97] Snaps saved in this way will not show up when swiping through Memories and instead require a passcode to view.[98] At the same time, recipients of Snaps can circumvent the auto-delete function by taking a screenshot of others' content they receive.[99] While Snapchat does not block a recipient's ability to take a screenshot of a Snap,[100] it provides notice to the sender when a screenshot was taken.[101] Also, Snapchat warns users on its website that screenshots or other capture software can circumvent the auto-delete function.[102] Chats can also be saved if the recipient holds down on the Chat.[103]

---

93. *Id.*

94. *About Memories*, SNAPCHAT, [https://perma.cc/4G26-3WXT].

95. *Id.*

96. *Id.*

97. *How to Use My Eyes Only,* SNAPCHAT, [https://perma.cc/4WET-XCBH] ("If you ever get a Snap that you want to keep extra private, you can always add it to My Eyes Only! That way, you can hand over your phone to friends when sharing Memories, without being worried they might catch an eyeful of something meant just for you [see-no-evil monkey emoji].")

98. *Id.*

99. A screenshot is a picture of the contents of a smartphone's screen. *See* Magid, *supra* note 5 (describing how screen capture is possible in Snapchat).

100. *See id.*

101. *See Friends Screen Icon Guide*, SNAPCHAT, [https://perma.cc/3B5S-QXX9] (explaining the icons that show a screenshot has been taken of a Snap with or without audio, or of a Chat message).

102. *See, e.g.*, *When Does Snapchat Delete Snaps and Chats*, SNAPCHAT, [https://perma.cc/SS2Q-P9QE] ("Snapchatters who see your messages can always potentially save them, whether by taking a screenshot or by using some other image-capture technology (whether that be a separate piece of software, or even simply taking a photo of their screen with a second camera)."). Notably, technology exists to prevent recipients from taking a screenshot, but Snapchat has not incorporated such a function into its app. *See, e.g.*, Carmel DeAmicis, *This Company Invented a Weird Trick to Stop*

From a behavioral intervention standpoint, Snapchat steers users to share images and videos in a seemingly intimate environment. For example, when a user opens the app, the home screen of the app is the camera function.[104] A key function within Snapchat is the use of Filters, which allows users to add multiple overlays to their images.[105] Lenses also allow "real-time special effects and sounds" to be added to images.[106] Snap, Inc., the maker of Snapchat, even describes itself as a "camera company."[107] It is clear that Snapchat promotes the use of images and videos over mere text.

Further, users are encouraged to earn trophies for trying Snapchat features or using the app frequently.[108] Examples of trophies include the Ogre for sending 1,000 Snaps using the "selfie" front-facing mode on your camera, the Moon for sending 50 Snaps using night mode, the Frypan for sending a Snap between 4:00 AM and 5:00 AM, and the Happy Devil for screenshotting a Snap.[109] Snapchat also assigns users a score based on how many Snaps they send or receive, the number of Stories they post, and other metrics.[110] In these ways, Snapchat is designed to encourage frequent and image-heavy social interactions among its users. Its self-destruct default is a front-end feature that greatly minimizes users' digital footprints, but it may also incentivize the frequent and more intimate use of the app.[111]

Even though Snapchat encourages frequent and image-heavy social interaction, on the back end, Snapchat strives to make deletion its default.[112] Like all social media platforms, Snapchat collects and stores

People from Taking Ephemeral Message Screenshots, GIGAOM (Oct. 30, 2014, 12:24 PM), [https://perma.cc/7AU8-FLXY].

103. *See When Does Snapchat Delete Snaps and Chats*, *supra* note 102.

104. *Capture a Snap*, SNAPCHAT, [https://perma.cc/K3LT-TJVN] ("[S]napchat opens right to the camera, just tap the camera button to take a photo . . . .").

105. *Add a Filter*, SNAPCHAT, [https://perma.cc/3A63-MPHY].

106. *Face Lenses & World Lenses*, SNAPCHAT, [https://perma.cc/KUZ4-9QPX].

107. *Snap, Inc.*, SNAP INC., [https://perma.cc/WH5A-C438] ("Snap Inc. is a camera company. We believe that reinventing the camera represents our greatest opportunity to improve the way people live and communicate.").

108. *Trophies*, SNAPCHAT, [https://perma.cc/A9A3-QPCU] ("Trophies help mark special achievements you've earned by using Snapchat in special ways. You can earn them by earning a certain Score, using certain Filters, sending creative Snaps, and more!").

109. *Id.*

110. *See My Score*, SNAPCHAT, [https://perma.cc/9TVB-SGAZ].

111. One of the concerns with Snapchat is its use for "sexting," which is sending sexual or nude images or videos. Magid, *supra* note 5.

112. *When Does Snapchat Delete Snaps and Chats?*, *supra* note 102.

user profile information and metrics about usage habits.[113] These aspects of a user's Snapchat account can be downloaded by the user.[114] But the substance of the communications themselves are not saved. According to Snapchat, it designed its servers to immediately and automatically delete previously viewed Snaps.[115] For unopened individual Snaps, auto-deletion occurs after thirty days.[116] Group Chat Snaps that are unopened also delete automatically after twenty-four hours.[117] Chats are also automatically deleted.[118] For one-on-one Chats, auto-deletion occurs after both parties have viewed the Chat and closed the Chat screen.[119] Group Chats delete after twenty-four hours, even if not viewed by everyone in the Group.[120] For content shared to all Friends using the My Story feature, Snapchat deletes data after twenty-four hours, or earlier if the user deletes the content.[121] Thus, Snapchat's data storage practices appear to parallel the user's front-end decisions about the lifespan of content.

But digital crumbs nonetheless may linger. Even though Snapchat does not store Snap content on its own servers, the device itself may contain some Snapchat records.[122] As the company explains on its blog, a user's Snap is uploaded to Snapchat's servers when it is created, and the selected recipient gets a notification of the Snap.[123] When the user opens the message, a file is placed in a temporary folder, which could be "internal memory, RAM or external memory like an SD Card—depending on the platform and whether it's a video or a picture."[124] Once the Snap is viewed, the temporary file on the device is meant to be deleted quickly:

113. Snapchat collects information on usage, such as filters used, persons communicated with, and frequency of interactions; content of messages, such as metadata and whether the recipient viewed a Snap; log-in history; device information, such as type of hardware, device identifiers, and mobile phone data. *Privacy Policy*, SNAP INC., [https://perma.cc/4SRF-56SG]. Snapchat also collects location information and may use cookies or similar technology. *Id.* It shares some user information with third parties, like advertisers. *Id.*

114. *Download My Data*, SNAPCHAT, [https://perma.cc/A9XD-SUZ4].

115. *When Does Snapchat Delete Snaps and Chats?, supra* note 102.

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

120. *Id.*

121. *Id.*

122. *How Snaps are Stored and Deleted*, SNAP INC. (May 9, 2013), [https://perma.cc/93S4-QSGS].

123. *Id.*

124. *Id.*

> After a snap has been opened, the temporary copy of it is deleted from the device's storage. We try to make this happen immediately, sometimes it might take a minute or two. The files are deleted by sending a "delete" instruction to the phone's file system. This is the normal way that things are usually deleted on computers and phones—we don't do anything special (like "wiping").[125]

Additionally, Snapchat discourages attempts to circumvent the app to access Snaps. It reminds users that "rooting" or "jailbreaking" goes against the warranty for many phones.[126] And it also notes that forensic tools may allow for retrieval of some deleted data, joking that users should "keep that in mind before putting any state secrets in your selfies :)."[127]

The fact that some Snapchat content can be accessed despite auto-deletion has been a point of controversy. The ability for forensic examiners to unearth deleted Snaps made headlines in 2013, when a Utah-based company discovered deleted Snapchat files on an Android device.[128] An examiner was able to download an Android's phone data using forensics software.[129] He then removed the ".NoMedia" file extension from a Snapchat file and was able to view the content.[130] The examiner noted that the files were sought as evidence in divorce and a missing teenager case.[131] Others have had some success accessing deleted Snapchat files on iOS devices.[132]

Snapchat's representations about its data practices led to a complaint by the FTC for deceptive trade practices that resulted in a final settlement order. The FTC alleged that Snapchat made false and misleading representations by stating that messages "disappear forever"

125. *Id.*

126. *Id.* (noting that recipients should just take a screenshot or photo with a second camera to save a Snap within the app instead of trying to access files on the device directly).

127. *Id.*

128. Kashmir Hill, *Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos from Android Phones*, FORBES (May 9, 2013, 4:51 PM), [https://perma.cc/7S73-SV5W].

129. *Id.*

130. *Id.*

131. *Id.*; *see also* Trent Leavitt, *Snapchat Unveiled: An Examination of Snapchat on Android Devices*, DECIPHER FORENSICS (Jan. 23, 2014), [https://perma.cc/QW84-MW2X].

132. *See, e.g.*, Katie Notopoulos, *How Anybody Can Secretly Save Your Snapchat Videos Forever*, BUZZFEED NEWS (Dec. 27, 2012, 6:22 PM), [https://perma.cc/X6MX-LH9J].

and that users will get notified if a screenshot was taken.[133] The Complaint notes all the ways "deleted" content was unencrypted and could still be accessed on devices, including by connecting a phone to a computer to browse and save files.[134] Additionally, third-party apps could circumvent Snapchat's auto-deletion feature. As to the screenshot notification, the notice feature did not work with older operating systems on some devices and could be circumvented with third-party apps.[135] The FTC Complaint also included some of Snapchat's collection practices for user data, including geolocation data and contact information.[136] Snapchat changed some of its representations and practices following the Complaint, and a final decision and order outlined specific steps Snapchat must take to correct its practices.[137]

Since Snapchat entered the market in 2011, other companies have developed ephemeral apps targeted at other demographics or industries. Confide is an application that allows confidential messaging, including encryption,[138] self-destruction,[139] and screenshot protection.[140] While Snapchat's Filters and other functions appeal to a teen or young-adult demographic, Confide is targeted at adults and limits these frills.[141] It is a self-proclaimed tool that empowers users to share confidential

133. Complaint at 3–4, *In the Matter of Snapchat, Inc.*, (No. 132-3078) (2014). [https://perma.cc/D5K9-23EJ].

134. *Id.*

135. *Id.*

136. *Id.* at 5–6.

137. Decision and Order, *In the Matter of Snapchat, Inc.*, (No. C-4501) (Dec. 23, 2014). The Decision and Order requires Snapchat to avoid misrepresentations about the extent to which messages are deleted after viewing, the extent to which screenshot notification works, the details about the information Snapchat collects, and "the steps taken to protect against misuse or unauthorized disclosure of covered information." *Id.* at 2. Additionally, Snapchat was required to add a comprehensive privacy plan that addressed the identified risks and issues surrounding confidentiality, with specific implementation steps. *Id.* at 3. Reporting and other compliance obligations are also included, some of which will last for a twenty-year period. *Id.* at 2–6.

138. *Your Confidential Messenger*, CONFIDE [hereinafter CONFIDE], [https://perma.cc/6X2F-9XRS] (noting that the app uses industry-standard, end-to-end encryption that goes through Transport Layer Security to prevent interception).

139. *Id.* (Confide touts its content as truly ephemeral: it is wiped from servers and cannot be saved or retrieved).

140. *Id.* Unlike Snapchat, Confide builds in technology to prevent screenshots or, where not technically feasible, to minimize what information can be captured in the screenshot. *Id.* (explaining how iOS devices prevent fully blocking screenshots but that messages are unveiled in small sections without the sender's name visible to minimize the effectiveness of screenshots). Additionally, Confide gives notice when a screenshot was attempted and removes the recipient from the message. Steven Tweedie, *Confide, a Snapchat for Adults, Just Got Even Faster and Better to Use*, BUS. INSIDER (Sept. 11, 2014, 10:00 AM), [https://perma.cc/UZ4D-8JCN].

141. *See* Tweedie, *supra* note 140.

information without a digital record: "Retake Control of your Digital Conversations and Communicate with Confidence: Discuss sensitive topics, brainstorm ideas or give unfiltered opinions without fear of the Internet's permanent, digital record and with no copies left behind."[142] Additionally, Confide purports to mimic live conversation instead of traditional electronic communications: "Messages disappear forever after they are read once, making them as private and secure as the spoken word."[143] Some of Confide's unique features include the ability to send attachments and encrypted voice messages.[144] All of this works without meaningfully saving digital contents of messages.[145]

Vaporstream, another ephemeral secure messaging app, also markets expressly to businesses.[146] Like Snapchat and Confide, Vaporstream claims it facilitates secure and confidential messaging.[147] But Vaporstream targets industries like healthcare, higher education, and legal specifically, arguing that its secure messaging improves compliance with privacy-related regulations.[148] Notably, Vaporstream claims it helps meet regulatory and other legal obligations through its service, that "keeps you secure and compliant . . . ."[149] In this way, Vaporstream offers ephemeral communication options to specific industries, with some built-in design features to help with data retention requirements.

Other enterprise ephemeral applications are applying the core principles of privacy by design in the business context.[150] Wickr, as another example, emphasizes both privacy by design and security as primary goals of its products.[151] Thus, features like end-to-end encryption, network controls, and auto-deletion not only offer privacy for communications, but they also serve an important purpose in preventing

142. CONFIDE, *supra* note 138.

143. *Id.*

144. *Id.*

145. *Id.*

146. VAPORSTREAM, [https://perma.cc/MJ7D-ME9L].

147. *Id.*

148. *Secure Messaging Solutions*, VAPORSTREAM, [https://perma.cc/B2X4-9N8U]. Vaporstream cites industry-specific privacy principles as one of the reasons industries should use its service. *Id.* For example, Vaporstream calls its service "HIPAA compliant" and asserts "efficient communications are an imperative for every healthcare organization." *Id.* It claims it is "[i]ncreasing [c]ampus [s]afety [t]hrough [s]ecure [t]ext" for higher education, see *Increasing Campus Safety Through Secure Text*, VAPORSTREAM, [https://perma.cc/L88D-3V8P].

149. *See Meeting Regulatory and Legal Obligations*, VAPORSTREAM, [https://perma.cc/RXK7-8UWF].

150. *Security*, WICKR [hereinafter WICKR], [https://perma.cc/PR4C-MH54] ("Whether personal or business, your conversations & data are private by design.").

151. *Id.*

unauthorized access to business data.[152] This security feature of ephemeral apps is another positive trend.

The unique nature of social media—both ephemeral apps and more traditional, yet dynamic platforms like Facebook—must be taken into account in the preservation and spoliation analysis. While the principles and goals of preservation apply equally to social media accounts, this unique form of ESI requires a more nuanced analysis.

II. ESI EXCEPTIONALISM

The civil discovery process is designed to allow broad access to information before trial so that fairness can be maintained in an adversarial justice system.[153] But discovery is not limitless. Rather, the rules define civil discovery based on whether information is potentially relevant.[154] Countervailing concerns such as burden, expense, embarrassment, privilege, and proportionality serve as limits on discovery.[155] Thus, even relevant information is outside the scope of discovery because of the impact it has on the rights of the opposing party.[156] While ESI is as discoverable as traditional forms of information in civil cases, the advent of digital records has caused changes to the Federal Rules over time due to the unique nature of ESI.[157]And due to the volume and nature of ESI, additional limitations have been recognized for ESI.[158] One of the key limits deals with the nature of how ESI is stored—and deleted. This Section will examine (A) how the Federal Rules define ESI and (B) the scope of ESI discovery, including social data and ephemeral content.

152. *See id.*; Casey C. Sullivan, *Wickr GC Jennifer DeTrani on Ephemeral Messaging, Discovery, and the Waymo-Uber Suit*, LOGIKCULL BLOG (Dec. 20, 2017), [https://perma.cc/K6BE-Q4GB] (discussing Wickr's role in reducing enterprise security risks).

153. *Hickman v. Taylor*, 329 U.S. 495, 501 (1947).

154. *See* FED. R. CIV. P. 26(b)(1).

155. *See* FED. R. CIV. P. 26–37.

156. *See Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, *supra* note 16, at 246–47.

157. FED. R. CIV. P. 34 advisory committee's note to 2006 amendment.

158. *See* Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 566–67 (2001). Redish notes that ESI creates unique challenges that should be dealt with specifically in revised procedural rules. *Id.* at 567. Procedural rules, however, draw on "fundamental social, moral, political, and economic values society seeks to foster in shaping its civil litigation process." *Id.* at 568 n.20 (defining "litigation matrix").

A. Defining ESI

The Federal Rules of Civil Procedure do not define the term "Electronically Stored Information."[159] The decision seems intentional: according to the committee notes for the 2006 amendments, "[t]he wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information."[160] Instead, ESI includes information "stored in any medium" and is meant to include future technological developments.[161] Other experts have offered definitions of ESI, such as data that is created and/or stored in electronic form.[162]

The concept of ESI in the Federal Rules can be traced back to the 1970 amendments to Rule 34. There, the scope of document discovery was expanded to include some types of electronically stored content in the form of "data compilations."[163] Specifically, the 1970 committee notes stated that Rule 34:

> [A]pplies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form . . . [such as] a print-out of computer data.[164]

Even at that time, the advisory committee contemplated that "documents" is a concept that evolves with changing technology.[165] Following the 1970 amendments, the idea of producing "documents" under Rule 34 was often interpreted to include ESI.[166] Nonetheless,

159. FED. R. CIV. P. 34 advisory committee's note to 2006 amendment.

160. *Id.*

161. *Id.*

162. *See, e.g.*, Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 333 (2000) (citation omitted) (defining electronic discovery as "information intentionally created by a computer user and stored in electronic form").

163. *See* FED. R. CIV. P. 34 advisory committee's note to 1970 amendment.

164. *See id.*

165. *See id.*

166. *See* FED. R. CIV. P. 34 advisory committee's note to 2006 amendment ("Lawyers and judges interpreted the term 'documents' to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional

although several cases made clear that Rule 34 encompasses all forms of electronic content,[167] considerable judicial discretion applied and debates as to the rules' applicability to new forms of technology persisted.[168]

As a result, the 2006 amendments to the Federal Rules expressly added the term "Electronically Stored Information" to the body of the Rules.[169] In doing so, the Committee deleted the term "data compilation" as "unnecessary because it is a subset of both documents and electronically stored information."[170] Instead, ESI was incorporated as a distinct concept, with references to it throughout the Federal Rules.

Notably, Rule 26, as to the scope of discovery, created two subcategories of ESI, accessible and inaccessible, both of which are treated differently.[171] Courts and scholars have tried to further classify the types of ESI that exist, with a category of inaccessible ESI some call "ephemeral data" being particularly relevant here.

1. ACCESSIBLE ESI

Accessible ESI refers to data that is stored in a "readily usable format."[172] As a result, the data can be easily accessed without restoring from backup media or otherwise manipulating it into a readable form.[173] In the seminal *Zubulake* decisions from the early 2000s, which form the foundation of some of the current e-discovery principles in the Federal Rules,[174] a few categories of accessible ESI were noted. First, accessible ESI may be "active, online data" that is actively being created, received, or processed.[175] Examples here are hard drives[176] or "active user e-mail files."[177] Another category of

concept of 'document.' Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents.").

167. *See, e.g.*, Scheindlin & Rabkin, *supra* note 162, at 350–51 (noting uncertainty as to how rules should apply to new technologies as they emerge).

168. *See, e.g.*, *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 532 (1st Cir. 1996) (noting that trial courts have broad discretion in pretrial discovery matters).

169. FED. R. CIV. P. 26(a)(1)(B) advisory committee's note to 2006 amendment.

170. *Id.*

171. *See infra* Sections I & II.

172. *See Zubulake v. UBS Warburg LLC* (*Zubulake I*), 217 F.R.D. 309, 320 (S.D.N.Y. 2003).

173. *Id.*

174. *See id.*

175. *Id.* at 318.

176. *Id.*

accessible ESI is "near-line data" that includes a "robotic storage device" for accessing retrievable records at fairly quick speeds.[178] Examples include optical disks.[179] Lastly, offline storage or archives are another category of accessible ESI.[180] While offline archives take longer to restore, they nonetheless can be retrieved and accessed without too much intervention or effort.[181]

2. INACCESSIBLE ESI

By contrast, inaccessible data exists in a form that is not ready to use.[182] This category of data may need to be de-fragmented, reconstructed, or otherwise restored in order to be usable.[183] The *Zubulake* decisions identified two categories of inaccessible ESI: backup tapes and "[e]rased, fragmented, or damaged data."[184]

As to backup tapes, the way data is stored on these devices makes it difficult to retrieve and read its contents.[185] As a result, the process of restoring backup tapes can be costly and time-consuming.[186] Some fragmented data may have been broken up and stored in different places by virtue of the way storage media works, so as to be "fragmented"

177. The defendant in *Zubulake I* produced some emails that were easily accessed through active data stored on the HP OpenMail system, and the court identifies this as an example of accessible ESI. *Id.* at 320.

178. *Id.* at 318–19.

179. *Id.* at 319. The defendant in *Zubulake I* admitted it had some emails that it could access through Tumbleweed, its optical disk program. *Id.* at 320. The court categorized this data as "only slightly less accessible" but still falling within the scope of accessible ESI. *Id.*

180. *Id.* at 319.

181. *See id.* (describing how offline archives may consist of a storage shelf of magnetic tape media containing backups or archives of records, requiring more time to access and retrieve); Lee H. Rosenthal, *An Overview of the E-Discovery Rules Amendments,* 116 YALE L.J.F. (2006), [https://perma.cc/Q8X3-57VN] ("Rule 26(b)(2) is amended to address another key difference separating electronic from conventional discovery: electronically stored information, unlike words on paper, may be incomprehensible when separated from the system that created it. The way that the information is created and stored may introduce a new obstacle to parties seeking to access it, in addition to the familiar obstacles of distance and dispersion.").

182. *Zubulake I*, 217 F.R.D. at 320.

183. *Id.*

184. *Id.* at 319.

185. *Id.* Specifically, backup tapes require data to be read in sequence, and contents are not organized in a way for easy document access or management. They also use data compression, which adds time to the restoration process. *Id.*

186. *Id.* The defendant in *Zubulake I* stored some old emails on backup tapes via a program called NetBackup. *Id.* at 320. The court noted that this data is inaccessible, in that it requires cost and time to restore into a usable format. *Id.*

data.[187] Data also could have been damaged or erased in whole or in part from the storage media altogether.[188] Restoration may be impossible or extremely costly for some inaccessible data.[189]

"Ephemeral" content is a particular type of inaccessible ESI that must be considered. In this context, data is ephemeral if it is temporary or transitory and not intentionally created by users.[190] It is typically ancillary or secondary to other electronic information, often "created by a computer as a temporary by-product of digital information processing."[191] Notably, ephemeral data is "not consciously created, viewed, or transmitted to the user."[192] This subcategory of data is "ephemeral" in that it is not intended to be stored for any meaningful time period and is easily overwritten.[193] Examples of ephemeral data include server log data stored in random access memory [RAM][194] and temporary caches that automatically delete internet history.[195]

Social media content may be accessible or inaccessible, depending on the location of information sought. Old posts in a Facebook account are generally "accessible" in that they can be accessed by the account-holder through the "download" account feature.[196] Similarly, for Snapchat, some account activity and data are also available in a "download" file.[197] But the substantive content from Snapchat is inaccessible or no longer exists.[198] Computer forensics may be able to find some transitory files that were temporarily stored on a device, but generally these files are deleted quickly.[199] As a whole, Snapchat is

187. *See id.*

188. *See id.* at 319.

189. *See id.*

190. JAY E. GRENIG & WILLIAM C. GLEISNER, III, 1 EDISCOVERY & DIGITAL EVIDENCE § 4:11 (2016). Some have called this subcategory of data "'outlier' ESI" in that it is not usually considered in the discovery process because it is not particularly visible or accessible. *See* Jennifer H. Rearden & Farrah Pepper, *Oh No, Ephemeral Data!*, N.Y. L.J., Mar. 22, 2010, at 1. In this way, outlier ESI, such as ephemeral data, still falls within ESI generally but certainly qualifies as inaccessible ESI by virtue of its temporary and fleeting nature. *Id.*

191. *See* GRENIG & GLEISNER, *supra* note 190 (quoting Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. BALT. L. REV. 349, 366 (2008)).

192. *Id.* (quoting Withers, *supra* note 191, at 366).

193. *Id.* (quoting Withers, *supra* note 191, at 366).

194. *See Columbia Pictures Industries v. Bunnell*, 2007 WL 2080419 (C.D. Cal. 2007).

195. *See Healthcare Advocates, Inc. v. Harding*, 497 F. Supp. 2d 627, 640 (E.D. Pa. 2007).

196. *See Downloading Your Info*, *supra* note 83.

197. *Download My Data*, *supra* note 114.

198. *See id.*

199. Hill, *supra* note 128.

designed to make the substance of messages disappear after a short duration, with no meaningful retention features.[200] Thus, content created in Snapchat is likely "inaccessible" ESI that is akin to transitory, "ephemeral" files. Nonetheless, like other ESI, ephemeral social media content may fall within the scope of discovery, even though the scope of preservation duties should be limited.

B. The Scope of ESI Discovery

The Federal Rules define the general scope of discovery as including "any nonprivileged matter that is relevant to any party's claim or defense."[201] But discovery's scope is limited to exclude requests that are duplicative, cumulative, or available from another, better source.[202] And discovery is also subject to a proportionality requirement, which serves to further limit the scope of discovery based on several proportionality factors.[203] Under the proportionality factors, courts should consider whether the discovery is:

> [P]roportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.[204]

Thus, while broad discovery is a core tenet of the Federal Rules, its scope is balanced against the cost and need for the discovery.[205]

---

200. *Download My Data*, *supra* note 114.

201. FED. R. CIV. P. 26(b)(1).

202. FED. R. CIV. P. 26(b)(2)(C)(i).

203. In the 2015 Amendments to the Federal Rules, the proportionality requirement was moved up in Rule 26 in order to make it an express limit on the scope of discovery. *See* FED. R. CIV. P. 26(b)(1). For an analysis of how the proportionality factors should be applied to discovery of social media content, see *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, *supra* note 16, at 237–42.

204. FED. R. CIV. P. 26(b)(1).

205. *See Zubulake v. UBS Warburg LLC* (*Zubulake I*), 217 F.R.D. 309, 315–16 (S.D.N.Y. 2003) (noting that cost, burden, and need are factors that guide the scope of civil discovery). Cost-shifting is an important mechanism within the Federal Rules to help address some of the burdens of broad electronic discovery. *See id.* at 321–24. However, cost-shifting is not always appropriate, and it is only an option in cases involving inaccessible ESI. *Zubulake v. UBS Warburg LLC* (*Zubulake III*), 216 F.R.D. 280, 284 (S.D.N.Y. 2003) (ordering some cost-shifting for discovery of emails that must be restored from backup tapes). In order to determine when cost-shifting is appropriate, the court in *Zubulake I* articulated a factor test that considers several

For ESI, the scope of discovery generally remains the same as with traditional forms of potential evidence.[206] However, inaccessible ESI has been treated differently under the Rules. For inaccessible ESI, the Rules contain an additional hurdle to discovery in the form of a good cause threshold: a party is not required to produce ESI that is "not reasonably accessible because of undue burden or cost."[207] If the requesting party files a motion to compel, the party resisting discovery bears the burden of showing that the ESI "is not reasonably accessible because of undue burden or cost."[208] If the resisting party makes this showing, the party requesting discovery then has to show good cause.[209]

Upon a showing of good cause, the court may grant the discovery "considering the limitations of Rule 26(b)(2)(C)" which includes all of the general objections to discovery, such as when the discovery is cumulative, duplicative, obtainable from another source for less burden or expense, or beyond scope of discovery generally.[210] Lastly, the court is permitted to further define the conditions for ESI discovery, thereby granting a lot of judicial discretion.[211]

The Federal Rules also allow for additional considerations as to the form of production.[212] Requests for production may expressly include ESI, even if the producing party needs to translate the ESI into a reasonably usable form,[213] and can specify the forms of ESI requested.[214] The responding party should produce ESI in the form in

factors, including the tailoring of the discovery, availability of discovery from other sources, the cost of production, proportionality of costs in relation to the amount in controversy, the parties' resources, and the importance of the issues at stake. *See Zubulake I*, 217 F.R.D. at 323–24 (citing *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002)); *see also Zubulake III*, 216 F.R.D. at 284–90 (applying the *Zubulake I* test to shift some costs for email discovery to plaintiff).

206. FED. R. CIV. P. 26(a) advisory committee notes to 2006 amendment (Rule 26(a)(1) encompasses ESI and has a broad meaning); *see* FED. R. CIV. P. 34(a)(1)(A) (ESI included within the scope of discovery requests for production of documents).

207. FED. R. CIV. P. 26(b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.").

208. *Id.*

209. *Id.*

210. FED. R. CIV. P. 26(b)(2)(C)(i).

211. *See id.*

212. FED. R. CIV. P. 34(a)(1)(A).

213. *Id.*

214. FED. R. CIV. P. 34(b)(1)(C).

which it is ordinarily maintained, as it is kept in "the usual course of business or must organize and label them to correspond to the categories in the request," but is not required to produce ESI in more than one form.[215]

The different treatment of inaccessible ESI reflects a trend in the Federal Rules to recognize the unique nature of ESI and the challenges posed by vast storage capacities. And the rules continue to evolve to address ESI's changing nature. Social data and ephemeral content, in particular, require special attention.

1. SOCIAL DATA DISCOVERY

Social data fall within the realm of ESI for discovery purposes.[216] And social media has become an important facet of discovery in many civil cases. Most social data discovery happens through discovery requests to account-holders: social media platforms themselves generally do not disclose third-party content pursuant to civil subpoenas, citing the Stored Communication Act.[217] Rather, platforms direct parties to seek discovery directly from account-holders, who have access to their own data through the "download your info" feature on most social media platforms.

But courts sometimes take an overly broad approach to the scope of discovery of social media, allowing almost complete and unfettered access to entire accounts without many limits. Cases addressing social media discovery tend to take three different approaches: (1) a "factual predicate" approach that relies on visible, public account content as the predicate for access to privacy-protected contents, (2) a broad presumption of unfettered discovery without much tailoring, or (3) a "reasonable particularity" approach that attempts to limit discovery to specific claims and issues in the litigation.[218]

First, the "factual predicate" approach looks to publicly available social media data before allowing access to privacy-protected content. *Romano v. Steelcase Inc.* [219] is a lead example of this approach. There, the court allowed the broad discovery of the plaintiff's Facebook page after she alleged severe neck and back injuries and loss of enjoyment in

215. FED. R. CIV. P. 34(E)(i)–(iii).

216. Fed. R. Civ. P. 34(a)(1)(A).

217. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 968–69 (C.D. Cal. 2010).

218. For a complete discussion of these three approaches, see *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, *supra* note 16, at 273–75, 277; see also *The Facebook Digital Footprint*, *supra* note 16 (analyzing different approaches courts take to social media discovery).

219. 907 N.Y.S.2d 650, 653 (N.Y. Sup. Ct. 2010).

life.[220] The discovery was based in part on plaintiff's Facebook profile photo, which depicted her smiling on vacation in Florida.[221] Because the photo contradicted the injuries she claimed in the case, it served as the factual predicate to support the broad discovery of the private Facebook contents.[222] Notably, no meaningful limits were added based on the relevance or time frame of the posts.[223] This approach places too much emphasis on user-controlled settings (like what is left public) and fails to provide other limits, like relevance, as required under the Federal Rules.[224]

Second, some courts appear to presume the entirety of a social media account is discoverable and impose few limits on the scope of what must be produced.[225] Under this approach, some courts have ordered litigants to produce or exchange login credentials for direct access to accounts, with no limits based on relevance.[226]

Lastly, the "reasonable particularity" approach demonstrates an attempt by courts to impose relevance-based limits on social media discovery.[227] For example, in *EEOC v. Simply Storage*,[228] the court limited discovery in a sex discrimination case to that which is specifically relevant to the claims and defenses, noting that general emotional harm claims may not suffice for broad access to entire accounts.[229] The court also considered the proportionality factors in crafting its limits on the scope of civil discovery.[230] While the ultimate scope of discovery granted was quite broad because of the severe

220. *Id*. at 653–54.

221. *Id.* at 654.

222. *Id.*

223. *See id.* at 656.

224. *See Georgel v. Preece*, No. 0:13-CV-57-DLB, 2014 WL 12647776, at *5 (E.D. Ky. Feb. 28, 2014) (acknowledging that the factual predicate approach may be unfair to the party seeking discovery); *See Forman v. Henkin*, No. 1 (N.Y. Feb. 13, 2018), https://www.courthousenews.com/wp-content/uploads/2018/02/henkin.pdf [https://perma.cc/WHH2-K52L] (rejecting the factual predicate approach); McPeak, *supra* note 16.

225. *See, e.g.*, *Gallion v. Gallion*, No. FA114116955S, 2011 WL 4953451 (Conn. Super. Ct. Sept. 30, 2011) (ordering password exchanges in a family law case); Order Granting Motion to Compel Discovery, *McMillen v. Hummingbird Speedway, Inc.*, (No. 113–2010 CD), 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010) [hereinafter *McMillen* Order] (order granting motion to compel password in personal injury case).

226. *See McMillen* Order, *supra* note 225.

227. *See, e.g.*, *EEOC v. Simply Storage*, 270 F.R.D. 430 (S.D. Ind. 2010).

228. *Id.*

229. *Id.* at 435.

230. *Id.* at 433 (referencing FED. R. CIV. P. 26(b)(2)(C)).

emotional distress damages alleged, the court nonetheless crafted some relevance-based boundaries.[231]

To date, few cases address the scope of civil discovery of ephemeral social media apps like Snapchat. Snapchat has been included as evidence by reference in some civil cases,[232] and has been the subject of discovery requests.[233] It is likely that Snapchat and similar apps will be treated the same as other transitory, "ephemeral" content for the purposes of discovery.

2. DISCOVERY OF TRANSITORY, "EPHEMERAL" CONTENT

For ESI that is ephemeral in nature, courts have allowed discovery, but with recognized limits due to the temporary nature of such content. The first major case allowing discovery of ephemeral ESI is *Columbia Pictures, Inc. v. Bunnell*,[234] a copyright infringement action.[235] There, the court allowed discovery of server log data stored in a computer's RAM, holding that such data is ESI within the scope of discovery.[236] Defendants argued that RAM data was not ESI because the data is not *stored* within the meaning of the rule.[237] In particular, they argued that data is "stored" if it is made available "for later retrieval," as opposed to temporarily housed on the computer for the purpose of quick deletion.[238] The court disagreed, holding that "data stored in RAM, however temporarily, is electronically stored information subject to discovery under the circumstances of the instant case."[239] To support its holding, the court looked to the dictionary definition of "storage" and noted that RAM is the memory function of a

231. *See id.* at 434–36 (stating that social networking site content is not shielded from discovery just because it is "locked" or "private" and that such content must be produced when it is relevant to a claim or defense in the case).

232. *See, e.g.*, *Roof v. Newcastle Pub. Sch. Dist.*, No. CIV-14-1123-HE, 2016 WL 502076, at *1 (W.D. Okla. Feb. 8, 2016) (Snapchat messages referenced in battery and Title IX claims against high school teacher and school district for inappropriate romantic contact with a student); *Ramirez v. Mo. Dep't of Soc. Servs.*, 501 S.W.3d 473, 478 (Mo. Ct. App. 2016) (Snapchat conversation referenced in case alleging teacher had inappropriate communications with student; unclear whether communications themselves were ever in evidence).

233. *See, e.g.*, *Georgel v. Preece*, No. 0:13-CV-57-DLB, 2014 WL 12647776, at *5 (E.D. Ky. Feb. 28, 2014) (denying motion to compel discovery of social media information, including Snapchat, because the requests were too broad).

234. 245 F.R.D. 443 (C.D. Cal. 2007).

235. *Id.* at 445.

236. *Id.* at 443.

237. *Id.* at 446–47.

238. *Id.* at 446.

239. *Id.*

computer, which necessarily "stores" data regardless of whether that data is quickly overwritten or not meant for later retrieval.[240] It also looked to the advisory committee notes to the 2006 amendments to Rule 26 and the intent to use broad and flexible definitions of ESI.[241] Thus, data that is simply placed in RAM is ESI within the scope of discovery.[242]

ESI is an important component of the Federal Rules, subject to broad discovery but with specific limitations, such as the additional good cause threshold created for inaccessible ESI. Nonetheless, even ephemeral data is within the scope of discovery, which means it is potentially within the scope of preservation duties.

III. PRESERVATION AND SPOLIATION

Lawyers and parties have a duty to preserve potential evidence when litigation is anticipated or pending. They also have a duty to avoid spoliation of evidence subject to a duty to preserve.[243] The scope of these duties, however, is not always clear and draws on numerous sources of law, including common law,[244] criminal law,[245] tort law,[246]

240. *Id.* The court also looked to the definition of RAM itself, which is a "read/write, nonsequential-access memory used for the *storage* of instructions and data." *Id.* at 447 (citing NAT'L COMM. SYS., FEDERAL STANDARD 1037C: TELECOMMUNICATIONS: GLOSSARY OF TELECOMMUNICATION TERMS R-8 (Gen. Servs. Admin., 4th ed. 1996) (emphasis added by court)).

241. *Id.* at 447 (noting that the 2006 amendments were meant to be "expansive and includes any type of information that is stored electronically.") (citing FED. R. CIV. P. 34 advisory committee's note to 2006 amendment).

242. *Id.* at 447–48. *See also MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993) (holding that Copyright Act's requirement of something being "fixed in a tangible medium of expression" and not merely for a "transitory duration" was met when a computer copied software into RAM).

243. The very definition of spoliation varies among different sources. *See, e.g.*, Charles R. Nesson, *Incentives to Spoliate Evidence in Civil Litigation: The Need for Vigorous Judicial Action*, 13 CARDOZO L. REV. 793, 793 (1991) ("Spoliation is the act of destroying or otherwise suppressing evidence in litigation. By its nature spoliation is invisible. The evidence may have been unknown to anyone but the spoliator. The act itself need leave no trace.").

244. *See, e.g.*, *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999) (common-law definition of spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation"). Even without substantive or procedural rules authorizing spoliation sanctions, courts historically have inherent authority to address spoliation issues. *See, e.g.*, *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583 (4th Cir. 2001); *Zubulake v. UBS Warburg LLC* (*Zubulake IV*), 220 F.R.D. 212, 216 (S.D.N.Y. 2003); Paul W. Grimm et al., *Proportionality in the Post-Hoc Analysis of Pre-Litigation Preservation Decisions*, 37 U. BALT. L. REV. 381 (2008).

245. In the criminal context, spoliation falls under tampering with evidence, obstruction of justice, or hindering prosecution. *See* RESTATMENT (THIRD) OF THE LAW

legal ethics rules,[247] and civil procedure rules.[248] These sources of law often parallel each other and may incorporate or refer to each other. But no single body of law clearly defines lawyer preservation duties and spoliation.[249] The result is that lawyers and litigants face unclear standards for avoiding spoliation, and the analysis is further complicated by the specific challenges created by disappearing data.

Nonetheless, the duty to preserve, when triggered and applicable, applies to ESI. The duty may include preserving emails and other documents at least on back-up media, and can encompass metadata and deleted content.[250] It also includes social media content,[251] as well as instant messaging, though some courts limit preservation duties to messages that fall under the umbrella of relevant business records.[252]

GOVERNING LAWYERS § 118 (AM. LAW INST. 2000) (summarizing potential criminal and civil liability for spoliation of evidence, including negligent spoliation).

246. Several states have adopted a tort for spoliation of evidence. *See* Eric M. Larsson, *Cause of Action for Spoliation of Evidence*, *in* 40 CAUSES OF ACTION §§ 42–56 (2d ed. 2009) (summarizing the states that have recognized an independent tort for spoliation of evidence).

247. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT r. 3.4 (AM. BAR ASS'N 2017); *See* Charles W. Wolfram, *Toward a History of the Legalization of American Legal Ethics—II the Modern Era*, 15 GEO. J. LEGAL ETHICS 205, 206–08 (2002).

248. *See* FED. R. CIV. P. 37(e).

249. *See generally* JAY E. GRENIG & JEFFREY S. KINSLER, HANDBOOK OF FEDERAL CIVIL DISCOVERY & DISCLOSURE E-DISCOVERY & RECORDS § 4:4 (4th ed. 2017).

250. *See, e.g.*, *Brown Jordan Int'l, Inc. v. Carmicle*, No. 0:14-CV-60629-ROSENBERG/BRANNON, 2016 WL 815827, at *37 (S.D. Fla. Mar. 2, 2016) (destruction of metadata associated with a defendant's screenshots of employee emails led to presumption that the metadata was unfavorable to the defendant); *Pulaski Bank v. First State Bank of St. Charles*, Civil Action No. 12-2433-HKV, 2012 WL 3062778, at *3 (D. Kan. July 26, 2012) (defendant ordered to preserve metadata); *Victor Stanley v. Creative Pipe, Inc.*, 269 F.R.D. 497, 524 (D. Md. 2010) (noting that preservation duties extend to metadata and deleted data). *But see Phillips v. Netblue, Inc.*, No. C-05-4401 SC, 2007 WL 174459, at *3–4 (N.D. Cal. Jan. 22, 2007) (no duty to preserve hyperlinked content in emails).

251. While Rule 37 does not mention social media expressly, the Committee Notes make clear that attorneys are responsible for assessing all of their clients' ESI, including that contained in social media accounts. *See* FED. R. CIV. P. 37 advisory committee notes to 2015 amendments (noting that "[i]t is important that counsel become familiar with their clients' information systems and digital data — including social media—to address these issues."); Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 43–50 (2006) (describing cases that define culpability for destruction of potential evidence).

252. *See, e.g.*, *Broadspring, Inc. v. Congoo, LLC*, No. 13-CV-1866 (JMF), 2014 WL 4100615, at *24–25 (S.D.N.Y. Aug. 20, 2014) (although the court noted that instant messages are subject to a duty to preserve, it only awarded costs and attorney's fees for violating a court preservation order and declined an adverse inference instruction); *Day v. LSI Corp.*, No. CIV 11–186–TUC–CKJ, 2012 WL 6674434, at *12 (D. Az. Dec. 20, 2012) (company had duty to preserve instant messages where the

The scope of preservation duties for ephemeral and transitory data, however, is not entirely clear.[253] Two major sources of preservation duties are discussed here: the Federal Rules and legal ethics rules.

A. Preservation Duties Under Federal Rules of Civil Procedure

An important part of the discovery process is ensuring potential evidence is preserved and not destroyed before discovery is completed.[254] Although discovery is not limitless, a broad range of potential evidence nonetheless must be preserved, as long as it is discoverable and the duty to preserve was triggered.[255]

The procedural rules themselves outline the scope of discovery and refer to duties to preserve potential evidence.[256] In particular, Rule 37 allows a party to move to compel discovery, obtain a protective order, or request cost-shifting, attorney's fees, or sanctions for failing to comply with discovery.[257] Rule 37(e) also contains a specific provision dealing with preserving ESI.[258] If a party should have preserved ESI "in the anticipation or conduct of litigation" but failed to do so, the court has several remedial options depending upon the party's intent.[259] If the party "acted with the intent to deprive another party of the information's use in the litigation," the court can presume the destroyed evidence was unfavorable to the party, instruct the jury to make such a presumption, or dismiss the case altogether.[260] But without intent, the court's options are more limited. Instances where the destruction lacks the requisite intent instead hinge on a showing of prejudice to the other party.[261] If prejudice can be shown, the court can take remedial

company made personnel decisions over instant message); *Mikhlyn v. Bove*, No. 08-CV-3367 (ARR)(RER), 2011 WL 4529613, at *6 (E.D.N.Y. Sept. 28, 2011) (failure to preserve highly relevant Skype chats among parties to the litigation resulted in monetary sanctions); *Océ N. Am., Inc. v. Brazeau*, No. 09 C2381, 2010 WL 5033310, at *6 (N.D. Ill. Mar. 18, 2010).

253. *See* John G. Browning, *Burn After Reading: Preservation and Spoliation of Evidence in the Age of Facebook*, 16 SMU SCI. & TECH. L. REV. 273, 274–85 (2013) (noting the unique spoliation challenges posed by social media, including new ephemeral apps like Snapchat).

254. *See id.*

255. *See id.*

256. *See id.* at 277–79.

257. FED. R. CIV. P. 37. Inherent authority of courts was also used to impose penalties when spoliation precedes a discovery order. *See, e.g.*, *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591–92, 595 (4th Cir. 2001).

258. FED. R. CIV. P. 37(e).

259. *Id.*

260. FED. R. CIV. P. 37(e)(2).

261. FED. R. CIV. P. 37(e).

measures that must be "no greater than necessary to cure the prejudice."[262] Rule 37(e) is often referred to as a safe harbor provision, protecting litigants from spoliation sanctions.[263]

1. EVOLUTION OF SPOLIATION SAFE HARBORS

Rule 37(e)'s safe harbor for ESI spoliation, as it currently reads, was added in the 2015 Amendments. Before the 2015 Amendments, Rule 37 contained a safe harbor for when ESI was "lost as a result of the routine, good-faith operation of an electronic information system."[264] This older version of Rule 37, which first appeared in 2006, in part tried to address a unique spoliation issue that only comes up with ESI: auto-deletion of content.[265]

With electronic storage systems, the system itself needs to override or otherwise periodically delete old content. This means that a person or company can unintentionally destroy content—even without their knowledge—just by operation of the system itself. Thus, the 2006 Amendments, which first added the concept of ESI to the Federal Rules in general, included a safe harbor for spoliation caused by the "routine, good-faith operation" of an information storage system.[266]

Nonetheless, under the 2006 version of Rule 37, once a preservation obligation kicked in, litigants may have had a duty to end auto-deletion of content and preserve content more broadly: "[t]he good faith requirement of Rule 37(f) [the 2006 version of Rule 37(e)] means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve."[267] Cases also expanded the preservation requirement when a litigation hold existed,[268] thereby narrowing a litigant's ability to rely on the "good-faith, routine operation" safe harbor in Rule 37.[269]

---

262. FED. R. CIV. P. 37(e)(1).

263. FED. R. CIV. P. 37(e).

264. FED. R. CIV. P. 37(f) (amended 2006, 2015).

265. *See* ADVISORY COMM. ON FED. RULES OF CIVIL PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE ADVISORY COMMITTEE ON CIVIL RULES 3, 9–10 (2012).

266. *See* FED. R. CIV. P. 37(f).

267. FED. R. CIV. P. 37(f) committee's note to 2006 amendment.

268. *See Risk Aversion*, *supra* note 8, at 543–44.

269. *See, e.g.*, *William T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1448 (C.D. Cal. 1984) (company had duty to preserve documents despite internal document destruction procedures); Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 J. CORP. L. 417, 424–25 (1999); *See* A. Benjamin Spencer, *The*

According to some scholars, the 2006 version of Rule 37 did not cure all of the inconsistencies or challenges with sanctions for ESI spoliation.[270] Some lawyers and litigants over-preserved ESI at considerable expense.[271] For example, in 2010, lawyers who litigated cases in federal court cited ESI discovery as costly and confusing.[272] Many criticized the lack of clarity provided by the 2006 version of Rule 37, noting that parties did little to define preservation at the outset of litigation but feared sanctions if any ESI was deleted.[273] Additionally, courts took broad and different approaches to spoliation sanctions in part due to the limited guidance provided by Rule 37. Several authors

Preservation Obligation: Regulating and Sanctioning Pre-Litigation Spoliation in Federal Court, 79 FORDHAM L. REV. 2005, 2012–13 (2011); Alexander B. Hastings, Note, *A Solution to the Spoliation Chaos: Rule 37(e)'s Unfulfilled Potential to Bring Uniformity to Electronic Spoliation Disputes*, 79 GEO. WASH. L. REV. 860, 877–78 (2011).

270. *See, e.g.*, Robert Hardaway et al., *E-Discovery's Threat to Civil Litigation: Reevaluating Rule 26 for the Digital Age*, 63 RUTGERS L. REV. 521, 585–86 (2011). *See also* Thomas Y. Allman, *Inadvertent Spoliation of ESI After the 2006 Amendments: The Impact of Rule 37(e)*, 3 FED. CTS. L. REV. 25 (2009); Thomas Y. Allman, *The Justifcation for a Limted Preservation Safe Harbor for ESI*, 5 NW. J. TECH. & INTELL. PROP. 1 (2006); Nicole D. Wright, *Federal Rule of Civil Procedure 37(e): Spoiling the Spoliation Doctrine*, 38 HOFSTRA L. REV. 793 (2009).

271. Thomas Y. Allman, *The 2015 Civil Rules Package as Transmitted to Congress*, 82 DEF. COUNS. J. 375, 401–02 (2015) (summarizing business concerns with over-preservation).

272. A 2010 national survey of plaintiff and defendant attorneys on federal civil cases showed that litigation costs have increased due to numerous factors including electronic discovery and disputes over discovery. *See* EMERY G. LEE III & THOMAS E. WILLGING, LITIGATION COSTS IN CIVIL CASES: MULTIVARIATE ANALYSIS: REPORT TO THE JUDICIAL CONFERENCE ADVISORY COMMITTEE ON CIVIL RULES 1 (2010). According to empirical analysis and statements by some lawyers, discovery can be blamed for the increased cost of litigation. *Id.* at 5; *see also* THOMAS E. WILLGING & EMERY G. LEE III, IN THEIR WORDS: ATTORNEY VIEWS ABOUT COSTS AND PROCEDURES IN FEDERAL CIVIL LITIGATION 3 (2010). And lawyers have been slow to adjust to ESI. *See id.* at 16–17 (in 2010, some lawyers surveyed reported knowing little about how to handle large-volume ESI cases); John H. Beisner, *Discovering a Better Way: The Need for Effective Civil Litigation Reform*, 60 DUKE L.J. 547, 567 (2010) (noting that discovery is often used in a vexatious and abusive manner, particularly as to costs and burden of ESI discovery); Gross, *supra* note 9; Scott M. O'Brien, Note, *Analog Solutions: E-Discovery Spoliation Sanctions and the Proposed Amendments to FRCP 37(E)*, 65 DUKE L.J. 151, 153–54 (2015) (criticizing the 2015 Amendment to Rule 37 as granting too much discretion to trial courts and not doing enough to curtail discovery abuse); Lee H. Rosenthal, *From Rules of Procedure to How Lawyers Litigate: 'Twixt the Cup and the Lip*, 87 DENV. U.L. REV. 227, 228–30 (2010) (cataloguing the ongoing criticisms of civil discovery rules from their inception).

273. *See supra* note 272. *See also Apple Inc. v. Samsung Elecs. Co.*, 881 F. Supp. 2d 1132, 1144–51 (N.D. Cal. 2012) (noting the lack of clarity in spoliation sanctions); Philip J. Favro, *The New ESI Sanctions Framework Under the Proposed Rule 37(e) Amendments*, RICH. J.L. & TECH., Mar. 20, 2015, at 3–4.

have examined the broad and inconsistent sanctions imposed by courts for ESI spoliation.[274]

Thus, the 2015 Amendments sought to address the huge growth of ESI and the challenges of adequately preserving potential evidence, recognizing the inconsistent and often harsh approaches courts took for imposing sanctions for spoliation of ESI.[275] The Committee Notes make clear that huge volume of ESI and inconsistent standards for imposing sanctions created the need for a revision:

> This limited rule [referring to the 2006 version of Rule 37(e)] has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of such information. Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough.[276]

Thus, the current version of Rule 37(e) marks a significant change that is meant to clarify preservation and spoliation duties while still looking to common law to define these duties.[277] It primarily relies on intent for determining when spoliation sanctions are appropriate and is meant to require reasonable steps to preserve, but not "perfection" in preserving all ESI.[278]

The committee also noted that, when applying current Rule 37(e), several factors should guide the court in determining whether spoliation occurred.[279] First, the Rule may be inapplicable altogether when the

274. *See, e.g.*, Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. & TECH. L. REV. 71 (2004) (Judge Scheindlin, who wrote the seminal *Zubulake* decisions, and her co-author discuss the controversial nature of adding safe harbors to Rule 37 in 2006 and analyze five years of written opinions to identify how courts imposed sanctions for destruction of electronic content); Dan H. Willoughby, Jr. et al., *Sanctions for E-Discovery Violations: By the Numbers*, 60 DUKE L.J. 789 (2010).

275. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment; Willoughby, Jr. et al., *supra* note 274, at 806–05 (describing the variety of sanctions that courts have used for e-discovery violations).

276. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

277. *See id.* ("Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve.").

278. *See* FED. R. CIV. P. 37(e); FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

279. *Id.*

ESI is out of the party's control.[280] For loss within the party's control, preservation efforts may still have been reasonable based on good-faith operation of an electronic system or the use of "cloud" or external storage systems.[281] Courts should also consider whether lost content can be restored or obtained through additional discovery.[282] Lastly, proportionality is also a relevant inquiry:

> The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. . . . A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.[283]

Thus, the law remains flexible in curtailing the burdens and scope of preservation duties, especially in light of the vast amount of data that may exist.

2. EXAMPLES OF ESI SPOLIATION

Numerous courts have ordered sanctions, adverse inferences, and other penalties for destruction of electronic evidence.[284] But the decision to store data in inaccessible formats, rather than accessible ones, is not in and of itself sanctionable. For example, in *Quinby v. WestLB AG*,[285] the court declined to sanction a company for moving emails to backup tapes from an accessible media form, even though the move rendered the ESI inaccessible.[286] The court noted that the duty to preserve does not mean a party must maintain data in easily accessible formats.[287]

280. *Id.*

281. *Id.*; *see also Stevenson v. Union Pacific R. Co.*, 354 F.3d 739, 746 (8th Cir. 2003) (noting that adverse inference may be improper when documents were destroyed pursuant to a reasonable document retention policy that "was not instituted in bad faith").

282. *Id.*

283. *Id.*

284. *See, e.g.*, Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 47–50 (2006) (describing cases that define culpability for destruction of potential evidence).

285. No. 04Civ.7406(WBP)(HBP), 2005 WL 3453908 (S.D.N.Y. Dec. 15, 2005).

286. *Id.* at *8 nn.9–10 and accompanying text.

287. *Id.* at *8 n.10.

Nonetheless, the court also declined to shift the costs of restoring e-mail for review and production.[288]

Routine, good-faith operation of a system also excuses some preservation failures,[289] though courts may allow adverse inferences or decline to shift costs when companies deliberately select opaque or inaccessible data management systems.[290] Nonetheless, courts do not impose a duty to create a record where none otherwise exists. For example, one court was unconcerned when a company failed to save customer service chat room conversations, even though a short-term digital record of those conversations did exist.[291] In *Malletier v. Dooney & Bourke, Inc.*,[292] the plaintiff sought spoliation sanctions after defendant failed to preserve a record of conversations that occurred via its website's chat room feature.[293] The court noted that the defendant lacked the technology to readily save those conversations until it more recently added software that saved them for up to two weeks.[294] Further, the court noted that plaintiff's arguments were "akin to a demand that a party to a litigation install a system to monitor and record phone calls coming in to its office on the hypothesis that some of

288. *Id.* at *9.

289. *See, e.g.*, *ClearOne Commc'ns, Inc. v. Chiang*, No. 2:07 CV 37 TC, 2008 WL 704228, at *4 (D. Utah Mar. 10, 2008) ("[Defendant] did not maintain an email storage system that would retain a copy of the September 5, 2005 email. No evidence suggests that this was done in bad faith, but is rather the effect of design of the email system [defendant] employed. However questionable the design may be, the effect is that the routine operation of [defendant's] computer system did not capture the email. No sanction is needed on this point, as [plaintiff] is free to establish at trial that no one has complete access to or knows the entire contents of [witness'] sent email. Each party will be free at trial to argue the implications of that fact.").

290. *See, e.g.*, *Zurich Am. Ins. Co. v. Ace Am. Reinsurance Co.*, No. 05 Civ. 9170 RMB JCF, 2006 WL 3771090, at *2 (S.D.N.Y. Dec. 22, 2006) ("A sophisticated reinsurer that operates a multimillion dollar business is entitled to little sympathy for utilizing an opaque data storage system, particularly when, by the nature of its business, it can reasonably anticipate frequent litigation. At the same time, the volume of data accumulated by [defendant] makes a search of its entire database infeasible. The parties shall therefore propose a protocol for sampling [defendant's] claim files to obtain examples of claims files in which issues of the allocation of policy limits has been addressed."); *Xpedior Creditor Trust v. Credit Suisse First Bos. (USA), Inc.*, 309 F. Supp. 2d 459, 465–67 (S.D.N.Y. 2003) (no apparent preservation issue for company that decommissioned data storage system and rendered its computer files inaccessible, but court declined to shift costs of restoration to party seeking discovery).

291. *See Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ.5316 RMB MHD, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (no duty to save chatroom conversations).

292. *Id.* at *1.

293. *Id.* at *2.

294. *Id.*

them may contain relevant information."[295] The court went on to note that no such requirement exists under the law.[296]

Spoliation can also occur with content contained in social media accounts, like Facebook. The starkest example of sanctions for Facebook spoliation is the case of *Lester v. Allied Concrete Co*.[297] The *Lester* case involved over $700,000 in sanctions all stemming from the deletion of one picture on Facebook—and the series of bad acts that followed.[298] The plaintiff was a young widower whose wife was crushed by a concrete truck.[299] During discovery, defense counsel obtained a copy of a Facebook photo showing the plaintiff holding a beer at a party while wearing an "I [heart] hot moms" t-shirt.[300] Defense counsel somehow obtained the photo from Facebook and attached it to a discovery request for the entirety of the private portions of the Facebook account.[301] Rather than responding to the discovery request with potentially relevant content from the Facebook account, Murray, the plaintiff's attorney, instructed his paralegal to contact the client and tell him to "clean up his Facebook page."[302] Understandably, this directive prompted the paralegal to send the client an email that essentially instructed the client to delete content from his social media account.[303] The client, in turn, deactivated his account, but later restored it, after which he deleted at least sixteen photographs from the account.[304] Without question, this amounted to spoliation: litigation was pending, a specific discovery request for Facebook content was served on plaintiff, and social media data was intentionally deleted in response.[305]

What then followed was an ill-advised attempt to cover up the spoliation. Murray withheld correspondence about the account and his

295. *Id.*

296. *Id.* However, if a company records voice conversations during the course of business, a duty to preserve those recordings may exist. *See, e.g.*, *E*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582, 590 (D. Minn. 2005). *See also* Mia Mazza et al., *In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, RICH. J.L. & TECH., Mar. 19, 2007, at 74–75 (noting that businesses should have the freedom to change their internal information systems without fearing penalty for doing so in future litigation).

297. 736 S.E.2d 699 (Va. 2013).

298. *Id.* at 702–03.

299. *Id.* at 701.

300. *Id.* at 702.

301. *Id.*

302. *Id.*

303. *Id.*

304. *Id.* It appears that Lester deactivated his account but was able to reactivate it before it was deleted. *Id.*

305. *See id.*

client lied about the spoliation.[306] Murray even lied himself in a deposition.[307] Ultimately, computer forensic experts figured out that sixteen photos were deleted.[308] And the correspondence showing the intentional destruction of social media content was also discovered.[309] In the end, Lester won his case and obtained a $10.6 million verdict.[310] But that award was reduced by $700,000 in sanctions all stemming from a lawyer's desire to get rid of one unflattering photo from Facebook.[311]

Negative consequences have also occurred in cases where an entire Facebook account was deleted,[312] or where Facebook messages and responses were not preserved.[313] In other cases, courts have found culpability in removing individual posts from Facebook after litigation is pending, even though they recognize that removing content is part of normal usage. For example, in *Painter v. Atwood*,[314] the court held that the plaintiff in a sexual harassment case spoliated evidence when she deleted select Facebook content, including photos on her Timeline of the defendant's wife and children.[315] The court noted that the deletions occurred after Painter hired a lawyer for this matter, and that she, therefore, had a duty to preserve social media content that could relate to the case.[316] While the court acknowledged that it is not unusual for regular Facebook users in their early twenties to routinely delete content, the court further held that Painter had some culpability: she

306. *Id.* at 703.

307. *Id.*

308. *Id.*

309. *Id.* at 702.

310. *Id.* at 709; Christopher Danzig, *Facebook Spoliation Costs Widower and His Attorney $700K in Sanctions*, ABOVE THE LAW (Nov. 8, 2011, 1:53 PM), [https://perma.cc/NP6V-GKEX].

311. Danzig, *supra* note 310.

312. *See, e.g.*, *Gatto v. United Airlines, Inc.*, Civil Action No. 10–cv–1090–ES–SCM, 2013 WL 1285285, at *2 (D.N.J. Mar. 25, 2013). In *Gatto*, the court ordered the plaintiff to give defendant his login credentials for his Facebook page for discovery purposes and, after defense counsel logged into the account, the plaintiff received a notice from Facebook of suspicious account activity. *Id.* The plaintiff deactivated, and later deleted, the account in response to the notice. *Id.* Although plaintiff claimed the deletion was inadvertent, the court noted that plaintiff's actions were intentional and prevented defendant from accessing the discoverable information. *Id.* at *4.

313. *Patel v. Havana Bar, Rest., & Catering*, No. 10-1383, 2011 WL 6029983, at *1, *6 (E.D. Pa. Dec. 5, 2011) (spoliation occurred when plaintiff deleted several Facebook Messenger exchanges with potential witnesses).

314. No. 2:12-CV-01215-JCM, 2014 WL 1089694, at *1 (D. Nev. Mar. 18, 2014).

315. *Id.* at *6.

316. *Id.*

deleted items that directly related to the suit after the duty to preserve kicked in.[317] The *Painter* court ultimately allowed for an adverse inference as to the deleted posts.[318] Taken as a whole, these cases demonstrate that social media spoliation can result in negative consequences in civil cases.

No cases have expressly addressed spoliation of *ephemeral* social media content in civil cases. But one high-profile allegation of wrongdoing through use of self-destructing technology has been raised in *Waymo, LLC v. Uber Tech., Inc.*,[319] a trade secret theft case.[320] There, Waymo accused Uber of intentional spoliation because Uber instructed its employees to use the ephemeral app Wickr.[321] In a pretrial order, the court declined to order an adverse inference or sanctions, but noted that Waymo may admit evidence of Uber's use of ephemeral messaging "to explain gaps in Waymo's proof that Uber misappropriated trade secrets or to supply proof that is part of the res gestae of the case . . . ."[322] But the court also cautioned that Waymo cannot use ephemeral messaging evidence in a way that is cumulative, speculative, or distracting.[323] Further, Uber is allowed to present evidence that "its use of ephemeral communications shows no wrongdoing, including by pointing out Waymo's own use of ephemeral communications."[324] Notably, the court cautioned that Waymo cannot attempt to vilify Uber by virtue of its decision to use ephemeral messaging in general.[325] Ultimately, the court held that it is for the jury to decide whether either party acted improperly based on the admissible evidence presented.[326]

Other cases have dealt with ephemeral content in general. In those cases, courts have hesitated to impose broad preservation duties on ephemeral content, even though such content is discoverable. For

317. *See id.*

318. *Id.* at *9. No sanctions were imposed for the deleted Facebook photos because Painter still had the photos and produced those separately. *Id.* at *4, *9; *see also Katiroll Co. v. Kati Roll & Platters, Inc.*, Civil Action No. 10–3620 (GEB), 2011 WL 3583408, at *3 (D.N.J. Aug. 3, 2011) (changing Facebook profile picture in trade dress case was unintentional spoliation that did not warrant sanctions).

319. *Waymo, LLC v. Uber Tech., Inc.*, (No. C 17-00939 WHA) (2018).

320. *See* Omnibus Order on Extent to Which Accusations Re Uber's Litig. Misconduct May Feature at Trial at 30–35, *Waymo, LLC v. Uber Tech., Inc.*, (No. C 17-00939 WHA) (2018) [hereinafter Omnibus Order].

321. *See* Reuters, *Uber's Use of Encrypted Messaging App Wickr May Set Legal Precedents*, FORTUNE (Dec. 2, 2017), [https://perma.cc/8MHV-E2YH] (describing allegations of Uber's use of Wickr).

322. Omnibus Order, *supra* note at 5.

323. *Id.* at 34.

324. *Id.*

325. *Id.* at 5.

326. *Id.*

example, in *Convolve, Inc. v. Compaq Computer Systems*,[327] automatically overwritten data was discoverable, but failure to preserve it was not sanctionable.[328] The court noted that no duty to preserve attached to the data at issue.[329] Similarly, in *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*,[330] automatic deletion of cached internet files was not sanctionable.[331] The court noted that such files are automatically replaced in a very short time and the company did not do anything to affirmatively delete files.[332]

A few criminal cases may offer insight into how ephemeral social media content may be handled in civil discovery. For Snapchat content that has been destroyed, cases seem to refer to the evidence based on testimony of witnesses who saw the communication in Snapchat before it was destroyed. For example, in *People in Interest of R.C.*,[333] a juvenile defendant, R.C., faced criminal disorderly conduct charges arising from a Snapchat photo of his friend's face, on which R.C., using the in-app drawing tool, drew an ejaculating penis.[334] The picture was described to the court by the three people who saw it, and footnote one of the opinion explains Snapchat and includes two screen grabs to show a non-offensive doodle on a selfie.[335] The court analyzed whether the image constitutes fighting words, at one point characterizing the image as "cartoonish" which, as the dissent points out, has no support in the record because the photo was destroyed.[336] Ultimately, the court held that the digital image, as described, did not amount to fighting words and thus was not sufficient for a breach of the peace claim.[337]

The fact that a Snapchat image has been destroyed does not preclude a finding of liability. In *People v. Harner*,[338] a criminal case,

327. 223 F.R.D 162 (S.D.N.Y. 2004).

328. *Id.* at 177.

329. *Id.*

330. 497 F. Supp. 2d 627 (E.D. Pa. 2007).

331. *Id.* at 642.

332. *Id.*

333. 2016 COA 166, ¶ 1, *cert. denied*, No. 16SC987, 2017 WL 5664821 (Colo. Nov. 17, 2016).

334. *Id.* at ¶ 3.

335. *Id.* at ¶ 3 n.1.

336. *Id.* at ¶ 14, ¶¶ 18–32.

337. *Id.* at ¶ 34; *see also N.L.O. v. State*, 222 So.3d 1196, 1201 (Ala. Crim. App. 2016) (Snapchat Story by defendant depicting gun and threatening message, along with other evidence, insufficient to establish guilt in burglary case against a juvenile); *L.Z. v. K.Q.*, No. A–4776–14T3, 2016 WL 3865840, at *5 (N.J. Super. Ct. App. Div. July 18, 2016) (Snapchat video supported Final Restraining Order against defendant who sent graphic Snapchat video to Plaintiff's contacts; court accepted testimony of plaintiff about video contents because video was destroyed and not in evidence).

338. No. 331122, 2017 WL 2683735, at *1 (Mich. Ct. App. June 20, 2017).

the defendant requested and received a nude photo of a minor via Snapchat.[339] He was convicted of criminal sexual conduct even though the Snapchat photo no longer existed: "[i]t is irrelevant that no such photographs were discovered on Harner's cellphone because his repeated requests for nude photographs, and not his receipt thereof, formed the basis for the offense."[340] Thus, the fact that the photo itself was not recoverable was of little consequence to the case itself.

Indeed, at least in the criminal context, courts are recognizing that ephemeral communication methods like Snapchat are beyond the purview of physical evidence. One California court notes that the intrusiveness of cell phone searches and other privacy-based constitutional challenges may be a non-issue in the future, as people move to self-destruct apps and fewer digital archives.[341] In a footnote, the court even notes that "had [defendant] used the popular app, 'Snapchat' to photograph the pile of money, this motion to suppress may have never been filed, since Snapchat photographs disappear within ten seconds."[342] Nonetheless, the scope of preservation duties under the Federal Rules are not entirely clear. And legal ethics rules must also be considered.

B. Legal Ethics Rules

Preservation, in the broadest sense, is an ethical obligation of lawyers. This obligation includes a duty to advise clients about preservation and spoliation. The main rule on the ethics of preservation is Model Rule 3.4 of the ABA's Model Rules of Professional Conduct, which form the basis of many states' ethics rules.[343] Rule 3.4, Fairness to Opposing Party and Counsel, states that 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" nor "counsel or assist another person to do any such act."[344] The comments make clear that this rule equally applies to "computerized information."[345] It also contains a general requirement that lawyers obey the rules of the tribunal.[346] Rule 3.4 recognizes that

339. *Id.* at *2.

340. *Id.*

341. *United States v. Caballero*, 178 F. Supp. 3d 1008, 1018 n.9 (S.D. Cal. 2016).

342. *Id.*

343. *See Model Rules of Professional Conduct*, AM. BAR ASS'N, [https://perma.cc/PCN8-U88Y].

344. MODEL RULES OF PROF'L CONDUCT r. 3.4 (AM. BAR ASS'N 2014).

345. MODEL RULES OF PROF'L CONDUCT r. 3.4 cmt 2 (AM. BAR ASS'N 2014).

346. MODEL RULES OF PROF'L CONDUCT r. 3.4(c) (AM. BAR ASS'N 2016).

the right to access potential evidence in litigation is "an important procedural right"[347] and one that is crucial in an adversarial system of justice.[348]

Nonetheless, the comments to Model Rule 3.4 refer to "applicable law" as establishing specific obligations.[349] For example, Comment 2 expressly states that "[a]pplicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense."[350] With its general prohibition on destroying evidence and reference to applicable law, Rule 3.4 does little to define the scope of preservation duties for lawyers. Instead, it incorporates the substantive law and adds a parallel ethics rule that makes a substantive law violation an ethical issue. Thus, this Rule provides little guidance on when a duty to preserve is triggered, what constitutes spoliation of evidence, or when safe harbors kick in for good-faith destruction of potential evidence.

Some ethics advisory opinions have offered additional guidance on preservation of social media content in particular. These opinions are largely consistent with each other, and touch upon three important aspects of social media preservation: (1) advising about social media usage generally, (2) advising clients to change social media content or curate contents, and (3) allowing clients to delete social media content altogether.

First, as to social media usage in general, lawyers have an ethical duty to stay abreast of relevant technology and to advise clients about its risks and benefits.[351] This includes explaining the consequences of posting something on social media.[352] Lawyers may even formulate a social media policy with the client to help limit what the client posts.[353]

347. MODEL RULES OF PROF'L CONDUCT r. 3.4 cmt. 2 (AM. BAR ASS'N 2016).

348. MODEL RULES OF PROF'L CONDUCT r. 3.4 cmt. 1 (AM. BAR ASS'N 2016).

349. *Id.*

350. MODEL RULES OF PROF'L CONDUCT r. 3.4 cmt. 2 (AM. BAR ASS'N 2016). This comment also refers to applicable law allowing lawyers to take temporary possession of evidence in order to preserve it. *Id.*

351. *See* MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2016).

352. W. Va. Office of Disciplinary Counsel, *L.E.O. No. 2015-02: Social Media and Attorneys,* 9 [hereinafter W. Va. Office of Disciplinary Counsel], [https://perma.cc/7J4D-JBQM].

353. *See* N.Y. STATE BAR ASS'N, SOCIAL MEDIA ETHICS GUIDELINES OF THE COMMERCIAL AND FEDERAL LITIGATION SECTION OF THE NEW YORK STATE BAR ASSOCIATION 23 (2017), [https://perma.cc/ACE5-768U] (referencing Guideline No. 5.B); *see also* N.Y. Cty Lawyer Ass'n, *NYCLA Ethics Opinion 745: Advising a Client Regarding Posts on Social Media Sites*, 3–4 (2013) [hereinafter *NYCLA Ethics Opinion*

Second, lawyers may advise clients to increase or change privacy settings to limit the audience for their social media posts.[354] But it may be necessary to preserve content before making changes. For example, the New York State Bar guidelines state that lawyers can advise clients to change privacy settings, even after litigation is pending, but recognizes that preservation duties may require that the account be preserved before doing so:

> [n]or is there any ethical bar to advising a client to change her privacy or security settings to be more restrictive, whether before or after a litigation has commenced, as long as social media is appropriately preserved in the proper format and such is not a violation of law or court order.[355]

Lawyers are also able to advise clients about what to post on social media, but they cannot advise clients to falsify records and, if false records are created, cannot use them in court.[356] While lawyers can advise clients what new (and favorable) content to post on social media, clients should not post knowingly false or misleading content.[357] The guideline notes that lawyers may want to regularly monitor their clients' social media usage to monitor their posts.[358]

Third, several opinions state that lawyers can even advise clients to delete social media content, with some caveats. The West Virginia bar, for example, states that deletion is allowed as long as potentially relevant content is first preserved.[359] Similarly, the New York State bar

745], [https://perma.cc/7MP5-SDNP] (lawyers have a duty to consult clients about social media).

354. W. Va. Office of Disciplinary Counsel, *supra* note 352, at 9; *See* N.Y. STATE BAR ASS'N, *supra* note 353, 22–23 (referencing Guideline No. 5.A. and how lawyers may advise clients to tighten up social media privacy settings); *see also* Prof'l Ethics Fla. Bar, *Proposed Advisory Opinion 14-1*, 1 (Jan. 23, 2015) [hereinafter *Fla. Proposed Advisory Opinion 14-1*], [https://perma.cc/V52Y-C4CW] (lawyers may advise clients about optimal social media privacy settings).

355. N.Y. STATE BAR ASS'N, *supra* note 353, at 22–23 (comment to Guideline No. 5.A.).

356. W. Va. Office of Disciplinary Counsel, *supra* note 352, at 9.

357. N.Y. STATE BAR ASS'N, *supra* note 353, at 23 (citing Guideline No. 5.B.). The guideline permits the lawyer to "counsel the client to publish truthful information favorable to the client." *Id.*

358. *Id.* n.89.

359. W. Va. Office of Disciplinary Counsel, *supra* note 352, at 9 ("Although attorneys may instruct their clients to delete information from the clients' social media pages that may be damaging to the clients, provided the attorneys' conduct does not constitute spoliation or is otherwise illegal, attorneys must take the appropriate steps to preserve the aforementioned information in the event that it is deemed discoverable or becomes relevant to the clients' cases."); *see also NYCLA Ethics Opinion 745*, *supra*

also notes that deletion is allowed but, if a duty to preserve applies, an "appropriate record of the social media information or data" should be first.[360] The comments to this guideline further explain preservation duties, noting that the duty to preserve is triggered when litigation is reasonably anticipated, as defined by substantive law.[361] The comment further states that "a lawyer may more freely advise a client on what to maintain or remove from her social media profile" when litigation is not pending or reasonably anticipated.[362]

The Federal Rules of Civil Procedure and legal ethics rules and guidelines, when read together, provide little guidance on preservation duties for ephemeral content. Given that most ephemeral content is inaccessible ESI, the Federal Rules seem to acknowledge that preservation of this category of ESI in many contexts is impractical and not warranted when balancing costs with the needs of the case. Further, the legal ethics rules and guidelines do not impose independent preservation duties and instead incorporate other, substantive law to define what must be preserved and when the duty arises. Together, these sources provide unclear guidance on what litigants and lawyers should do to avoid negative consequences from disappearing data.

IV. TOWARD A BALANCED APPROACH TO DISAPPEARING DATA

Civil discovery norms will need to adapt to the shift to disappearing data. The trend towards ephemeral apps and smaller digital footprints is a positive development and one that plays an

note 353, at 3–4 (deletion permitted as long as duty to preserve met); *Fla. Proposed Advisory Opinion 14-1*, *supra* note 354, at 2–3; N.C. State Bar, *2014 Formal Ethics Opinion 5* (July 17, 2015), [https://web.archive.org/web/20180226012746/https://www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2014-formal-ethics-opinion-5/]; Pa. Bar Ass'n, *Formal Opinion 2014-300: Ethical Obligations for Attorneys Using Social Media*, 7 (2014), [https://perma.cc/H934-FLS7]; Phila. Bar Ass'n Prof'l Guidance Comm., *Opinion 2014-5*, 5 (2014), [https://perma.cc/J7LM-JL8K].

360. N.Y. STATE BAR ASS'N, *supra* note 353, at 22 (comment to Guideline No. 5.A.).

361. *Id.* (comment to Guideline No. 5.A.); *see also Fla. Proposed Advisory Opinion 14-1*, *supra* note 354, at 2 (the duty to preserve may begin when a lawyer is hired to assess a potential claim).

362. N.Y. STATE BAR ASS'N, *supra* note 353, at 22 (comment to Guideline No. 5.A.); *see also NYCLA Ethics Opinion 745, supra* note 353, at 4 (lawyers can warn clients about future social media posts without "facilitat[ing] the client's publishing of false or misleading information that may be relevant to a claim" and can advise the client to increase privacy settings or even delete content "[p]rovided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence").

important role in privacy self-regulation. Technology companies, through privacy-by-design principles, strive to make platforms that minimize data creation and retention.[363] These companies also rely on behavioral interventions, which steer users to choose certain privacy-enhancing options within an application.[364] The result is that more data is fleeting in nature, which is positive in slowing the big data trend—but challenging in the context of civil discovery.

The scope of civil discovery is broad and potentially includes all forms of ESI.[365] But civil discovery should not stunt the progress the technology sector is making in reducing the volume of data created and retained. Onerous preservation schemes run the risk of penalizing individuals and companies who are following the important trend of data minimization. Even though digital crumbs may be left behind with new ephemeral applications,[366] the mere fact that the industry is shifting to forms of communication that mimic in-person conversation should be taken into account when crafting discovery and preservation limits.

Therefore, the Federal Rules should continue down the path of eliminating sanctions and other penalties for good-faith deletion of certain ESI. And courts applying discovery rules should recognize that ephemeral content is a fleeting form of inaccessible ESI that, though discoverable, rarely need be preserved.[367] Like the cases recognizing that preservation duties fall short of requiring parties to archive transitory, ephemeral content,[368] disappearing data, in general, may be beyond the scope of preservation in many cases. Such an approach is

363. *See supra* note 1 and accompanying text (defining privacy by design).

364. *See supra* note 2 and accompanying text.

365. *See generally* FED. R. CIV. P. 34(a).

366. Snapchat allows for saving some Snaps. *See How to Use My Eyes Only*, *supra* note 97. Additionally, Snapchat's representations about auto-deletion have resulted in FTC action. *See* Complaint at 1, 3–4, *In the Matter of Snapchat, Inc.* (F.T.C. Feb. 23, 2014) (No. C-4501).

367. While loss of ephemeral content may constitute prejudice, communications sent via ephemeral applications may be captured by one of the recipients of the communication (via a picture taken by another device or, in some applications, through a screen capture using the receiving device). *See supra* note 99 (describing screen captures in Snapchat). And those that saw the ephemeral communication may be able to testify about it, provided hearsay rules do not bar the testimony. *See generally* FED. R. EVID. 801–07 (Article VIII of the Federal Rules of Evidence outlines the rules for hearsay). As with conversations, ephemeral digital communication may also be adequately handled through circumstantial or parol evidence. *See generally* FED. R. EVID. 401–10 (Article IV of the Federal Rules of Evidence outlines the rules for circumstantial and parol evidence).

368. *See Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ.5316 RMB MHD, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (no duty to save chatroom conversations).

fair and balanced in light of industry privacy-by-design goals and the particular concerns of individual litigants and corporate interests.

For individual litigants, civil discovery should consider the fact that normal usage of technology involves altering or deleting social data. To impose onerous preservation duties is to hinder individual freedom of expression and free use of social media platforms.[369] For corporate litigants, over-preservation has been identified as a serious problem by some, and one that can be addressed through a fair and balanced approach to ephemeral data preservation.[370] At the same time, overly onerous rules are not the solution because they will lead to over-preservation and a possible decline in industry trends towards greater privacy.

A. Fairness for Individual Litigants

Individuals are now the unwitting stewards of vast digital archives, some of which consist of dynamic content subject to change or deletion. The challenges posed by disappearing data are especially pronounced for individual litigants, who are unlikely to think through a personal retention policy or otherwise proactively understand and address their data habits.[371] And the civil discovery rules may not be designed to best handle small, individual actions. The result is a confusing landscape for unsophisticated parties, which bolsters the need for a fair and balanced approach to disappearing data.

The civil discovery rules seek to minimize cost and inefficiencies in litigation.[372] Recent changes highlight the continued commitment to reducing costs and burden, such as through the proportionality factors now prominently featured in Rule 26's definition for civil discovery's scope.[373] But the quest for efficiency and cost reduction may disparately impact small cases and individual litigants, as opposed to corporations

369. *See generally Packingham v. North Carolina*, 137 S. Ct. 1730, 1735–37 (2017) (describing how vital social media has become as a forum for expression and communication, so that the First Amendment protects social media access and speech rights).

370. *See, e.g.*, *Risk Aversion*, *supra* note 8, at 538.

371. Some data habits are influenced by behavioral interventions built into social media platform design, as part of a privacy-by-design effort. *See* Hartzog & Stutzman, *supra* note 1, at 411–12.

372. *See* FED. R. CIV. P. 1 ("[The Federal Rules] should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding."); *see also* Steven S. Gensler, *Justness! Speed! Inexpense! An Introduction to the Revolution of 1938 Revisited: The Role and Future of the Federal Rules*, 61 OKLA. L. REV. 257, 267–69, 271 (2008).

373. *See* FED. R. CIV. P. 26(b)(1); see *supra* Section II.B.

and complex cases.[374] Indeed, scholars have observed that those who serve on committees or otherwise influence the rulemaking process disproportionately represent the defense bar.[375] As a result, the rules may be written with the concerns of large, corporate litigants and complex cases in mind—concerns that do not necessarily align with those of individual litigants.[376] Instead, the rules often harm individual litigants who have a harder time accessing the proof they need to maintain claims.[377]

Because the ESI rules are written with corporate litigants in mind, in many ways they fail to take into account the ways in which the average person uses technology. But even an individual litigant now possesses or controls ESI; it is their data stored in the cloud (via web services or mobile apps), on a home computer, on external hard drives or other data storage devices, and on mobile devices (like tablets and smartphones).[378] And included within the umbrella of ESI is their social media content.[379]

Social media is a key example of why disappearing data is a special problem for individual litigants. An avid social media user may create dozens of comments and pictures in several applications a day.[380] Because social media accounts are dynamic, non-static data sets, normal usage may include changing or deleting old posts. And the use of ephemeral apps like Snapchat is on the rise, further enabling individuals to create ephemeral content and disappearing data.

But preservation duties are not obvious to individuals, and lawyers may be derelict in their duties to properly advise individual litigants about spoliation.[381] Courts have already found social media spoliation in

374. Coleman, *supra* note 11, at 1007–12.

375. *Id.* at 1022 (noting the various ties between large corporate entities and the influencers who provide input on the Federal Rules and their interpretation by courts); *see also* Patricia W. Hatamyar Moore, *The Anti-Plaintiff Pending Amendments to the Federal Rules of Civil Procedure and the Pro-Defendant Composition of the Federal Rulemaking Committees*, 83 U. CIN. L. REV. 1083, 1144–52 (2015) (analyzing the membership of the Civil Rules Committee and how the members' conservative ideological biases and corporate affiliations likely influence the rules the committee promulgates).

376. See Coleman, *supra* note 11, at 1015–19.

377. *Id.* at 1009–10.

378. *See Risk Adverse*, *supra* note 8, at 540–42.

379. *See, e.g.*, *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010) (listing "social networking-websites" as ESI discovery).

380. *See* GREENWOOD, PERRIN & DUGGAN, *supra* note 5, at 10 (explaining that many online adults who use social media tend to use more than one platform).

381. *See, e.g.*, *Cajamarca v. Regal Entm't Grp.*, No. 11 Civ. 2780 (BMC), slip op. at 5 (E.D.N.Y. Aug. 31, 2012) (plaintiff's counsel sanctioned for frivolous claim). In *Cajamarca*, the plaintiff's counsel failed to advise the plaintiff in her sexual harassment claim about preserving data stored on her laptop. *Id.* at 2. The plaintiff

some cases involving an individual who destroyed social media content intentionally or inadvertently.[382] While spoliation is obvious with purposeful destruction of ESI with the intent of depriving an adversary of it in litigation,[383] less egregious violations may be a function of platforms and not intentional bad acts by account-holders. And social media is an important tool of self-expression that is integrated into nearly all aspects of one's life.[384] The result is that onerous preservation schemes will impact the freedom of individuals who are using social media in its intended way as an ordinary user. Thus, courts should be wary of taking too broad an approach as to the preservation of disappearing data.

B. Balancing Concerns as to Corporate Litigants

Even though many of the civil discovery rules are tailored to address issues arising with businesses or other large entities, disappearing data is a new challenge for corporate litigants as well. Some scholars point out that the rules, when amended, are tailored to deal with the concerns of businesses (as opposed to individual litigants) and thus focus disproportionately on business needs.[385] But preservation costs for companies, and concerns of over-preservation, have had a major, negative impact on companies in the last decade.[386] The 2015 amendments are intended to alleviate some of the problems associated with over-preservation,[387] but clarity is still needed as to disappearing data.

---

deleted content from her hard drive that would have been relevant to her claims, in particular the extent of her injuries. *Id.* at 5 (noting that, with access to the deleted content, "the tenuousness of [plaintiff's] damages claim would likely have become even more apparent and might well have resulted in the withdrawal or nominal settlement of the claim").

382. *See, e.g.*, *Painter v. Atwood*, No. 2:12-cv-01215–JCM–RJJ, 2014 WL 1089694, at *6 (2014); *Patel v. Havana Bar, Rest., & Catering*, No. 10-1383, 2011 WL 6029983, at *6 (E.D. Pa. Dec. 5, 2011).

383. *See, e.g.*, *Allied Concrete Co. v. Lester*, 736 S.E.2d 699, 702 (Va. 2013).

384. *See* Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 586–87 (2014); Woodrow Hartzog, *The Value of Modest Privacy Protections in a Hyper Social World*, 12 COLO. TECH. L.J. 333, 345–46 (2014).

385. *See* Coleman, *supra* note 11, at 1009, 1018, 1027.

386. *See generally* INST. FOR THE ADVANCEMENT OF THE LEGAL SYS., FINAL REPORT ON JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND THE INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM (2009), [https://perma.cc/S2F2-JGNA] (discussing the prohibitive expense and inefficiency of e-discovery); *Risk Aversion*, *supra* note 8, at 540, 542, 545–46.

387. FED. R. CIV. P 37(e) advisory committee's note to 2015 amendment.

The nature of data, availability of storage, and risk-averse policies have all contributed to the over-preservation problem. First, large enterprises create more digital content than ever before.[388] Companies now have data that is stored on computers, servers, removable media like USB drives and external hard drives, in cloud storage, on backup tapes, and on personal devices.[389] All aspects of business may create a digital record, which is replicated and possibly stored in multiple locations.[390] And the most ephemeral of communication forms, in-person conversation or an unrecorded phone call, have been replaced with texting, emailing, and other digital communication.[391] The trend has been for physical data to supplant traditionally ephemeral communications.[392]

Second, an enterprise's capacity to store these new forms of digital content has exploded as well. Companies expand and build technology infrastructures or rely on renting additional storage capacity in the cloud, so that data can be accessed and shared online among workers and outside entities.[393] And the promised utility of "big data" motivates some companies to save even more electronic content in the hopes of analyzing it and capitalizing on it.[394]

But the increased amount of digital content, coupled with the ability to store more of it, has also lead to pressures to preserve and archive.[395] Preservation duties, as defined by common law but giving rise to myriad sanctions for spoliation, are not sufficiently clear in many contexts.[396] And large companies may have multiple litigation holds in effect at any given time.[397] Fear of adverse impact in litigation motivates companies to over-preserve, often at great cost and burden.

Thus, the 2015 changes to Rule 37 are a welcome revision for many businesses, as the new rule seeks to eliminate the harshest sanctions for inadvertent or good-faith deletion of electronic content. And elevation of proportionality as a limit on discovery also serves

388. *Risk Aversion*, *supra* note 8, at 539–40 (providing an example of one international energy firm, which as of 2005, had 800 terabytes of information stored, including 5.2 million emails generated a day and from over 100,000 computing devices across hundreds of worldwide offices).

389. *Id.* at 539–41.

390. *Id.* at 540–41.

391. *Id.* at 541–42.

392. *Id.*

393. *See id.*

394. *Id.* at 542.

395. *Id.* at 542–43.

396. *Id.* at 543.

397. *Id.* at 543–44.

corporate interests.[398] But the boom of ephemeral content and disappearing data is also affecting businesses and their record retention practices. Apps like Confide[399] and Wickr[400] provide ephemeral communication options marketed and designed specifically for businesses.

But the civil discovery rules and their application should recognize that a return to ephemeral communication—albeit in a fleeting digital form—is a natural and positive shift away from the explosion of permanent digital records for all categories of content. The capability to choose a communication form that leaves a digital record (like an email) does not mean spoliation occurs by going with an ephemeral form (like in-person conversation) instead. And new technologies offering disappearing data are seeking to closely replicate live conversation in a more convenient transmittal method.[401]

Stonewalling, however, is also a concern.[402] On the one hand, corporate litigants want to end the over-preservation problem, but on the other hand, they risk facing discovery abuses that stem from skirting preservation duties. Rule 37's bad-faith standard is a move in the right direction for recognizing that corporate litigants cannot shirk preservation duties through disappearing data tools.[403] Fair boundaries need to be created, and ones that do not allow corporate malfeasance.

Fortunately, other regulations and sector-specific standards already exist to require or incentivize fair data practices. For example, certain financial records in the mortgage industry must be retained for three years.[404] In the employment context, the Occupational Safety and Health Standards contain requirements for keeping personnel records,

398. *See generally* COMM. ON RULES OF PRACTICE & PROCEDURE, REPORT OF THE JUDICIAL CONFERENCE, at app. B-5 (2014), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2014.pdf [https://perma.cc/4MU8-99A2]; *see also* Thomas Y. Allman, *Local Rules, Standing Orders, and Model Protocols: Where the Rubber Meets the (e-Discovery) Road*, RICH. J.L. & TECH. at 1, 23–24 (2013) (describing local initiatives to make e-discovery more fair and affordable).

399. CONFIDE, *supra* note 138 (describing the levels of front-end privacy features, like word-by-word disappearing text, and back-end privacy safeguards, like end-to-end encryption).

400. *See WICKR*, *supra* note 150.

401. *See, e.g.*, *Privacy Policy*, *supra* note 113 (describing how deletion is Snapchat's default design and that it is intended to replicate the ephemeral nature of real-time conversations).

402. *See, e.g.*, Nesson, *supra* note 243, at 795–98 (describing the incentives lawyers have to engage in spoliation and the challenges of assessing how common—and detrimental to fairness—spoliation is in civil litigation).

403. *See* FED. R. CIV. P. 37(e)(2).

404. 12 U.S.C. 2803(j)(6) (2012).

payroll information, tax data, and other specific files.[405] The financial sector remains highly regulated, and the Federal Deposit Insurance Corporation has "record retention requirements" that contemplate specific record retention policies.[406] And health data must comply with record requirements as outlined in the "security rule" of the Health Care Portability and Accountability Act.[407] Under these and other provisions, specific industries are held to record creation and retention requirements or expectations. As a result, the risk of using ephemeral apps in lieu of business records is minimized.

Thus, a fair and balanced approach to disappearing data furthers the business need to reduce over-preservation and allows a return to ephemeral conversations. While stonewalling is a concern, other substantive law mandating record-keeping and industry norms for data retention serve as one layer of protection against corporate malfeasance. Further, The Federal Rules still provide a wide panoply of remedies for bad-faith conduct, which should still deter intentional acts of spoliation.[408] Therefore, onerous preservation duties of ephemeral data are not warranted.

CONCLUSION

Civil discovery norms promote broad discovery, but within limits. ESI, in particular, poses unique challenges due to the way it is created, stored, and destroyed. These challenges are now even greater due to the boom of ephemeral social media apps, like Snapchat, and business-specific ephemeral communication tools, like Confide. In particular, preservation duties and the boundaries of spoliation need to be considered in this new era of ESI. Thus, courts should be wary of imposing broad preservation duties for ephemeral content.

As a starting point, the trend towards ephemeral apps represents a positive industry trend of minimizing data. Privacy by design provides ways to promote privacy in the very design of new technologies. This trend represents the future of ESI and should be fostered. But the Federal Rules of Civil Procedure and other rules require preservation

405. *See* Occupational Safety and Health Standards, 29 C.F.R. 1910 (2017); OSHA, *A Brief Guide to Recordkeeping Requirements for Occupational Injuries and Illnesses*, U.S. DEP'T LAB., [https://perma.cc/8HZK-SCUE].

406. *See* 12 C.F.R. § 380.14 (2017) (noting that companies need internal policies that conform to regulators' requirements for document retention); *see also* Fin. Indus. Regulatory Authority, Inc., FINRA Manual Section 3110, [https://perma.cc/UVB6-LUK8]; SEC Rule 17-A4, 240 C.F.R. § 240.17(a)–(b)(4) (2017) (requiring members to keep records of instant messages for three years).

407. *See* HIPPAA Privacy Rule, 45 C.F.R. §§ 160, 164(A), (E) (2017).

408. *See* FED. R. CIV. P. 37.

of some electronic content, and litigants who use platforms that facilitate disappearing data may fear that they run afoul of preservation rules.

Onerous preservation duties run the risk of making the Federal Rules out of step with technological realities. And civil discovery norms may unnecessarily steer businesses away from privacy by design and data minimization. The key, then, is to avoid imposing overly broad preservation duties of disappearing data. By doing so, both individual and corporate litigants will benefit from a fair and balanced approach, and important privacy objectives through data-minimizing design goals will not be undermined.