The University of Akron
IdeaExchange@UAkron

Akron Law Review | Akron Law Journals

June 2018

Self-Destruct Apps: Spoliation by Design?

Agnieszka McPeak

Please take a moment to share how this work helps you through this survey. Your feedback will be important as we plan further development of our repository.
Follow this and additional works at: http://ideaexchange.uakron.edu/akronlawreview

 Part of the Civil Procedure Commons

Recommended Citation
McPeak, Agnieszka (2017) "Self-Destruct Apps: Spoliation by Design?," *Akron Law Review*: Vol. 51 : Iss. 3 , Article 5.
Available at: http://ideaexchange.uakron.edu/akronlawreview/vol51/iss3/5

This Article is brought to you for free and open access by Akron Law Journals at IdeaExchange@UAkron, the institutional repository of The University of Akron in Akron, Ohio, USA. It has been accepted for inclusion in Akron Law Review by an authorized administrator of IdeaExchange@UAkron. For more information, please contact mjon@uakron.edu, uapress@uakron.edu.

SELF-DESTRUCT APPS: SPOLIATION BY DESIGN?

*Agnieszka McPeak**

I. INTRODUCTION

This Article analyzes the impact that ephemeral or "self-destruct" apps, like Snapchat, have on civil discovery and identifies a tension between privacy policy and preservation duties. Under privacy principles in the United States and Europe, technology companies are encouraged—and at times mandated—to build privacy-enhancing features into the very design of new technology. This concept, often called "privacy by design," is a positive trend that reduces the amount of data created and retained by platforms and intermediaries. Ephemeral apps, like Snapchat and Confide, embody privacy by design by offering self-destructing communication tools that mimic live conversation and avoid permanent records. At the same time, the Federal Rules of Civil Procedure (Federal Rules) contemplate broad access to relevant information, including electronically stored information (ESI). Information that is within the scope of discovery is also subject to a preservation duty. Failure to preserve can amount to spoliation, with potentially serious consequences in litigation.

The Federal Rules recently expanded safe harbors for good-faith deletion of ESI, recognizing that the explosion of digital data has led to concerns of over-preservation. But courts will need to determine the scope

* Associate Professor of Law, University of Toledo. This project benefitted greatly from the support of the University of Toledo URFO Summer Research Award and Fellowship.

Published by IdeaExchange@UAkron, 2017

of preservation duties with a new and unique form of electronic communication: ephemeral apps. As ephemeral apps continue to gain popularity, there exists a risk that onerous preservation duties will be out of step with privacy-by-design initiatives.

This Article explores the tension between privacy by design, as embodied by ephemeral apps, with the scope of preservation duties in civil discovery. Specifically, Section II begins by examining the increasing usage of ephemeral apps resulting from evolving market demands for privacy. Section III discusses how ephemeral apps, as a form of ESI, fit within the scope of civil discovery, and Section IV examines the duty to preserve potentially relevant ESI pursuant to the Federal Rules. Section V then considers the impact ephemeral apps, which tend to mimic live interaction rather than electronic records, may have on existing civil discovery limits. Lastly, Section VI concludes by cautioning against characterizing ephemeral apps as spoliation by design: onerous or overly expansive preservation duties for self-destructing content are not warranted or desirable.

II. EPHEMERAL APPS AS PRIVACY BY DESIGN

"Ephemeral" or "self-destruct" apps allow users to send messages, pictures, videos, or other communication in a format that automatically deletes content.[1] Snapchat, for example, is a fast-growing ephemeral social network and is especially popular among 13- to 24-year-olds, but is gaining ground among older demographics as well.[2] Apps like Snapchat

1. Snapchat allows users to send content to all their contacts, to a subset of contacts, or to a single recipient. *See Privacy Policy*, SNAPCHAT, https://www.snap.com/en-US/privacy/privacy-policy/ [http://perma.cc/Z3BF-ZQ3D] (last visited Sept. 28, 2017). Content sent within the app is not automatically saved to the sender's profile or account, and it defaults to automatically disappear from the recipient's view within seconds as well. *See id.* It is this disappearing nature of messages that makes Snapchat an ephemeral app. *See id.*

2. Hannah Kuchler & Tim Bradshaw, *Snapchat's Youth Appeal Puts Pressure on Facebook*, FINANCIAL TIMES (Aug. 21, 2017), https://www.ft.com/content/07e4dc9e-86c4-11e7-bf50-e1c239b45787 [http://perma.cc/BG8X-EMFW]; s*ee also* Shannon Greenwood, Andrew Perrin, & Maeve Duggan, *Social Media Update 2016*, PEW RESEARCH CTR., INTERNET & TECH. (Nov. 11, 2016), http://www.pewinternet.org/2016/11/11/social-media-update-2016/ [http://www.pewinternet.org/2016/11/11/social-media-update-2016/]. According to the Pew Research Center, 72% of all adults use a smartphone. Of those, 24% specifically use messaging apps that auto-delete, like Snapchat. *Id.* However, when broken down by age, 56% of 18- to 29-year-olds use auto-delete apps, while only 13% of those age 30 to 49 and 9% of those over 50 use them. *Id.* Overall, online adults have dramatically increased their social media usage over the last decade: In 2005, only 7% used any form of social media. Andrew Perrin, *Social Media Usage: 2005-2015*, PEW RESEARCH CTR., INTERNET & TECH. (Oct. 8, 2015), http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ [http://perma.cc/JKA9-ZET5]. In 2015, the number jumped ten-fold to 65%. *Id.*

mark an important shift towards greater privacy (or at least obscurity)[3] in social networking technology: Snapchat embraces the principle of privacy by design in its corporate philosophy,[4] front-end user features,[5] and back-end data creation and retention policies.[6]

Privacy by design is the idea that new technology should be designed with privacy as a key consideration from its inception, rather than as an afterthought.[7] It means privacy-enhancing features are part and parcel of the app itself. For example, an app can minimize the amount of data it asks for, reduce what is stored, and provide cues to users to choose privacy-promoting practices when available.[8] By thinking about privacy design features from the onset, creators can avoid excessive data creation and retention.

But privacy by design is not just an industry goal. It is also an important facet of privacy policy and regulation in the United States and

---

3. *See* Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 411-12 (2013) (describing how, in the social media context, privacy by design means designing ways for users to maintain some level of obscurity).

4. According to Snapchat's website, deletion is its default:

> Just like talking to someone in person or on the telephone, having a conversation through Snaps and Chats allows you to express whatever is on your mind at the time, without automatically creating a permanent record of everything you've ever said. Of course, you can also choose to save a Snap before you send it and recipients can always take screen-shots—Snapchat makes it easy to save what's important and discard the rest.

See Our Approach to Privacy, SNAPCHAT, https://www.snap.com/en-US/privacy/our-approach/ [http://perma.cc/WRZ6-XABR] (last visited Sept. 28, 2017).

5. Snapchat users are able to select how long certain messages are visible, with options ranging from one second to 24 hours depending on how the content is sent or posted. *See Snapchat Support, How to Create and Send Snaps*, SNAPCHAT, https://support.snapchat.com/en-US/a/create [http://perma.cc/3LS7-5D7S] (last visited Sept. 28, 2017). Notably, Snapchat lets users set some messages to "infinity" so that it only disappears after the message is closed. *See id.* Snapchat also lets users save the content they created themselves to a "Memories" folder that can sync with the phone's camera roll. *See About Memories*, SNAPCHAT, https://support.snapchat.com/en-US/article/using-memories [http://perma.cc/9UEY-7KKD] (last visited Sept. 28, 2017).

6. On the back end, Snapchat does not store user-generated content on its servers for long durations. Instead, Snapchat proclaims that "delete is our default" and strives to delete content from its servers shortly after messages are viewed. *See Snapchat Support, When Does Snapchat Delete Snaps and Chats*, SNAPCHAT, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted [http://perma.cc/H3CP-M88W] (last visited Sept. 28, 2017); *see also Retrieve a Copy of a Snap*, SNAPCHAT, https://support.snapchat.com/en-US/a/snap-content [http://perma.cc/6EVE-UATV] (last visited Sept. 28, 2017) ("[E]xpired Snaps typically cannot be retrieved from Snapchat's servers by anyone, for any reason. In most cases, opened Snaps are automatically deleted once they have been viewed or have expired. Also, any unopened Snaps are deleted after 30 days.").

7. "Privacy by design" has been described as "a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture." Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1421 (2011).

8. *See id.* When an app is designed, certain cues can be built in to steer the user to choices that maximize privacy and minimize data disclosures by the user. *See also* Hartzog & Stutzman, *supra* note 3.

in Europe. The Federal Trade Commission, the U.S. agency that has taken the lead in regulating privacy and protecting consumers, has issued a report that includes privacy by design as an industry best-practice goal.[9] The Department of Commerce has also issued a Green Paper that outlines a consumer privacy initiative that includes privacy by design as a goal.[10] In Europe, the General Data Protection Regulation (GDPR)—once it is implemented—will mandate privacy by design as one of many consumer protection features, and U.S. companies will likely meet the higher standards of the GDPR in order to participate in the global marketplace.[11]

In the context of social media, privacy by design may take the form of promoting obscurity and minimizing data retention.[12] Social media, by its very nature, requires sharing and disclosing personal information. But even social media platforms can use privacy-promoting design features such as allowing pseudonyms, nudging users into disclosing less, and retaining fewer records of past posts.[13]

Snapchat is a key example of privacy by design in a social media app, given that its core feature is the self-destructing message. Indeed, users can share disappearing text, photos, or videos with all their contacts, smaller audiences, or one-on-one exchanges.[14] This means no record is automatically kept on the user-end of the app once the message disappears.[15] On the back end, Snapchat retains content for a few hours or up to a month for certain types of messages.[16] This is a significant departure from other social media platforms, like Facebook, which keeps a detailed archive of users' timelines, chats, and other content.[17]

Snapchat's model is not only gaining popularity for individual users.

9. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [http://perma.cc/9K72-P9KM].

10. DEP'T OF COM. INTERNET POL'Y TASK FORCE & DIGITAL ECONOMY LEADERSHIP TEAM, FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS 27-31 (2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf [http://perma.cc/RU84-9EMT].

11. *See* European Parliament & Council Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art. 25, Data Protection by Design and by Default, 2016 O.J. (L 119) 48.

12. *See* Hartzog & Stutzman, *supra* note 3.

13. *See id*.

14. *See* sources cited *supra* note 5.

15. *See* sources cited *supra* note 5.

16. *See* sources cited *supra* note 6.

17. This detailed archive is available for download by the account-holder directly. *See Downloading Your Info*, FACEBOOK, https://www.facebook.com/help/131112897028467 [http://perma.cc/TC3T-GHRS] (last visited July 6, 2017).

Ephemeral apps are now popping up in other contexts as well. Vaporstream[18] and Confide[19] are a few lead examples. Confide has a similar self-destruct design as Snapchat, but without the filters, lenses, and other frills.[20] It touts itself as a confidential messaging tool that enables users to send confidential information without creating a digital record of it: "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."[21] Similarly, Vaporstream offers ephemeral messaging for businesses in various industries.[22] Notably, Vaporstream claims that it provides options for retaining some content in order to comply with sector-specific regulations on information governance.[23]

Taken together, ephemeral apps demonstrate that a market demand for self-destructing electronic communication tools exists, and that privacy by design is a realistic model for social media apps. In addition, the popularity of apps like Snapchat is a positive development for both individual users and businesses. Individual users may very well recognize the benefits of smaller digital footprints and the erosion of privacy that data creation and use poses, which may explain the market demand for ephemeral apps. Social media is a key tool for self-expression and communication; formats that allow greater anonymity and less permanence may facilitate more openness and freedom.[24] For businesses, the last decade saw an explosion in the amount of data created and stored by companies.[25] Ephemeral communication tools may help ease the burden of managing massive amounts of data.[26]

---

18. *See Vaporstream*, VAPORSTREAM, https://www.vaporstream.com/ [http://perma.cc/S8AQ-JJRM] (last visited July 6, 2017).

19. *About Confide*, CONFIDE, https://getconfide.com/ [http://perma.cc/WCB7-E8T3] (last visited July 6, 2017) (describing the levels of front-end privacy features, like word-by-word disappearing text, and back-end privacy safeguards, like end-to-end encryption).

20. *See id.*

21. *Id*.

22. *See Vaporstream*, *supra* note 18.

23. *See Compliance*, VAPORSTREAM, https://www.vaporstream.com/product/compliance/ [http://perma.cc/9ZB9-6533] (last visited July 6, 2017).

24. The Supreme Court of the United States recently noted that social media is an important forum for self-expression, and one that is protected by the First Amendment. *See generally* Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

25. *See* Kenneth J. Withers, *Risk Aversion, Risk Management, and the "Overpreservation" Problem in Electronic Discovery*, 64 S.C. L. REV. 537, 540 (2013). Withers describes how, in 2005, one multi-national corporation had over 800 terabytes of information stored across hundreds of locations worldwide. *Id.*

26. *See id.* Traditional ephemeral communication tools, like in-person conversations and phone calls, have been replaced by texting, emailing, or other digital tools that expand the volume of

But as ephemeral apps grow in popularity, the Federal Rules must also account for their use and popularity. The question then becomes: are these apps simply spoliation by design?

III. CIVIL DISCOVERY OF EPHEMERAL APPS

Before addressing preservation and spoliation of ephemeral apps, it is important to define the scope of discovery for this new type of ESI. With a few exceptions, the Federal Rules permit ESI discovery to the full extent of traditional, physical content.[27] This means that ESI is discoverable if it is unprivileged and "relevant to any party's claim or defense."[28] The usual limits on discovery still apply, however. This means that discovery must not be cumulative, duplicative, obtainable from a better source, or disproportionate.[29] Three types of ESI are relevant to ephemeral apps: social media content, inaccessible ESI, and transitory, ephemeral data.

First, social media, in general, falls within the scope of ESI discovery.[30] Discovery requests for social media content tend to focus on the account-holders directly, and not on social media platforms.[31] Courts have struggled with creating meaningful boundaries for the scope of social media discovery, and jurisdictions tend to take different approaches for assessing what is discoverable. For example, some take the "factual predicate" approach, whereby the publicly-visible portions of the social media account must create a factual predicate to support the potential relevance of the private content.[32] Other courts focus on the reasonable particularity of the discovery request, looking at the specificity of the

corporate records. *Id.* at 541-42.

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

28. *Id.*

29. Proportionality has always been a concept contained in the Federal Rules, but after the 2015 amendments, it appears more prominently in Rule 26's scope of discovery. *See* FED. R. CIV. P. 26(b)(2)(c)(1). For an analysis of how the proportionality factors should be applied to protect against overly intrusive discovery of large digital archives, including social media, *see* Agnieszka McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235 (2015).

30. For a discussion of how courts should handle the scope of social media discovery, *see* Agnieszka McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887 (2013).

31. Social media platforms enable account-holders to download their entire account contents, which allows platforms to cut themselves out of the discovery process by referring third-party subpoena issuers to the account-holders directly as the better source of the information. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010).

32. *See, e.g.*, Romano v. Steelcase, Inc., 907 N.Y.S.2d 653 (2009) (allowing broad discovery of private Facebook content after defendant showed plaintiff's public profile picture contradicted her claims in the litigation).

discovery request and relevance of the content requested.[33] The "reasonable particularity" approach is the soundest.[34] Notably, some courts have taken an overly broad and all-inclusive approach to social media discovery, allowing complete access to entire accounts without much concern for relevance.[35] This last approach may even include forcing litigants to disclose their login credentials and passwords.[36]

Second, as to inaccessible ESI, the Federal Rules may require a showing of good cause before ordering discovery. The Federal Rules define inaccessible ESI as "not reasonably accessible because of undue burden or cost."[37] For example, ESI is inaccessible if it is stored in a format that requires recreation, defragmentation, restoration, or other sometimes-costly steps to make the data usable again.[38] Inaccessible ESI is still within the scope of discovery, but the Federal Rules add a good cause threshold as a requirement for discovery.[39] This means that a party who challenges discovery of ESI must show that it is inaccessible, and the party seeking discovery of inaccessible ESI then has the burden of showing good cause for the discovery.[40] If good cause exists, courts may grant discovery but also have options for shifting costs or otherwise defining the parameters of production.[41]

Lastly, courts have also examined the discoverability of transitory, ephemeral data, another category of ESI. Ephemeral data, in this context, has been defined as content that is temporary, transitory, and unintentionally created by the user.[42] Examples include server log data stored in random access memory (RAM) and internet cache files.[43] Courts

33. *See, e.g.*, EEOC v. Simply Storage, 270 F.R.D. 430 (S.D. Ind. 2010) (allowing some private social media content to be discovered in an employment discrimination case).

34. *See* Forman v. Henkin, No. 01015, 2018 WL 828101 (Ct. App. N.Y. Feb. 13, 2018) (rejecting the factual predicate approach); McPeak, *supra* note 30.

35. *See, e.g.*, Gallion v. Gallion, No. FA114116955S, 2011 WL 4953451 (Conn. Super. Ct. Sept. 30, 2011) (ordering family law litigants to exchange passwords to their Facebook accounts); McMillen v. Hummingbird Speedway, Inc., No. 113–2010 CD, 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010) (granting a motion to compel social media passwords in a personal injury case).

36. *See* cases cited *supra* note 35.

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

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

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

40. *Id.*

41. *Id.*

42. *See* Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. BALT. L. REV. 349, 367 (2008); JAY E. GRENIG & WILLIAM C. GLEISNER, III, eDISCOVERY & DIGITAL EVIDENCE, *Ephemeral Data* § 4:11, Westlaw (database updated March 2016); Jennifer H. Rearden & Farrah Pepper, *Oh No, Ephemeral Data! After 'Bunnell,' the Sky Has Not Yet Fallen*, N.Y.L.J., March 22, 2010, at § 6.

43. *See, e.g.*, Columbia Pictures Industries v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419 (C.D. Cal. May 29, 2007).

have held that ephemeral ESI still falls within the scope of discovery: transitory data is "stored" so as to fit within the definition of electronically *stored* information.[44] Thus, ephemeral ESI is not exempt from discovery, even though it is fleeting in nature.

Self-destruct app content is both social media and ephemeral ESI, and it may fit in the category of "inaccessible ESI" as well.[45] However, even though self-destruct apps fall within the scope of discovery, most substantive content likely no longer exists. For example, a request for Snapchat data to the account-holder will only yield basic account information and not the content of communications.[46] In general, Snap, Inc. itself does not archive the substance of user content.[47] In extreme cases, computer forensic tools can find some Snapchat content on the device that created it, but this would be a costly and inefficient step that may nonetheless yield very little substance.[48] Thus, in many ways, Snapchat mimics the ephemeral nature of real-time phone or face-to-face communication by minimizing the amount of data retained. This means fewer records exist, and there is less access to potentially relevant content in civil discovery. The question then becomes: is there a duty to preserve ephemeral data created and transmitted via ephemeral apps?

IV. PRESERVATION AND SPOLIATION OF ELECTRONICALLY STORED INFORMATION

If an item falls within the scope of discovery, litigants and lawyers may face a duty to preserve it once litigation is anticipated or pending.[49]

---

44. *See id.*

45. *What is Inaccessible ESI and How Does It Affect Costs?*, ILS (May 12, 2014), https://www.ilsteam.com/what-is-inaccessible-esi-and-how-does-it-affect-costs [http://perma.cc/58WQ-ZUPD].

46. Snapchat stores the following data within the app, which is accessible to the user: Username, current email address and phone number, birthday, name, Snapcode (profile picture), Snap privacy settings, Stories privacy settings, list of Friends (contacts), list of blocked Friends, and Snapcash transactions. *See My Data*, SNAPCHAT, https://accounts.snapchat.com/accounts/downloadmydata (last visited Sept. 28, 2017). Snapchat also lets users download additional account information, which includes account history, Snap Count (number of Snaps sent), "Local, Live, and Crowd-Sourced Content History and Information," purchase history, content and app engagement history, and demographic profile. *Id.*

47. *See Privacy Policy*, *supra* note 1.

48. *See* Kashmir Hill, *Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos from Android Phones*, FORBES (May 9, 2013, 4:51 P.M.), https://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/ [http://perma.cc/NL84-PDJU] (describing how computer forensics may be able to recover deleted Snaps on some devices).

49. Preservation duties draw from various sources of law, including criminal law, tort law, and legal ethics rules. *See, e.g.*, West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999)

Failure to meet a duty to preserve can lead to a multitude of repercussions for spoliation,[50] including sanctions under the Federal Rules.[51]

In the context of ESI, some unique preservation challenges emerge. The age of big data has drastically increased the volume of digital records that are created and capable of being stored.[52] Data may exist in many duplicative locations and forms.[53] Temporary files are created and deleted often, and other files need to be deleted over time to make room for new content.[54] Electronic storage systems move and delete content as part of their normal operation[55] and, at the same time, cloud storage and other technological innovations increase the amount of digital content that must be managed.[56] But as storage capacities increase, the cost of ESI preservation continues to be a major concern for companies.[57]

Generally, Federal Rule 37 outlines the duty to preserve in civil cases.[58] The current version of Rule 37(e), titled "Failure to Preserve Electronically Stored Information," provides some safe harbors for good-

("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."); *see* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 118 (AM. LAW INST. 2000) (describing criminal and negligent spoliation that can give rise to criminal or civil liability); *see* Eric M. Larsson, *Cause of Action for Spoliation of Evidence*, 40 CAUSES OF ACTION §§ 42–56 (2d ed. 2009) (listing the states that recognize an independent tort for spoliation of evidence).

50. *See, e.g.*, FED. R. CIV. P. 37.

51. *See* FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("New Rule 37(e) replaces the 2006 rule. It authorizes and specifies measures a court may employ if information that should have been preserved is lost, and specifies the findings necessary to justify these measures. It therefore forecloses reliance on inherent authority or state law to determine when certain measures should be used.").

52. *See, e.g.*, Meg Leta Ambrose, *Lessons from the Avalanche of Numbers: Big Data in Historical Perspective*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 201 (2015).

53. *See* Gil Press, *A Very Short History of Big Data*, FORBES (May 9, 2013, 9:45 AM) https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data [http://perma.cc/H2GT-CMM7]; Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 397 (2014) (describing how wearable devices, mobile technology, and cloud computing contribute to the massive quantity of data that is increasingly available).

54. *See generally* Withers, *supra* note 25.

55. In 2006, when the specific provisions for ESI discovery were first added to the Federal Rules, preservation duties recognized that good faith deletion of ESI occurs just through routine operation of storage systems:

> Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part.

See FED. R. CIV. P. 37 advisory committee's note to 2006 amendment.

56. *See* Withers, *supra* note 25; Richards & King, *supra* note 53.

57. *See* sources cited *supra* note 56.

58. FED. R. CIV. P. 37.

faith destruction of ESI.[59] It states that, if ESI "is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery," courts may impose specific remedies.[60] First, if a party is prejudiced by the loss, the court "may order measures no greater than necessary to cure the prejudice."[61] But if the loss was intentional, additional options for remedies are available to the court, including a presumption that the lost ESI was unfavorable to the party that caused the loss, a jury instruction about a negative inference, or a default judgment or dismissal of the suit altogether.[62] By limiting the remedies for good-faith deletion of ESI, the Federal Rules recognize that digital content is unique in how it is stored and created. Routine deletion alone is not sufficient grounds for penalizing a party.

But even with broader safe harbors for spoliation, uncertainty still exists as to what must be preserved. Generally, a party may move content from an accessible format to an inaccessible one; courts impose no duty to maintain records in the format that is most convenient for a potential adversary in litigation.[63] Parties generally are not required to create a record where one otherwise does not exist, such as by creating reports or adding technology that allows all phone calls to be recorded.[64] Additionally, deletion that occurs through the good-faith operation of a system is not necessarily spoliation.[65] Similarly, no preservation duties may apply to transitory, ephemeral content that is automatically overwritten.[66]

But preservation duties may require a party to *suspend* automatic

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

60. *Id.*

61. *See* FED. R. CIV. P. 37(e)(1).

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

63. *See, e.g.*, Quinby v. WestLB AG, No. 04Civ.7406(WBP)(HBP), 2005 WL 3453908, at *8 n.10 (S.D.N.Y. Dec. 15, 2005) (showing that the court did not impose sanctions when the company moved emails from an accessible media to inaccessible backup tapes, though the court also did not shift costs of restoring data to requesting party).

64. *See* Malletier v. Dooney & Bourke, Inc., No-04-Civ. 5316(RMB)(MHD), 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006). The court held that no duty existed for the company to install systems to archive chatroom conversations, as such a requirement would be "akin to a demand that a party to a litigation install a system to monitor and record phone calls coming in to its office . . . ." *Id.*

65. *See* FED. R. CIV. P. 37 advisory committee's note to 2006 amendment.

66. *See, e.g.*, Convolve, Inc. v. Compaq Computer Systems, 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (holding that overwritten transitory data files, while discoverable, are not subject to preservation duty); Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 642 (E.D. Pa. 2007) (holding that there are no sanctions for automatic deletion of cached internet files); *Malletier*, 2006 WL 3851151, at *2 (holding that there is no duty to save chatroom conversations for which the company had no readily available technology for storing them).

deletion of ESI.[67] In other words, once litigation is anticipated or pending, parties may have a duty to change their retention habits to prevent ESI destruction. Additionally, preservation duties may extend to metadata.[68] In the social media context, courts have allowed adverse inferences in civil cases, such as when a plaintiff in a sexual harassment case "unfriended" the defendant and his wife on Facebook, even though editing Friends lists on Facebook is a commonplace occurrence.[69] Thus, while the scope of ESI preservation has been narrowed by the 2015 amendments to Rule 37, some uncertainty remains.[70] The proliferation of self-destruct apps amplifies this uncertainty.

V. TREATING EPHEMERAL APPS LIKE LIVE CONVERSATION

A tension is emerging between privacy policy and the civil discovery rules. On the one hand, technology industry actors and regulators emphasize the need to minimize data creation, collection, and retention.[71] Ideas like privacy by design mark a shift away from big data and towards privacy-maximizing technology tools.[72] This is a positive trend, and one that may reflect a market demand for greater privacy, or at least a push by government agencies for industry self-regulation. On the other hand, the civil discovery rules hinge on fair and open access to relevant information. The rules mandate not only broad discovery, but preservation of relevant content once litigation is anticipated or pending. How then do we reconcile the proliferation of ephemeral apps and the need for access to information in litigation?

The key may be to recognize that some digital tools mimic live interaction. They are meant to function like the truest form of ephemeral

67. *See* FED. R. CIV. P. 37 advisory committee's note to 2006 amendment ("Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation.").

68. In some cases, courts have penalized parties that allow relevant metadata to be destroyed. *See, e.g.*, Victor Stanley v. Creative Pipe, Inc., 269 F.R.D. 497, 524 (D. Md. 2010) (explaining that metadata and deleted data are subject to preservation); Brown Jordan Int'l, Inc. v. Carmicle, No. 0:14-CV-60629, 2016 WL 815827, at *37 (S.D. Fla. Mar. 2, 2016), *aff'd*, 846 F.3d 1167 (11th Cir. 2017) (allowing an adverse inference for destruction of metadata associated with screenshots).

69. *See* Painter v. Atwood, No. 2:12-CV-01215-JCM, 2014 WL 1089694, at *6 (D. Nev. Mar. 18, 2014), *reconsideration denied*, No. 2:12-CV-1215 JCM NJK, 2014 WL 3611636 (D. Nev. July 21, 2014); *see also* Gatto v. United Air Lines, Inc., No. 10-CV-1090-ES-SCM, 2013 WL 1285285, at *5 (D.N.J. Mar. 25, 2013).

70. FED. R. CIV. P. 37 advisory committee's note to 2015 amendment.

71. *See, e.g.*, FED. TRADE COMM'N, *supra* note 9.

72. *See, e.g.*, Hartzog & Stutzman, *supra* note 3.

communication: in-person, face-to-face conversation.[73] While it is true that some sort of digital content is created—digital crumbs, perhaps—the mere fact that a transitory file existed does not elevate these communication tools to ESI subject to preservation for discovery purposes.

Take Snapchat for example. An individual may use Snapchat regularly to send messages, images, and videos to others.[74] The default is that this content disappears automatically.[75] Even if litigation is anticipated or pending, a party to the litigation should still be able to use Snapchat in this normal way. This is akin to allowing parties to make phone calls without recording them or to have in-person conversations without otherwise creating a record of them. The mere fact that the party chose Snapchat, which auto-deletes content by design, should not amount to spoliation by design.

The same is true for businesses that choose ephemeral apps for some communications. Apps like Confide and Vaporstream, while geared towards more professional audiences, also enable private communications with similar auto-delete default features as Snapchat.[76] The concern, of course, is that businesses will use ephemeral apps to impede discovery of potentially damaging records. While companies should not be permitted to use ephemeral apps in bad faith to destroy or conceal relevant business records, communicating via ephemeral app alone is not improper.[77]

73. Ephemeral app companies describe their business models as trying to replicate the ephemeral nature of in-person communications. *See Privacy Policy*, *supra* note 1; *see also About Confide*, *supra* note 19.

74. *See Your Privacy Matters*, SNAPCHAT, https://www.snap.com/en-US/privacy/privacy-center/ [http://perma.cc/DQ57-E8M7] (last visited Jan. 30, 2018).

75. *See Privacy Policy*, *supra* note 1.

76. *See Vaporstream*, *supra* note 18; *About Confide*, *supra* note 19.

77. At the time of this writing, no court has defined the scope of preservation duties when a business intentionally uses ephemeral apps. However, an interesting issue relating to spoliation and ephemeral apps emerged in Waymo LLC v. Uber Techs., Inc., No. 3:17-cv-00939, 2017 U.S. Dist. LEXIS 213567 (N.D. Cal. Dec. 15, 2017). There, Waymo sued Uber for trade secret theft and other claims relating to self-driving car technology. In a pretrial hearing, it came to light that Uber employees instructed others within the company to use self-destructing, encrypted apps like Wickr. *See* Cade Metz, *Rebuking Uber Lawyers, Judge Delays Trade Secrets Trial*, N.Y. TIMES (Nov. 28, 2017), https://www.nytimes.com/2017/11/28/technology/uber-waymo-lawsuit.html [http://perma.cc/8977-WF9U]. In a pretrial ruling on the issue, 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." *See* Omnibus Order on Extent to Which Accusations Re Uber's Litigation Misconduct May Feature at Trial at p. 4-5, Waymo v. Uber Technologies, Inc., No. C 17-00939 WHA (Jan. 29, 2018). At the same time, the court cautioned against cumulative or prejudicial use of such evidence, noting that Waymo should avoid speculation and distraction. *Id*. The case settled during trial, and no further rulings address the ephemeral app spoliation issue. *See* Ross

Rather, ephemeral apps may be replacing unmonitored phone calls or in-person conversations in the business context, and thus should not be treated as regular ESI for preservation purposes.

The existence of other, sector-specific regulations that mandate retention of certain documents mitigates the fear of ephemeral apps impeding discovery of relevant business records. For example, files pertaining to occupational injuries and illness must be saved under the Occupational Safety and Health Standards;[78] record retention requirements exist under the Federal Deposit Insurance Corporation, which regulates the financial sector;[79] health information is regulated by the Health Care Portability and Accountability Act's security rule;[80] and mortgage and other records must be retained under applicable rules as well.[81] Some of these regulations even mandate retention of communications in instant messages.[82] Even without regulations, businesses will have an interest in keeping records of contracts, transactions, communications, and other information to protect their rights and interests. Thus, a duty to preserve all ephemeral app content is not necessary, as businesses have other rules and incentives for preserving business records.

Additionally, the mere fact that the substance of ephemeral communication may not be preserved does not foreclose discovery of other evidence of that communication. If an ephemeral app communication is relevant, metadata may establish the fact that the communication took place.[83] Parties with knowledge of the communication may testify as to its contents.[84] And the sender may have

---

Todd & Caroline Spiezlo, *Waymo, Uber Reach $244.8M Settlement on Driverless Car Trade Secrets*, THE RECORDER (Feb. 12, 2018, 1:45 PM), https://www.law.com/therecorder/sites/therecorder/2018/02/09/waymo-and-uber-settle-driverless-car-trade-secret-case/ [http://perma.cc/H2P3-NR4R].

78. *See* Recording and Reporting Occupational Injuries and Illness, 29 C.F.R. §§ 1904.0-1904.46 (2017).

79. *See* Federal Deposit Insurance Corporation Record Retention Requirements, 12 C.F.R. § 380 (2016).

80. *See* Health Care Portability and Accountability Act, 45 C.F.R. § 160 (2007).

81. *See* Home Mortgage Disclosure Act of 1975, 12 U.S.C. §§ 2801-2811 (1976).

82. *See* Financial Industry Regulatory Authority Manual, NASD Rule 3110, SCC Rule 17-A4(b)(4) (2015) (requiring members to keep records of instant messages for three years).

83. *See My Data*, *supra* note 46 (describing how a Snapchat account-holder can download some account information, including metadata showing that communications took place).

84. Civil cases have included other evidence about ephemeral app communications, even though the contents of messages themselves were destroyed. *See, e.g.*, Roof v. Newcastle Pub. Sch. Dist., No. 1-1 of McClain Cty., No. CIV-14-1123-HE, 2016 WL 502076, at *1 (W.D. Okla. Feb. 8, 2016) (referring to Snapchat message in Title IX and battery claims against a high school teacher and school district for inappropriate romantic contact with a student); Ramirez v. Missouri Dep't of Soc. Servs., Children's Div., 501 S.W.3d 473, 478 (Mo. Ct. App. 2016), *reh'g and/or transfer denied* (Aug.

saved an image[85] or the recipient could have defeated self-destruct defaults by taking a picture or screengrab of a message before it disappears.[86] Thus, a person's own record of the communication may be another source of the evidence. This is akin to a surreptitious recording of a conversation by one of the parties to it. Such a record would be discoverable if relevant,[87] but there is no duty to *create* the recording in the first place.

Additionally, if a record from an ephemeral app exists in a more permanent form, then preservation duties may attach. For example, once the recipient affirmatively circumvents the app's default features and saves a communication received via Snapchat, spoliation may occur if that person later deletes that saved record. Additionally, Snapchat gives users the option of saving an image they themselves created within the app's "Memories" feature, with the ability to sync those saved images to their mobile device's camera roll.[88] While the app allows for saving in this way, preservation rules should not mandate this additional, affirmative step. The "Memories" feature within the app is not automatic, and the technology may very well change to eliminate this function.[89] But if a user had saved something, a litigation hold would require preservation of that saved image.[90] However, other messages sent and received using default auto-delete settings in ephemeral apps should not be subject to preservation duties ordinarily.

To impose a duty to preserve ephemeral app contents across the board may have the effect of dissuading individuals and businesses from using these apps altogether. But ephemeral apps are a positive development that embrace the important industry goal of privacy by design. In light of these privacy trends, onerous preservation duties for ephemeral app content are unwarranted and undesirable.

30, 2016), *transfer denied* (Nov. 1, 2016) (explaining that a Snapchat conversation occurred, which formed part of an allegation that teacher had inappropriate communications with student).

85. An individual who creates a Snap may save it to their Memories, camera roll, or to cloud storage and, because Snapchat allows image timers to be set to "infinity," it may be easier for a recipient to save a copy of an image in the app as well. *See About Memories*, *supra* note 5.

86. *See Privacy Policy*, *supra* note 1.

87. *See* FED. R. CIV. P. 26.

88. *See Our Approach to Privacy*, *supra* note 4.

89. For example, the Snapchat "Memories" feature was added in July 2016, several years after the app first launched. *See About Memories*, *supra* note 5.

90. *See generally* Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (describing litigants' duty to preserve discoverable content through a "litigation hold").

VI. CONCLUSION

Ephemeral or self-destruct apps are gaining popularity in both individual and business contexts, and their auto-delete features serve an important, privacy-enhancing design feature. Embodying the concept of privacy by design, apps like Snapchat and Confide incorporate privacy into their very operation by retaining less user data as the default. But the concept of self-destructing content seems at odds with the broad scope of civil discovery and litigants' duties to preserve potentially relevant ESI.

In order to reconcile privacy-by-design innovations with the scope of preservation duties, courts should resist viewing self-destruct apps as spoliation by design. Instead, ephemeral apps may be akin to other ephemeral communication tools, like live conversation. Therefore, the use of ephemeral apps in general should not be viewed with suspicion. While content affirmatively saved from an ephemeral app should be subject to preservation, no duty should apply to preserve communications that are automatically deleted within the app. While evading discovery is a concern, other discoverable sources, like the parties to the communications themselves, can provide adequate information as to auto-deleted content. In the business context, some industry-specific regulations may require record-keeping, thereby minimizing the risk of abusing ephemeral apps as a tool for evading discovery.

As technology evolves, the concept of ESI preservation too must evolve. In the context of ephemeral apps, the trend towards data minimization should not be undermined by overly burdensome preservation duties.