Cleveland State Law Review

Volume 65 | Issue 1 Article

3-1-2017

Social Data Discovery and Proportional Privacy

Agnieszka McPeak
University of Toledo College of Law

SOCIAL DATA DISCOVERY AND PROPORTIONAL PRIVACY

AGNIESZKA MCPEAK*

ABSTRACT

Social media platforms aggregate large amounts of personal information as "social data" that can be easily downloaded as a complete archive. Litigants in civil cases increasingly seek out broad access to social data during the discovery process, often with few limits on the scope of such discovery. But unfettered access to social data implicates unique privacy concerns—concerns that should help define the proper scope of discovery.

The Federal Rules of Civil Procedure, as amended in 2015, already contain the tools for crafting meaningful limits on intrusive social data discovery. In particular, the proportionality test under Rule 26 weighs the burdens of discovery against its benefits, creating important boundaries on discovery's scope. Privacy burdens should be part of the proportionality analysis. By considering the privacy implications of social data discovery, courts can fashion fair and meaningful limits on the scope of social data discovery.

CONTENTS

I. INTRODUCTION

Social media accounts archive vast amounts of personal data and raise unique privacy concerns. One of these privacy concerns arises in the civil discovery process. More and more litigants seek social media content in civil litigation and often request complete and unfettered access to entire accounts. Courts struggle to define the scope of discovery and often fail to create meaningful limits, resulting in overly invasive social data discovery with little concern about individual privacy rights.

This essay addresses the privacy implications of overly broad access to big data in civil discovery, particularly "social data" aggregated in social media accounts. It argues that courts should set meaningful limits on overly broad social data discovery using the existing proportionality test under the Federal Rules of Civil Procedure or state law equivalents. Specifically, courts employing the proportionality test should

* Assistant Professor of Law, University of Toledo College of Law.

weigh the burden on privacy rights against the likely benefits of the proposed discovery. By including privacy burdens in the proportionality test, courts can prevent abusive access to highly personal, aggregated social data in civil litigation.

II. SOCIAL DATA AND PRIVACY

A. Defining Social Data

Virtually all aspects of an individual's online activities create a digital record of some kind. Often referred to as "Big Data," these digital records can be archived, processed, and turned into valuable information.[1] Big data is highly useful to governments and corporations—for example, by offering insights into our habits, preferences, and beliefs—but no comprehensive regulatory scheme has yet to address this data's collection and use. Privacy is one of the major concerns even for data that is stripped of personally identifiable information.[2]

One subset of big data is *social* data,[3] which includes personal information created and stored in an identifiable user's social media account. Social data poses unique and serious implications on individual privacy concerns.[4] Platforms like Facebook and Twitter aggregate large swaths of information that necessarily include detailed personal interactions over time.[5] For example, Facebook users post content like comments, photographs, videos, and article links.[6] The users catalog their activities and associations by checking in to locations using their phones' GPS data, maintaining a list of their Facebook Friends and Events, and adding personal details

[1] *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 394 (2014).

[2] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011) (noting that PII has not been clearly defined and that more nuanced categories of PII are needed); SEDONA CONFERENCE WORKING GRP. SERIES, SEDONA GUIDELINES: BEST PRACTICES ADDRESSING PROTECTIVE ORDERS, CONFIDENTIALITY & PUBLIC ACCESS IN CIVIL CASES 1 (Laurie Dore et al. eds., 2007); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000) (explaining the privacy risks and modes of protecting personally identified information); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1 (2013) (arguing that the concept of online obscurity should be used to help shape privacy laws).

[3] Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995, 1002 (2013) [hereinafter Hartzog, *Social Data*].

[4] *Id.* at 995. Hartzog refers to the contents of these large digital data compilations as "social data," which he defines as "the massive amounts of personal information shared via the user interface of social technologies." *Id.* at 997.

[5] *Id.* at 1002-03.

[6] *Facebook Help Center*, FACEBOOK, https://www.facebook.com/help/ (last visited Sept. 8, 2015) (explaining basic Facebook features).

about themselves to their profiles.[7] Users also exchange personal messages using Facebook's Messenger feature.[8]

User-controlled privacy settings are an important feature of most social media sites like Facebook. Users can choose to share things publicly or can limit their posts to their Friends.[9] Additionally, Facebook allows users to further limit visibility to "Friends except Acquaintances" or even smaller sub-sets of Friends.[10] For virtually all content in the account, Facebook creates and stores some digital record.[11] Not only does this record contain the content that users posted, but it also contains back-end data like logins, IP addresses from which the account was accessed, and targeted advertisement terms.[12]

Thus, the content of a Facebook account encompasses both user-created content and Facebook-created data as well. A user's activity across Facebook is compiled in the user's "Activity Log," and the account holder can easily download all account information as a zip file.[13] Notably, the download file does not differentiate content based on privacy settings or the user's intended audience.[14] Instead, all content—from content published publicly to private, one-on-one chat history—is lumped together in the downloaded account zip file.[15]

Other social media websites contain similar features. Twitter, for example, allows users to post 140-character comments, article links, photographs, and videos.[16] Users can keep their accounts private or viewable publicly, or users can

---

[7] *See Your Home Page*, FACEBOOK, https://www.facebook.com/help/753701661398957/?helpref=hc_fnav (last visited Sept. 8, 2016).

[8] *Sending a Message*, FACEBOOK, https://www.facebook.com/help/326534794098501 (last visited Sept. 8, 2015).

[9] *Profile & Timeline Privacy*, FACEBOOK, https://www.facebook.com/help/393920637330807/ (last visited July 19, 2016) (describing user privacy settings for Facebook Timeline).

[10] *See id.*

[11] *Accessing Your Facebook Data,* FACEBOOK, https://www.facebook.com/help/405183566203254 (last visited Sept. 8, 2015).

[12] *Id.* (explaining that Facebook users may find Facebook data in either the activity log or the downloaded data).

[13] *Id.*; *see also Download All Facebook Photos, Status, Wall Posts Together in Zip File*, FACEBOOK, http://www.facebook.com/note.php?note_id=10150118571353989 (last visited Sept. 8, 2016).

[14] *See* Jam Kotenko, *Want to Know What Data Facebook Has On You? A Primer on What You Get and How to Get It*, DIGITALTRENDS, (Sept. 22, 2013), http://www.digitaltrends.com/social-media/want-to-know-what-data-facebook-has-on-you-a-primer-on-what-you-get-and-how-to-get-it/ (noting that only current privacy settings are saved but not past settings).

[15] *See id.*

[16] *See Getting Started on Twitter*, TWITTER, https://support.twitter.com/articles/215585 (last visited July 19, 2016).

engage in one-on-one chats.[17] Twitter also compiles a user's Twitter data and allows users to download a file of their entire Twitter archive.[18]

Newer social media companies purport to track and store less user information than Facebook. Snapchat, for example, is known for its disappearing messages.[19] The media platform allows users to share photographs, videos, and comments with a single person or group of people.[20] The messages automatically disappear after a few seconds.[21] Users can also share "Stories" publicly or to their Snapchat Friends.[22] Stories generally appear for 24 hours before they disappear.[23] Even though Snapchat is most famous for its ephemeral content, it recently added a Memories feature that allows users to save content they created.[24] As such, even a Snapchat account may contain stored pictures and videos under "Memories."[25] Additionally, Snapchat has faced FTC charges over its storing of account content despite claims that messages completely disappear.[26] Like other social media companies, Snapchat also allows its users to download their account contents.[27]

---

[17] *See Protecting and Unprotecting Your Tweets*, TWITTER, https://support.twitter.com/articles/20169886 (last visited July 20, 2016); *Twitter About*, TWITTER, https://about.twitter.com/directmessages (last visited July 20, 2016).

[18] *See Downloading Your Twitter Archive*, TWITTER, https://support.twitter.com/articles/20170160 (last visited July 19, 2016) (explaining private messaging feature in Twitter).

[19] *See About Snaps*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-US/a/getting-started1 (last visited July 20, 2016); *see also* Larry Magid*, What is Snapchat and Why Do Kids Love it and Parents Fear It*, FORBES TECH (May 1, 2013), http://www.forbes.com/sites/larrymagid/2013/05/01/what-is-snapchat-and-why-do-kids-love-it-and-parents-fear-it/#6e557ff82551 (explaining how Snapchat's disappearing messages work and why the app is not foolproof).

[20] *See Send and Receive Snaps*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-US/ca/sending-and-receiving-snaps (last visited July 20, 2016).

[21] *About Snaps*, *supra* note 19 (noting that a sender can select to make a Snap viewable for up to 10 seconds, viewers can replay a Snap once, and viewers may not save Snaps unless they take a screen capture or picture of it with a separate camera).

[22] *See About Stories*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-US/about/stories (last visited July 20, 2016).

[23] *See Create a Story*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-US/article/post-story (last visited Sept. 8, 2016).

[24] *See About Memories*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-GB/about/memories (last visited July 20, 2016) ("Memories is a personal collection of the Snaps and Stories you save, backed up by Snapchat.").

[25] *Id.*

[26] *See, e.g.*, *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False, Press Release*, FED. TRADE COMM'N (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[27] *Accessing Your Snapchat Data*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-US/a/download-my-data (last visited Sept. 24, 2016). Snapchat compiles some data in the app, including username, email address, phone number, birthday, name, profile picture, privacy

By its very nature, social data touches upon the most intimate details of life in an aggregated data set that may include daily content spanning years. Users choose what information to share and with whom, create an online persona and social circle, and give away a wide range of personal information.[28] Users express a curated online identity to a select audience for the purposes of creating and maintaining social contacts.[29] As social data becomes a larger part of our online footprint, the risks of overly broad access to this personal information needs to be addressed. In particular, as our social interactions are aggregated over time, even mundane details amount to an intimate portrait of one's personal life.[30] Access to this information by unintended audiences presents a unique privacy harm that the law has yet to adequately address.[31]

B. Evolving Notions of Privacy

Big data—and social data in particular— are forcing us to reconsider existing privacy law principles. But the U.S. Constitution has yet to clearly define a right to information privacy, statutes fall short in providing meaningful protection of social data, and Fourth Amendment law generally is slow to adapt to new technology. In *Whalen v. Roe*,[32] the Supreme Court acknowledged that the disclosure of personal information may implicate a constitutional privacy interest under the Fifth Amendment's due process clause, but the court did not expressly recognize such a right.[33] That case ultimately upheld a New York state law that required the state to collect information about patients who are prescribed certain drugs.[34] Similarly, in *NASA v. Nelson*,[35] the Court again stated that a constitutional right to information privacy may exist, but ultimately held that a government employment questionnaire requesting personal information was constitutional.[36] These cases indicate that the Constitution may protect a right to information privacy, even though courts to date have not expressly enforced one.

---

settings, friends, and blocked friends. The information available for download includes account history and information, snap count, local, live, and crowd-sourced content history and information, purchase history, and support history. *Id.*

[28] *See* Hartzog, *Social Data*, *supra* note 3, at 997-99 (maintaining that guiding principles and policies are needed to protect the massive amount of information aggregated in social media accounts).

[29] *See id.* at 1003.

[30] *See id.*

[31] *See id.* Hartzog proposes a set of principles that should govern access to and the use of social data, including respecting an individuals expressed boundaries, identity, and chosen network. *Id.* at 998.

[32] 429 U.S. 589, 591 (1977).

[33] *Id.* at 605.

[34] *Id.* at 603-04; *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977).

[35] 562 U.S. 134 (2011).

[36] *Id.* at 159.

Instead, statutes are the primary source of protection for information privacy. Specific federal legislation shields narrow categories of personal information in some instances. Examples include consumer financial information,[37] information pertaining to minors,[38] educational records,[39] and personal medical records.[40] These statutes reflect that American society values privacy-based limits on the access and use of certain personal information. However, no federal privacy statutes protect social data in the civil discovery context.

Some evolution is occurring as to the privacy protections rooted in the Fourth Amendment.[41] But, the Fourth Amendment is also limited by doctrines such as the reasonable expectation of privacy requirement and the third-party disclosure rule—doctrines that, as they currently stand, substantially limit the scope of privacy protections available for social data in particular.[42] For example, under the reasonable expectation of privacy requirement, no Fourth Amendment protection exists when a person's expectation of privacy is not objectively reasonable.[43] Further, under the third-party disclosure rule, once information is disclosed to a third party, any reasonable expectation of privacy vanishes.[44] These doctrines become especially relevant when looking at new technologies. Most of what we do online or on our phones requires third-party disclosure, be it to an Internet service provider, third-party website, or electronic recipient. For social data, the very nature of the personal information created is *social*, meant to share with others in some way.

Nonetheless, in some Fourth Amendment cases, courts are beginning to adapt traditional doctrines to deal with new technology. For example, in *Riley v. California*,[45] the Supreme Court held that a warrant is required to search and seize an individual's cell phone even when that phone is seized incident to a lawful arrest.[46] The Court explained the unique nature of data stored on a cell phone: "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[47] The Court described the vast and thorough array of information stored on a phone, noting that the sheer volume of data far exceeds what anyone could carry with them in physical form.[48] In doing so,

---

[37] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-09 (2012).

[38] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (2012).

[39] *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1221 (2012).

[40] Health Insurance Portability and Accountability Act, 42 U.S.C. § 301 (2012).

[41] U.S. CONST. amend. IV.

[42] Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 263 (2015) [hereinafter McPeak, *Social Media*].

[43] *See* Katz v. United States, 389 U.S. 347, 360 (1957) (Harlan, J., concurring).

[44] *See* Smith v. Maryland, 442 U.S. 735, 745 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[45] 134 S. Ct. 2473 (2014).

[46] *Id.* at 2493.

[47] *Id.* at 2488-89.

[48] *Id.* at 2489-90.

the Court acknowledged that digital records on a smartphone are not merely analogous to a wallet or physical record.[49] Rather, the Court seemed to recognize that new privacy concerns are implicated by the vast amounts of personal information that can be stored and archived by modern technology.[50]

The *Riley* case supports the idea that bits and pieces of personal information, when collected and viewed as a whole, implicate privacy concerns.[51] This idea may draw on the mosaic theory of privacy, a concept that can be used to expand privacy protection in the digital age. In its most basic sense, the mosaic theory states that aggregated, non-private information, when viewed together, paints an intimate portrait of one's personal life.[52] Thus, even though each individual piece of information does not fit neatly into a category of privacy protection, the aggregate of that non-private information creates its own privacy concern.[53]

The mosaic theory has not been recognized expressly as a basis for privacy protection, but the Supreme Court has articulated similar concerns in recent cases. For example, in the *Riley* case, the Court noted that the content stored on a cell phone "reveal[s] much more in combination than any isolated record."[54] Further, in *United States v. Jones*,[55] the Court considered Fourth Amendment protections for warrantless collection of aggregated GPS data.[56] There, law enforcement generated over 2,000 pages of data on a suspect using a surreptitiously placed GPS device on a car.[57] The majority opinion held that an unconstitutional search occurred because of how the device was placed on the car, thereby avoiding the issue of whether the search method was proper.[58] However, Justice Sotomayor, in her concurrence, alluded to a mosaic theory-based privacy right.[59] In particular, Justice Sotomayor acknowledged that the data compiled by GPS technology "reflects a wealth of detail about . . . familial, political, professional, religious, and sexual associations."[60] Further, privacy concerns may be implicated due to the "quantum of intimate information about any person" that may be available in a large digital archive.[61]

---

[49] *Id.*

[50] *Id.*

[51] *Id.* at 2489.

[52] *See* United States Dep't of Justice v. Reporters Comm. Freedom of Press, 489 U.S. 749 (1989); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012).

[53] *See id.*

[54] *Riley*, 134 S. Ct. at 2479.

[55] United States v. Jones, 132 S. Ct. 945 (2012).

[56] *Id.*

[57] *Id.* at 948.

[58] *Id.*

[59] *See id.* at 954-55 (Sotomayor, J., concurring).

[60] *Id.* at 955 (Sotomayor, J., concurring).

[61] *See id.* (Sotomayor, J., concurring).

Significantly, Justice Sotomayor also noted that the third-party disclosure rule may no longer be a viable principle in light of the nature of new technology.[62]

Thus, privacy law may be evolving to take into account the privacy implications of big data and the unprecedented ability to digitally track and store personal information. Nonetheless, few privacy protections exist as to social data in the civil discovery context.

III. CIVIL DISCOVERY GENERALLY

The civil discovery process depends upon a balance between open access to information and safeguards against over-reaching. Although courts favor broad discovery, they simultaneously protect against fishing expeditions.[63] Although privacy-based concerns are not express limits on civil discovery, the value of achieving justice through complete and thorough access to information is counter-balanced by equally important limiting principles, such as relevance, burden, expense, embarrassment, and privilege.[64] In addition, proportionality is another important limit.[65]

A. Existing Privacy-Based Limits on Civil Discovery

Under the Federal Rules of Civil Procedure, privacy is not an enumerated limit on the broad scope of discovery.[66] Nonetheless, discovery is not limitless, and courts already reject some efforts to pry into all facets of one's personal life. Essentially, existing limits on discovery recognize some need to respect the privacy of litigants and witnesses to an extent.

Although privacy law itself is not a factor when deciding the scope of discovery under the Federal Rules, privacy concepts infiltrate the analysis, particularly as they relate to new technology and digital content.[67] Information that is subject to some sort of statutory or other privacy protection may very well be handled differently in civil discovery. For example, trade secrets are protected as private under the law and, as such, may be limited in their discovery or subject to a protective order.[68]

---

[62] *Id.* at 957 (Sotomayor, J., concurring).

[63] *See generally* Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007).

[64] *See* FED. R. CIV. P. 26-37.

[65] *See* FED R. CIV. P. 26.

[66] McPeak, *Social Media*, *supra* note 42, at 260.

[67] *Id.* at 235; *see, e.g.*, Allyson Haynes Stuart, *Finding Privacy in a Sea of Social Media and Other E-Discovery*, 12 NW. J. TECH. & INTELL. PROP. 149 (2014).

[68] *See* FED. R. CIV. P. 26(c) Advisory Committee's notes (1970). Protective orders are seen as an important tool for protecting privacy, even though they hinder public access to the courts. *See* Joseph F. Anderson, Jr., *Secrecy in the Courts: At the Tipping Point?*, 53 VILL. L. REV. 811 (2008) (chronicling both sides of the debate over confidentiality versus open access); Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 466 (1991) ("[I]t is consistent with the underlying goals of the Rules that the litigation system's sensitivity to privacy considerations be heightened, given today's unparalleled capacity to record, retrieve, and transfer data, as well as the range of decisions made about people on the basis of files, records, dossiers, and data banks."); Richard L.

Similarly, information relating to a minor may be redacted or otherwise protected.[69] Physical and mental exams are limited by a good cause requirement.[70] Protective orders and in-camera review may be used to minimize the spread and use of private information, without shielding it from discovery altogether.[71]

Furthermore, privacy-based limits are expressly considered in civil discovery under California law.[72] The California constitution contains a right to privacy, which has been applied in civil cases.[73] In particular, California courts recognize that privacy rights may trump the right to discovery in some instances.[74] Three elements must be met. First, the person trying to block discovery must have a legally protected privacy right, such as autonomy privacy or information privacy.[75] Second, there must be a reasonable expectation of privacy "under the specific circumstances."[76] Third, the privacy invasion must be serious enough "to constitute an egregious breach of the social norms underlying the privacy right."[77] Once all three are met, the privacy interest must still be balanced against "legitimate and important competing interests" such as the need for the information.[78] The court will also consider whether privacy concerns can be adequately addressed by limiting access to the private information, like through a protective order.[79] Notably, some of the information that may pose a serious privacy invasion may include revealing "personal or business secrets, intimate activities, or similar private information" or that risks "undue intrusion into one's personal life."[80] However, the bar for a

Marcus, *Myth and Reality in Protective Order Litigation*, 69 CORNELL L. REV. 1 (1983) (explaining some of the existing ways privacy trumps open access in civil discovery).

[69] *See* Hon. Margaret Dee McGarity, *Privacy and Litigation: Two Mutually Exclusive Concepts*, 23 J. AM. ACAD. MATRIM. LAW. 99, 103 (2010) (discussing ways to safeguard personal identifiers in litigation, including mandatory redaction and penalties for disclosure); SEDONA CONFERENCE WORKING GRP. SERIES, *supra* note 2, at 2.

[70] FED. R. CIV. P. 35(a)(2)(A).

[71] *See* FED. R. CIV. P. 26(c); 4 C.F.R. § 22.25 (2016).

[72] Denari v. Superior Court, 264 Cal. Rptr. 261, 267 (Ct. App. 1989).

[73] CAL. CONST. art. 1, § 1.

[74] *See* Alch. v. Superior Court, 82 Cal. Rptr. 3d 470, 479 (2008).

[75] *Id.* at 479. The court defines autonomy privacy as "the interest in making intimate personal decisions or conducting personal activities without observation, intrusion or interference" and information privacy as the interest "'precluding the dissemination or misuse of sensitive and confidential information.'" *Id.* (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 641 (Cal. 1994)).

[76] *Id.*

[77] *Id.* at 479-80 (quoting *Hill*, 865 P.2d at 641).

[78] *Id.* at 480 (quoting Pioneer Elecs., Inc. v. Superior Court, 150 P.3d 198 (Cal. 2007)).

[79] *See id.*

[80] *Id.* (quoting *Pioneer*, 150 P.3d at 198).

California constitutional invasion of privacy claim is set quite high, and it is used infrequently to limit civil discovery.[81]

Although privacy is not an express limit on discovery under the Federal Rules of Civil Procedure, many of the existing limits, at their core, draw on privacy-related values. In essence, courts already recognize that overly intrusive discovery violates individual rights and should not be permitted without justification.[82]

B. Proportionality

Proportionality is a limit on the scope of discovery that is gaining new importance after the most recent amendments to the Federal Rules of Civil Procedure. The concept of proportionality has been a part of the Federal Rules of Civil Procedure for decades and is mentioned in relation to several rules, from the scope of discovery to preservation duties.[83] Most recently, under the 2015 amendments, Rule 26(b)(1) allows discovery of "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case."[84] In particular, the proportionality analysis looks at the following factors:

> 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.[85]

The purpose of the proportionality test is to limit discovery's overuse with principles based on fairness and balance. From the beginning, proportionality was meant to serve as a limit on civil discovery's scope.[86]

In weighing the benefits of discovery against its burden, courts often focus only on *financial* burden. For example, in *Mancia v. Mayflower Textile Services*,[87] a Maryland district court noted that the requested discovery might be excessive

---

[81] Belluomini v. Citigroup, Inc., No. CV 13-017743, 2013 U.S. Dist. LEXIS 103882, 2013 WL 3855589, at *5 (N.D. Cal. July 24, 2013).

[82] *See* Bakhit v. Safety Marking, Inc., No. 3:13CV1049, 2014 WL 2916490, 2014 U.S. Dist. LEXIS 86761 (D. Conn. June 26, 2014).

[83] FED. R. CIV. P. 26 Advisory Committee's notes (1983 Amendments). The proportionality factors were added to the Federal Rules in 1983 as a way to limit overuse of the discovery process. *Id.* In 1993, two additional proportionality factors were added. FED. R. CIV. P. 26 Advisory Committee's notes (2015 Amendments). The 2000 amendments added certain cross-references to the proportionality factors, again emphasizing the need for judges to use proportionality as a limit to civil discovery. *See* FED. R. CIV. P. 26 Advisory Committee's notes (2000 Amendments); Hon. Elizabeth D. Laporte & Jonathan M. Redgrave, *A Practical Guide to Achieving Proportionality Under New Federal Rule of Civil Procedure 26*, 9 FED. CTS. L. REV. 19 (2015) (detailing the evolution of proportionality in the Federal Rules).

[84] FED. R. CIV. P. 26(b)(1).

[85] *Id.*

[86] *See id.*

[87] 253 F.R.D. 354, 364 (D. Md. 2008).

compared to the value of the plaintiffs' claims.[88] Similarly, in *In re Convergent Technologies Securities Litigation*,[89] the court recognized that proportionality is an important, common sense limit on even relevant discovery in stating,

> After satisfying this threshold requirement counsel *also must* make a common sense determination, taking into account all the circumstances, that the information sought is of sufficient potential significance to justify the burden the discovery probe would impose, that the discovery tool selected is the most efficacious of the means that might be used to acquire the desired information (taking into account cost effectiveness and the nature of the information being sought), and that the timing of the probe is sensible . . .[90]

The court in *Convergent Technologies* ultimately focused on the cost effectiveness of the discovery and largely denied the defendant's motion to compel.[91]

Nonetheless, the proportionality factors contemplate non-pecuniary burdens without quantifiable financial impact. In *Hunter v. Ohio Indemnification Co.*,[92] a California district court denied a deposition noting the burden on the witness, who had little or no knowledge about the issues and was caring for a spouse with a life-threatening illness.[93] Commentators have also urged courts to consider non-pecuniary burdens in the proportionality analysis.[94] Yet, courts are only just beginning to use the proportionality factors as a meaningful limit to discovery, and non-pecuniary considerations are rarely a part of the analysis so far.[95]

IV. SOCIAL DATA IN CIVIL LITIGATION

Litigants increasingly seek out social media content in civil litigation and, to date, courts struggle with applying the civil procedure rules to this new category of electronic discovery. Little consideration is given to the volume of information

---

[88] *Id.*

[89] 108 F.R.D. 328, 331-32 (N.D. Cal. 1985).

[90] *Id.* at 331.

[91] *Id.* at 349.

[92] No. C 06-3524, 2007 WL 2769805, at *1 (N.D. Cal. Sept. 21, 2007).

[93] *Id.*

[94] *See* Theodore C. Hirt, *The Quest for "Proportionality" in Electronic Discovery-Moving from Theory to Reality in Civil Litigation*, 5 FED. CTS. L. REV. 171, 199 (2011) (noting that proportionality should also be a limit in non-monetary or low-value cases); The Sedona Conference, *The Sedona Conference Commentary on Proportionality in Electronic Discovery*, 11 SEDONA CONF. J. 289, 300 (Conor R. Crowley et al. eds., 2010) (stating that, according to Principle 5, "[n]onmonetary factors should be considered when evaluating the burdens and benefits of discovery"); John L. Carroll, *Proportionality in Discovery: A Cautionary Tale*, 32 CAMPBELL L. REV. 455, 464 (2010) (cautioning against over-emphasis of monetary factors in the proportionality analysis); Gordon W. Netzorg & Tobin D. Kern, *Proportional Discovery: Making It the Norm, Rather Than the Exception*, 87 DENV. U. L. REV. 513, 529 (2010) (noting that proportionality should limit the scope of discovery, including non-monetary factors).

[95] Netzorg, *supra* note 94.

aggregated in social media accounts, and privacy concerns rarely serve as a meaningful limit to broad civil discovery.

In the social media context, account information is sought in all forms of civil litigation, including cases based on personal injury, family law, employment, and other claims.[96] Discovery often occurs between the parties because social media providers maintain that the Stored Communication Act prevents them from disclosing user content in response to a civil subpoena without the user's consent.[97] Even with consent, social media providers refer litigants to the download account feature, thereby cutting themselves out of the discovery process entirely.[98] Instead, discovery is handled through formal requests to account holders, and courts generally allow broad discovery.

Courts often set a low threshold for allowing discovery of social media accounts. In some cases, courts even have forced litigants to hand over their passwords so that the opposing party's counsel can log in to see all account content.[99] This approach offers broad and unfettered access to the entire account, including third-party content like privacy-setting protected posts made by the account-holder's Friends on their own Timelines.[100] It also means that opposing counsel must enter a live system with real-time content and complete access to the account-holder's administrative functions. It is fraught with opportunities for abuse, error, and privacy invasion.

In other cases, courts have required the party seeking discovery to establish a factual predicate for the discovery, often based on the publicly available content in the social media account.[101] Under this "factual predicate" approach, attempts to

---

[96] For a discussion of cases using social media evidence and the different approaches to social media discovery, see McPeak, *Social Media*, *supra* note 42, at 237-39; 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, 910-13 (2013) [hereinafter McPeak, *Facebook Digital Footprint*].

[97] Stored Wire and Elec. Commc'ns and Transactional Records Access (Stored Communication Act), 18 U.S.C. § 2701 (2012); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010); *see also* Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 117 (E.D.N.Y. 2013) (explaining that plaintiff's counsel should review Facebook content to determine what may be relevant and responsive).

[98] *See, e.g.*, *Information on Civil Subpoenas*, FACEBOOK, https://www.facebook.com/help/473784375984502 (last visited July 24, 2016) (directing users to download their own accounts); *see generally Guidelines for Law Enforcement*, TWITTER, https://support.twitter.com/articles/41949 (last visited July 24, 2016); *Accessing Your Snapchat Data*, SNAPCHAT SUPPORT, https://support.snapchat.com/en-US/a/download-my-data (last visited July 24, 2016); *Law Enforcement Guide*, SNAPCHAT SUPPORT, https://www.snapchat.com/static_files/lawenforcement.pdf?version=20150604 (last visited July 24, 2016).

[99] *See, e.g.*, Gallion v. Gallion, No. FA114116955S, 2011 Conn. Super. LEXIS 2517, 2011 WL 4953451 (Conn. Super. Ct. Sept. 30, 2011); McMillen v. Hummingbird Speedway, Inc., No. 113–2010 CD, 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010).

[100] *See, e.g.*, Appler v. Mead Johnson & Co., No. 3:14-CV-166-RLY-WGH, 2015 U.S. Dist. LEXIS 128182, 2015 WL 5615038, at *4 (S.D. Ind. Sept. 24, 2015).

[101] *See, e.g.*, Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 652-55 (N.Y. Sup. Ct. 2010) (using plaintiff's public Facebook profile photo to establish factual predicate for discovery of private portions of the account).

discover social media content can hinge on how savvy the account-holder was with privacy settings.[102] This results in outcomes that are inconsistent and, at times, unfair. Some courts allow virtually complete access to all social data based on a public profile picture, whereas others bar all social data discovery because public social media content is not contradictory enough of the party's claim in the litigation.[103]

Other courts recognize that relevance is the key inquiry and do not require a factual predicate based on public account content. These cases instead require that discovery requests state with reasonable particularity the private content sought.[104] While a better approach, defining relevance and creating meaningful boundaries to social data discovery remain a challenge.

For example, in *EEOC v. Simply Storage*,[105] the court stated that discovery of social media content is not automatic and instead is limited to what is relevant to claims and defenses, noting that the proportionality factors also should be considered.[106] The case involved employment discrimination claims in which the plaintiffs alleged severe and debilitating emotional distress among other damages.[107] Ultimately, the court allowed broad discovery of private Facebook content, including all contents within a specific date range that "reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state."[108] Notably, the court expressly stated that the severe and debilitating emotional distress claims warranted such broad discovery, but garden-variety damages may not justify as expansive access to private social media content.[109] Nonetheless, several cases citing to *Simply Storage* still allow broad discovery without identifying any claims of severe emotional distress.[110]

---

[102] *See* Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 115 n.1 (E.D.N.Y. 2013) (explaining how requiring factual predicate to be established by public content is both too broad and too narrow an approach). *See generally* McPeak, *Facebook Digital Footprint*, *supra* note 96.

[103] *Compare Romano*, 907 N.Y.S.2d at 653-55 (noting that public Facebook vacation photographs contradicted plaintiff's claim of loss of enjoyment of life and supported discovery of private content), *with* Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 388-89 (E.D. Mich. 2012) (noting that public Facebook photograph of plaintiff at a birthday party holding a small dog did not support discovery of private content because the activity depicted in the photograph did not contradict injuries and damages sought); *see also* Forman v. Henkin, 22 N.Y.S.3d 178, 182 (N.Y. App. Div. 2015) (requiring some sort of factual predicate as threshold for discovery of private social media content and rejecting the argument that allegations of physical injury in a tort claim justifies two years' worth of Facebook posts that may depict activity).

[104] *See, e.g.*, EEOC v. Simply Storage Mgmt., Inc., 270 F.R.D. 430, 434-36 (S.D. Ind. 2010).

[105] *Id.* at 434-35.

[106] *Id.* at 433 (quoting FED. R. CIV. P. 26(b)(2)(C)(iii)).

[107] *Id.* at 432-33.

[108] *Id.* at 436.

[109] *See id.* at 435-36; *see also* Mailhot v. Home Depot U.S.A., 285 F.R.D. 566, 572-73 (C.D. Cal. 2012) (holding that severe emotional distress claims supported broad discovery in

Under all approaches, courts mostly reject privacy-based arguments against social media discovery. Because civil litigation occurs among private litigants, constitutional principles like Fourth Amendment privacy protections do not apply directly.[111] But some of the concepts contained in constitutional law jurisprudence are referred to in civil discovery disputes. Courts note that users voluntarily create and use social media and the purpose of social media is to share information with others.[112] Thus, there is no reasonable expectation of privacy.[113] Further, social media necessarily requires disclosure to third parties, including the Internet service provider, social media provider, and Friends or other recipients of the content.[114] Thus, courts also note that any privacy protections are destroyed under the third-party disclosure rule.[115]

Despite the majority of cases permitting broad discovery over privacy concerns, a few cases have noted that some privacy interests may be implicated when litigants seek overly broad access to private portions of social media accounts. In *Appler v.*

---

limited date range). *But see* Ye v. Cliff Veissman, Inc., No. 14-CV-01531, 2016 WL 950948, at *3 (N.D. Ill. Mar. 7, 2016) ("The Court realizes that Defendants are seeking content relating to damage issues that are at times hard to ascertain, such as the grief, sorrow, and mental suffering of the decedent's next of kin following her death. But the fact that the decedent and her next of kin's mental and emotional state of minds may be relevant to Plaintiff's claim does not save Defendants' request from being overbroad."); Root v. Balfour Beatty Constr. LLC, 132 So. 3d 867, 870 (Fla. Dist. Ct. App. 2014) (quashing discovery of Facebook posts relating to mother's "relationships with her entire family and significant others, her mental health history, her substance use history, and her litigation history" as overly broad in a parental consortium claim).

[110] *See, e.g.*, Reid v. Ingerman Smith LLP, No. CV 2012-0307 (ILG) (MDG), 2012 U.S. Dist. LEXIS 182439, 2012 WL 6720752, at *2-3 (E.D.N.Y. Dec. 27, 2012) (permitting discovery as expansive as *Simply Storage* without allegations of severe emotional distress). *But see* Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 115-16 (E.D.N.Y. 2013) (denying discovery of all posts that deal with emotional state in garden-variety damages); Winchell v. Lopiccolo, 954 N.Y.S.2d 421, 425 (N.Y. Sup. Ct. 2012) (holding that plaintiff's claim of cognitive difficulty was not enough to justify unrestricted discovery of entire Facebook account).

[111] *See, e.g.*, Doe v. Senechal, 725 N.E.2d 225, 231 (Mass. 2000) (noting that the Fourth Amendment does not apply to civil litigation among private parties).

[112] *See, e.g.*, McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, 2010 WL 4403285, at *4 (Pa. Ct. Com. Pl. Sept. 9, 2010) (rejecting any reasonable expectation of privacy in social media because sites make clear that content is not confidential and disclosure is possible despite users' preferred privacy settings).

[113] *Id.*; *see also* Nucci v. Target Corp., 162 So. 3d 146, 154 (Fla. Dist. Ct. App. 2015) (noting that social media privacy settings do not create a reasonable expectation of privacy).

[114] *See* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010) (noting that there can be no reasonable expectation of privacy to materials posted to a social media account).

[115] *See, e.g.*, Davenport v. State Farm Mut. Auto. Ins. Co., No. 3:11-CV-632-J-JBT, 2012 U.S. Dist. LEXIS 20944, 2012 WL 555759, at *1 (M.D. Fla. Feb. 21, 2012) (rejecting right to privacy for social media content but still looking to relevance-based limits on broad discovery).

Mead Johnson & Co., LLC,[116] the defendant in an employment case sought the complete Facebook download file for plaintiff's account.[117] The court recognized that privacy interests may be implicated by the broad discovery request and balanced the relevancy of the discovery against the privacy burden.[118] Ultimately, the court allowed broad discovery of plaintiff's Facebook page but excluded certain categories on privacy grounds.[119]

Because most courts ignore privacy burdens, the ultimate result is that courts often allow broad discovery of all social media content. This access to social media content can include several years' worth of daily updates on one's whereabouts, associations, thoughts, feelings, activities, and preferences. Large portions of the account content may be wholly irrelevant to the claims and defenses and, when viewed as a whole, paint an intimate picture of the person. The account information is also personally identifiable, as rarely can the litigant's PII be excluded from discovery.[120] By not appreciating the unique nature of social data, courts often allow overly intrusive discovery that fails to consider individual privacy burdens.

V. ACHIEVING PROPORTIONAL PRIVACY IN CIVIL DISCOVERY

The civil discovery rules now must grapple with the availability of large digital archives of social data in civil litigation. Fortunately, the Federal Rules of Civil Procedure, as amended in December 2015, contain sufficient safeguards against overly broad social data discovery, *provided that* principles of privacy and proportionality serve as meaningful guides. Courts should recognize that privacy rights could be violated by overly broad discovery of social data. Further, the rules' emphasis on proportionality should encompass non-pecuniary burdens posed by broad discovery,[121] including the burdens on individual privacy rights.

VI. CONCLUSION

By recognizing the privacy implications of overly broad social data discovery, courts can draw meaningful boundaries to curtail discovery abuses. While privacy

---

[116] No. 3:14-CV-166-RLY-WGH, 2015 U.S. Dist. LEXIS 128182, 2015 WL 5615038, at *4 (S.D. Ind. Sept. 24, 2015).

[117] *Id.*

[118] *Id.* at 4, 6.; *see also* Smith v. Hillshire Brands, No. 13-2605-CM, 2014 U.S. Dist. LEXIS 83953, 2014 WL 2804188, at *5 (D. Kan. June 20, 2014) (refusing to recognize privacy rights in social media content, but nonetheless blocking overly broad discovery because it encompassed irrelevant, highly personal information like "private sexual conduct").

[119] Appler v. Mead Johnson & Co., No. 3:14-CV-166-RLY-WGH, 2015 U.S. Dist. LEXIS 128182, 2015 WL 5615038, at *15 (S.D. Ind. Sept. 24, 2015) ("Plaintiff does not need to include the following in the download produced: Credit Cards, Facial Recognition Data, IP Addresses, Phone Numbers, Family, and Religious Views. The last two of these categories may, in some cases, be publically viewable, but I find there is a protected privacy interest in this type of information and it has no relevancy here. Therefore, it does not need to be produced.").

[120] Cohen, *supra* note 2.

[121] *See, e.g.*, The Sedona Conference, *supra* note 94 (suggesting non-pecuniary factors should be part of the proportionality analysis).

law in general is slow to evolve to the realities of new technology, the proportionality test under the Federal Rules of Civil Procedure is already well suited for incorporating privacy burdens into its analysis. By considering proportional privacy, courts effectively can disaggregate digital data compilations to prevent overly intrusive discovery and otherwise shield litigants from unnecessary whole-cloth disclosure of the highly personal information compiled in their social data.