Social Media, Smartphones, and Proportional Privacy in Civil Discovery

*Agnieszka A. McPeak**

I. INTRODUCTION

At its core, the discovery process in civil litigation relies on a balance between open access to information and protections against over-reaching. Although broad discovery is favored, courts simultaneously warn that the civil discovery process is not meant to be a fishing expedition.[1] Thus, the value of achieving justice through complete and thorough access to information is counter-balanced by equally important limiting principles. These limiting principles include restrictions based on relevance, burden, expense, embarrassment, privilege, and proportionality.[2] Essentially, these limiting principles draw on an important societal value: privacy.

Privacy is a core concept that underlies the civil discovery rules, and it is one that courts must return to when resolving discovery disputes over digital data compilations. These compilations, particularly when viewed in the aggregate, present a detailed mosaic of one's personal life. The result is a highly revealing portrait of personal details that implicate individual privacy rights. In some cases, discovery of the private portions of social media accounts or the contents of a personal smartphone should be limited based on privacy concerns.

These privacy concerns can best be addressed as part of the

* Assistant Professor, University of Toledo College of Law. Thank you to the University of Toledo College of Law for the research support, guidance, and encouragement; to the faculty for their comments at the Toledo Law Spring Workshop Series; and to Bill Richman and Bryan Lammon for their input. Special thanks to Brian Owsley for his invaluable feedback and edits. Additionally, thank you to James Durham and participants at the University of Dayton School of Law Faculty Colloquium for their insights. Finally, thank you to the 43rd TPRC Research Conference on Communications, Information, and Internet Policy for the opportunity to present this paper and to fellow panelists and participants for their comments.

1. *See, e.g.*, Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007) (dismissing a complaint to protect antitrust defendants from potentially burdensome pretrial discovery). Although the court's majority opinion did not identify the complaint as such, Justice Stevens wrote that the majority regarded plaintiff's complaint as a "fishing expedition." *Id.* at 577 (Stevens, J., dissenting).

2. *See* FED. R. CIV. P. 26–37.

proportionality analysis for defining the limits of civil discovery. The 2015 amendments to Rule 26 of the Federal Rules of Civil Procedure emphasize a proportionality inquiry as a key limit to discovery: the information sought must be proportional to the needs of the case.[3] Although this test expressly considers the financial burden and expense of discovery, "burden" should go beyond mere financial considerations and instead encompass concepts like the *privacy* burden. Thus, this Article proposes that the non-pecuniary burdens on privacy should be factored into the proportionality analysis.

By recognizing the need for proportional privacy, courts can draw meaningful boundaries to define the scope of discovery, effectively disaggregating digital data compilations to prevent overly intrusive discovery. Other tools within the court's arsenal, such as protective orders, should be used more liberally to limit access to entire mosaics of highly personal information.

Part II of this Article defines discovery of digital data compilations, using private social media account contents and smartphones in "bring your own device" workplaces as primary examples. Part III explains the historical development of civil discovery under the Federal Rules of Civil Procedure through the 2015 amendments, while Part IV summarizes general principles of privacy law and existing discovery decisions as to social media accounts and smartphones, with an analysis of the intersection between privacy and discovery. In Part V, this Article lays out the mechanisms by which privacy protection can serve as an additional guide for defining the scope of civil discovery, particularly through examining privacy burdens as a factor in the proportionality test.

II. DEFINING DISCOVERY OF DIGITAL DATA COMPILATIONS

The digital age brings with it an unprecedented ability to track, store, and access personal information about people. The new technology on which we have come to rely creates and maintains records of nearly all facets of daily life. Companies collect and mine our data as part of a phenomenon known as "Big Data."[4] Personal details—from the intimate to the mundane—are aggregated in massive databases. Third parties,

---

3. *See* COMMITTEE ON RULES OF PRACTICE AND PROCEDURE, STANDING COMMITTEE, SUMMARY OF THE REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE 14 (2014), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2014.pdf [hereinafter Judicial Conference Committee Summary].

4. *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 394 (2014) (explaining the various definitions of "big data" and focusing on its social impact).

like internet service providers, websites, and other companies, often have broad access to this data and use it for marketing and other purposes.[5]

Our daily interaction with technology not only contributes to big data, but our personal information is also aggregated in individual data compilations, such as in a social media account or on our smartphones. The personal information stored in these digital data compilations, in some ways, was voluntarily created and shared by individual users.[6] Nonetheless, this facet of big data still implicates its own privacy concerns.

This section will examine two main examples of digital data compilations: private portions of social media accounts and smartphone contents. These compilations contain a stunning amount of highly personal information—especially when looked at in the aggregate.

A. The Social Media Example

Social media accounts create a compilation of personal information over time. Given the wealth of detailed information aggregated in a social media account, lawyers understandably seek out social media content as a potential source of evidence in litigation. Indeed, social media evidence has been referenced in court decisions in criminal[7] and civil cases, including family law, employment cases, personal injury suits, or procedural matters such as personal jurisdiction.

---

5. Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995, 1002 (2013).

6. *Id.* 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; *see also* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 622 (2011) (describing the dramatic effect technology has on daily life and proposing ways for the Fourth Amendment to better protect social media and other digital content).

7. Social media evidence can be crucial in criminal prosecutions as well. In one criminal case, a Facebook post was used to corroborate an alibi. *See* Damiano Beltrami, *I'm Innocent. Just Check My Status on Facebook*, N.Y. TIMES (Nov. 11, 2009) http://www.nytimes.com/2009/11/12/nyregion/12facebook.html. The defendant in a felony armed robbery contended that he was more than thirteen miles away from the crime scene at the time, using his father's computer to send a Facebook status update, which read, "WHERE MY IHOP?" *Facebook Message Frees NYC Robbery Suspect*, NBCNEWS.COM (Nov. 12, 2009, 6:09 PM), http://www.nbcnews.com/id/33883605/ns/technology_and_science-tech_and_gadgets/t/facebook-message-frees-nyc-robbery-suspect/#.UfBRlTmGj0s. The charges against him were dropped. *Id.* In another criminal case, MySpace photographs and captions were admissible to impeach a minor witness' statement that she had been a virgin prior to an alleged rape. *In re* K.W., 666 S.E.2d 490, 494 (N.C. Ct. App. 2008). Also, MySpace photos of a criminal defendant holding wads of cash, wearing sunglasses, and throwing money were deemed relevant in a drug trafficking case; the photos were ultimately excluded as prejudicial. United States v. Drummond, No. 1:09–cr–00159, 2010 WL 1329059, at *2 (M.D. Pa. Mar. 29, 2010).

For example, in family law, social media evidence has been used in child custody disputes or actions to terminate parental rights.[8] In employment cases,[9] social media communications may be the basis for, or evidence in, harassment claims.[10] Social media evidence also appears in cases involving employment contracts, such as breach of confidentiality agreements or non-compete clauses.[11] Some wrongful discharge[12] or discrimination suits[13] also involve social media evidence.

---

8. *See, e.g.*, *In re* Marriage of Bates, No. 11–1293, 2012 WL 1440340, at *6 (Iowa Ct. App. Apr. 25, 2012) (holding that a mother's posts on Facebook revealed a physical and emotional inability to care for her children); Adams v. Johnson, 33 So. 3d 551, 552–53 (Miss. Ct. App. 2010) (holding that a mother's MySpace photos depicting risqué photos of herself along with photos of her children invited the possibility of sexual predators viewing the photos of her children and placed her children in danger in a child custody determination); High v. High, 697 S.E.2d 690, 698 (S.C. Ct. App. 2010) (holding that a father's disturbing MySpace comments supported the family court's decision to award child custody to the mother); *In re* T.T., 228 S.W.3d 312, 322–23 (Tex. App. 2007) ("There was sufficient evidence for the jury reasonably to conclude that [the father] set up the [MySpace page], which stated he was single and did not want children.").

9. Although social media evidence may be relevant in employment cases, employers need to remain mindful of the Electronic Communications Privacy Act or, for public employers, Constitutional or other limitations when taking adverse employment actions in response to employees' social media usage. *See, e.g.*, Hispanics United of Buffalo, Inc., No. 3-CA-27872, 2011 WL 3894520 (N.L.R.B. Sept. 2, 2011) (concluding that the employees' posts on Facebook, which constituted the grounds for their discharge, were protected under the National Labor Relations Act, rendering their discharge improper).

10. *See, e.g.*, Debord v. Mercy Health Sys. of Kan., Inc., 860 F. Supp. 2d 1263, 1269 (D. Kan. 2012) (considering an employee's Facebook comments in a sexual harassment case filed against her employer and supervisor); Treat v. Tom Kelley Buick Pontiac GMC, Inc., 710 F. Supp. 2d 777, 788 (N.D. Ind. 2010) (considering graphic MySpace posts by the defendant as evidence of sexual harassment in employment discrimination claim); Amira-Jabbar v. Travel Servs., Inc., 726 F. Supp. 2d 77, 81 (D.P.R. 2010) (describing co-workers' race-based Facebook comments that were presented as evidence of race discrimination).

11. *See, e.g.*, Yoder v. Univ. of Louisville, 417 F. App'x 529, 530 (6th Cir. 2011) (vacating the district court's order granting the plaintiff summary judgment where the plaintiff appealed her dismissal from nursing school on grounds of breaching confidentiality based on her MySpace post describing a live birth that she witnessed in class in an unflattering tone); Eagle v. Morgan, No. 11–4303, 2011 WL 6739448, at *16–17 (E.D. Pa. Dec. 22, 2011) (declining to dismiss an unfair competition counterclaim supported by evidence of misappropriation of a LinkedIn account by the plaintiff); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 39 (Minn. Ct. App. 2009) (holding that a health care provider's post on MySpace containing information from a patient's medical file constituted sufficient evidence to satisfy the "publicity" element of the plaintiff's invasion of privacy claim).

12. *See, e.g.*, Jaszczyszyn v. Advantage Health Physician Network, 504 F. App'x 440, 441 (6th Cir. 2012) (affirming summary judgment for defendant-employer where an employee was terminated on grounds of fraud after her supervisor viewed Facebook photos of the employee drinking at a local festival despite being on leave for back pain); *Treat*, 710 F. Supp. 2d at 788 (discussing a printout of a MySpace page produced by the plaintiff during discovery to bolster her claim of sexual harassment in the workplace and retaliatory discharge).

13. *See, e.g.*, Ade v. KidsPeace Corp., 698 F. Supp. 2d 501, 510 (E.D. Pa. 2010) (granting the defendant's motion for summary judgment where plaintiff alleged race and national origin discrimination as the pretext for his termination on grounds of sexual assault after considering evidence from a co-worker's MySpace account that contained sexually explicit messages from the

Personal injury is another area in which social media evidence is becoming more prevalent. Images and statements on Facebook have contradicted a party's claims of injury or damages, or have reflected emotional and mental state.[14] Even more broadly, a party's social media usage has also been cited for establishing personal jurisdiction.[15] For example, Facebook posts have been used as a basis to establish minimum contacts with a forum state.[16]

The wide range of cases relying on social media evidence is not surprising given the stunningly detailed personal information aggregated in a social media account. Take for example Facebook, the lead social media website to date.[17] On Facebook, a user sets up an account[18] and lists her date of birth, the places she has lived, the schools she has attended, her political affiliations, her family members' names, her current and present employer, and other personal details.[19] She then uploads a public profile picture and cover photo.[20]

She customizes her default privacy settings to limit the audience for

---

plaintiff).

14. *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010) (citing images of plaintiff smiling and outside of her home despite claims of permanent injury that left plaintiff confined to her home and bed); EEOC v. Simply Storage Mgmt., 270 F.R.D. 430, 436 (S.D. Ind. 2010) (noting the appropriate scope of discovery includes "profiles, postings, or messages" that "reveal, refer, or relate to any emotion, feeling, or mental state").

15. *See, e.g.*, Sweetgreen, Inc. v. Sweet Leaf, Inc., 882 F. Supp. 2d 1, 3–4 (D.D.C. 2012) (holding that the defendant's Twitter and Facebook accounts were "informational in nature" but, because no business was conducted through those accounts, they did not provide a foundation upon which to base personal jurisdiction); Craigslist, Inc. v. Hubert, 278 F.R.D. 510, 516 (N.D. Cal. 2011) (referencing a Twitter post in a jurisdictional analysis); Deckers Outdoor Corp. v. Turner, No. CV10–7273 CAS (AGRx), 2011 WL 781937, at *4 (C.D. Cal. Feb. 28, 2011) (citing posts on Facebook and Twitter).

16. *See, e.g.*, Wine Grp. LLC v. Levitation Mgmt., LLC, No. CIV. 2:11–1704 WBS JFM, 2011 WL 4738335, at *5 (E.D. Cal. Oct. 6, 2011) (considering a company's Facebook page in establishing jurisdiction); Rios v. Fergusan, 978 A.2d 592, 601 (Conn. Super. Ct. 2008) (holding that a YouTube video sufficed to confer personal jurisdiction); Bulk Process Equip. v. Earth Harvest Mills, Inc., No. 10–4176 (DWF/JSM), 2011 WL 1877836, at *3–4 (D. Minn. May 17, 2011) (concluding that the defendant's product promotions on Facebook, among other evidence, demonstrated an intentional and ongoing relationship between the defendant and the plaintiff and sufficient contacts with Minnesota to confer personal jurisdiction).

17. As of January 2015, Facebook had over 1.35 billion monthly active users. *See* Gene Marcial, *Why "Lightning-In-The-Stock" Facebook May be Top Choice for 2015*, FORBES (Jan. 12, 2015, 1:39 PM), http://www.forbes.com/sites/genemarcial/2015/01/12/why-lightning-in-the-stock-facebook-may-be-top-choice-for-2015/.

18. *See Facebook Help Center*, FACEBOOK, https://www.facebook.com/help/ (last visited Sept. 27, 2015) (explaining basic Facebook features).

19. *See Update Your Basic Info*, FACEBOOK, https://www.facebook.com/help/334656726616576/ (last visited Sept. 27, 2015).

20. *See Get Started*, FACEBOOK, https://www.facebook.com/help/467610326601639/ (last visited Sept. 27, 2015) (providing instructions for using the features of Timeline).

what she posts to Facebook.[21] In this way, she determines that her Facebook page should be seen only by a self-selected circle of people and not the public at large.[22] She even creates subsets of people, like "Friends except Acquaintances" and "high school friends," so that she can further limit the audience for individual posts.[23]

She downloads the Facebook app to her smartphone and grants the app access to her phone's location services.[24] This enables Facebook to use (and sometimes store) the geolocation data from her cell phone.[25] As a typical Facebook user, she uploads photos from her computer or her phone,[26] posts information about her location and places she visits,[27] posts status updates, "likes" or comments on Friends' posts,[28] sends one-on-one messages,[29] clicks on article links,[30] plays games or other third-party apps,[31] tags Friends (or is tagged) in photos,[32] RSVPs to events,[33]

---

21. *See Profile & Timeline Privacy*, FACEBOOK, https://www.facebook.com/help/393920637330807/ (last visited Sept. 27, 2015) (describing privacy controls for a user's Facebook Timeline).

22. *See id.*

23. *See id.*

24. *See Facebook Mobile Apps*, FACEBOOK, https://www.facebook.com/help/297024380340522?sr=1&query=apps%20location&sid=0bS2CmLp60XWabSHO (last visited Sept. 27, 2015).

25. *See Facebook Locations*, FACEBOOK, https://www.facebook.com/help/115298751894487?sr=4&query=location%20&sid=0VIhBUSUNl2LW0Utd (last visited Sept. 27, 2015).

26. *See How Do I Upload Photos?*, FACEBOOK, https://www.facebook.com/help/174641285926169 (last visited Sept. 27, 2015).

27. "Checking In" allows users to indicate their current physical location using the geo-locating features of their cell phones. Thus, for example, a user may check into a coffee shop or other participating business, and the Timeline will show an update containing that location information. *See Nearby Places*, FACEBOOK, https://www.facebook.com/help/461075590584469/ (last visited Sept. 27, 2015).

28. A "like" occurs when the user hits a thumbs-up "like" button for a comment, photo, or page. Often, the Timeline lists those pages that a user has "liked." *See Like*, FACEBOOK, http://www.facebook.com/help/452446998120360/ (last visited Sept. 27, 2015); *Like Button*, FACEBOOK, https://developers.facebook.com/docs/reference/plugins/like/ (last visited Sept. 27, 2015).

29. The direct-messaging feature can be used to contact any user on the site, unless default privacy settings are adjusted to prevent such contact. *See Sending a Message*, FACEBOOK, https://www.facebook.com/help/326534794098501 (last visited Sept. 27, 2015). Users can even send emails to regular email addresses using the direct-messaging feature. A user's email is the vanity username @facebook.com. *See How Do I Use My @facebook.com Email Address?*, FACEBOOK, https://www.facebook.com/help/224049364288051/?q=messages%20email&sid=0IihjxpAFjL3JLkRT (last visited Sept. 27, 2015).

30. Facebook creates links to "trending articles" that appear on users' news feeds based on what their Friends or others are reading. *See How do I Customize What I See in Trending?*, FACEBOOK, https://www.facebook.com/help/1530318343864702 (last visited Sept. 27, 2015).

31. Examples include King's Candy Crush Saga, and Zynga's Farmville or Words With Friends. *See All Games*, FACEBOOK,

joins groups,[34] and engages in instant "chat" conversations.[35]

Facebook is also linked to several apps and websites that she uses.[36] For example, her workout app tracks her route and time for her jogs, and that information can be posted to her Facebook account.[37] Because she stays logged into Facebook while surfing the internet, Facebook's social plugin features enable her to "like" other sites or immediately see what her Facebook Friends are saying on the third-party website itself.[38] When she fills out detailed, fun personal quizzes, those quiz results may appear in her Facebook account as well.[39]

She does at least some of these Facebook activities multiple times a day, every day, for years. And for most of these activities, Facebook creates some sort of digital record in her account.[40] This record includes the things she affirmatively posts to Facebook, but it also contains data created by Facebook, such as IP addresses used to access the account and login dates.[41] This body of data is not difficult or expensive to access—

---

http://www.facebook.com/appcenter/category/games/?platform=web (last visited Sept. 27, 2015).

32. Tagging occurs when a user uploads or posts information and marks that a Facebook user is present, pictured, or involved in that particular item. Unless security settings are customized, tagged items appear just as prominently as other items on the user's Facebook Timeline. *See What is Tagging and How Does It Work?*, FACEBOOK, http://www.facebook.com/help/124970597582337/ (last visited Sept. 27, 2015).

33. *See Events Privacy*, FACEBOOK, https://www.facebook.com/help/216355421820757/ (last visited Sept. 27, 2015).

34. *See Groups*, FACEBOOK, http://www.facebook.com/about/groups (last visited Sept. 27, 2015).

35. *See Chat Basics*, FACEBOOK, https://www.facebook.com/help/332952696782239/ (last visited Sept. 27, 2015).

36. When a Facebook user gives an app permission to share an activity on her timeline, that app can then publish stories about her experiences within the app or on websites. *Apps for Timeline*, FACEBOOK, https://www.facebook.com/help/386448801418869 (last visited Sept. 27, 2015).

37. *See How Do I Connect or Disconnect My MapMyFitness Account to Facebook?*, MAPMYFITNESS, https://support.mapmyfitness.com/hc/en-us/articles/200462650-How-do-I-connect-or-disconnect-my-MapMyFitness-account-to-Facebook- (last visited Sept. 27, 2015).

38. Other social plugins include a "Comments Box" that allows public comment on the third-party website through a Facebook account, a "Send" button that shares a link to a particular user or group, and "Recommendations" that display the most-liked content from Friends. *See What are Social Plugins?*, FACEBOOK, http://www.facebook.com/help/103828869708800/ (last visited Sept. 27, 2015).

39. *See* Associated Press, *Why Online Quizzes Are Taking over Your Facebook Feed*, NY POST (Feb. 24, 2014, 11:44 AM), http://nypost.com/2014/02/24/why-online-quizzes-are-taking-over-your-facebook-feed/.

40. *See Accessing Your Facebook Data*, FACEBOOK, http://www.facebook.com/help/405183566203254/ (last visited Sept. 27, 2015) (explaining that Facebook users may find Facebook data in either the activity log or the downloaded data).

41. Facebook allows users to access a downloadable file containing the following content: Account Status History (dates when the account was reactivated, deactivated, disabled, or deleted); Active Sessions (date, time, device, IP address, machine cookie, and browser information for all stored active sessions); Ads Clicked (dates, times, and titles of ads clicked for a limited retention

in fact, she's able to download a zip file of all of this information with one click.[42]

Because of the types of activities possible on Facebook, she frequently adds and edits posts.[43] Her Facebook activity spans the whole day, from both her computer and her cell phone. She knows she can deactivate her account for some time and reactivate it when she experiences social media withdrawal.[44] But she continues to check it dozens of times a day. Indeed, she can no longer function without Facebook: it is her main mode of staying in touch with friends and family, her primary means of learning about current news and events, her only mode of being invited to parties, her means for looking up information about restaurants or stores, her connection to classmates and coworkers, and her primary mode of email-like messaging or chatting. Without a Facebook account, her world would narrow to the point of major social isolation.[45]

The broad range of detailed, daily personal information she posts on the private portions of her Facebook account captures a detailed picture of her daily activities and emotions. When looked at in the aggregate, the account conveys highly personal, private information about her life. These details—easily downloaded in one file—may be sought as evidence in a wide range of cases.[46]

---

period); past and present addresses associated with the account; Ad Topics (list of targeted topics determined using other data on the user's Timeline); alternate names used on the account; apps; history of chat conversations; check-in history; personal information such as education, date of birth, family members, group membership, religious views, political views, gender, hometown, work, languages spoken, phone numbers; events joined or invited to; facial recognition data (a unique number used to help suggest the user to be tagged in photos); group memberships, list of friends, deleted friends, and followers; IP addresses used to log into the account; logins and logouts; messages sent and received via Facebook; photos; photo metadata; searches made on Facebook; and videos. *Id.*

42. *See Download All Facebook Photos, Status, Wall Posts Together in Zip File*, FACEBOOK (Nov. 13, 2010, 3:45 AM), http://www.facebook.com/note.php?note_id=10150118571353989.

43. *See How Do I Edit a Post I've Shared?*, FACEBOOK, https://www.facebook.com/help/462476073850410?sr=1&query=edit%20a%20post&sid=0NfBAM8XbzGKoQcXl (last visited Sept. 27, 2015) (explaining how to edit a post after it's been shared).

44. *See* Dr. Shlomit Yanisky-Ravid, *To Read or Not to Read: Privacy Within Social Networks, the Entitlement of Employees to a Virtual "Private Zone," and the Balloon Theory*, 64 AM. U. L. REV. 53, 56 (2014) (noting that people increasingly must rely on modern technology like Smartphone apps and social media to communicate with others).

45. *Id.*

46. *See Downloading Your Info*, FACEBOOK, https://www.facebook.com/help/131112897028467/ (last visited Sept. 27, 2015) (describing how to download a zip file of one's entire Facebook account).

B. The Smartphone Example

Another example of digital data compilations is the smartphone or other personal computing device. Text messages, call logs, and even app data may be relevant to a wide range of criminal and civil cases.[47] Additionally, smartphones and other personal devices are becoming an issue in business cases as well.[48] The modern workplace creates a special challenge because personal and professional content may be combined on one device. In particular, a current business trend is "Bring Your Own Device" ("BYOD") policies that allow an employee to use their personal cell phone, tablet, or other device for work-related purposes rather than relying on a company-issued device.[49] Companies may prefer these policies because they reduce their hardware costs, allow flexibility for their employees, and enable people to work from anywhere at all times.[50] But BYOD workplaces also must create policies for data security, ownership of company information, and e-discovery issues such as access to and preservation of data.[51]

---

47. *See, e.g.*, Julie Chow, Note, *"Bring Your Own Devices": A Cautionary Tale for Public Employees During Investigatory Searches*, 41 HASTINGS CONST. L.Q. 623, 624 (2014) (discussing the implications of BYOD policies for public employees).

48. *See, e.g.*, Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 486 (S.D.N.Y. 2010), *abrogated on other grounds by* Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135 (2d Cir. 2012) (employer had duty to produce emails and documents on employee personal devices); Koosharem Corp. v. Spec Pers., LLC, No. 6:08-583-HFF-WMC, 2008 WL 4458864, *2 (D.S.C. Sept. 29, 2008) (same).

49. *See Daily Document Update—Survey Finds Companies are not Communicating their BYOD Policies to Employees*, 2012 WL 6646252 (CCH) ¶ 31,623 (summarizing survey results); Pedro Pavón, *Risky Business: "Bring-Your-Own-Device" and Your Company*, BUS. L. TODAY (Sept. 2013), at 1; Hope A. Comisky & Tracey E. Diamond, *The Risks and Rewards of a BYOD Program: Ensuring Corporate Compliance Without Causing "Bring Your Own Disaster" at Work*, 8 CHARLESTON L. REV. 385, 386 (2014); Kimberly Peretti & Bruce Sarkisian, *Peering Into Personal Space: Investigating Employee-Owned Mobile Devices*, 17 No. 10 J. Internet L. 3, 3 (2014).

50. Pedro Pavón, *Risky Business: "Bring-Your-Own-Device" and Your Company*, BUS. L. TODAY (Sept. 2013), at 1.

51. *See* Henry Z. Horbaczewski & Ronald I. Raether, *BYOD Bring Your Own Device: Know the Privacy and Security Issues Before Inviting Employee-Owned Devices to the Party*, ACC DOCKET (April 2012) at 70, 74, http://www.ficlaw.com/links/raether/RIR_byod.pdf (explaining general security and business risks with BYOD policies); Philip J. Favro, *Inviting Scrutiny: How Technologies Are Eroding the Attorney-Client Privilege*, 20 RICH. J.L. & TECH. 2, 2 (2014) (warning about impact BYOD policies may have on attorney-client privilege); Ari L. Kaplan, *Advice from Counsel: Trends That Will Change E-Discovery (and What to Do About Them Now)*, 12 AVE MARIA L. REV. 109, 110 (2014); Mark Michels & Emily Soverel, *Dialing Up Potentially Responsive Information from Mobile Devices*, ACC DOCKET (April 2014), at 48–49, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-fas-dialing-up-potentially-responsive-information-from-mobile-devices-123014.pdf; John G. Browning, *Burn After Reading: Preservation and Spoliation of Evidence in the Age of Facebook*, 16 SMU SCI. & TECH. L. REV. 273, 276 (2013) (addressing preservation issues with BYOD workplaces).

Personal devices used for business result in vast amounts of personal information being commingled with company data. For example, an employee may have her own iPhone that serves as both her personal and work device. Like many modern smartphones, her iPhone functions like a mini computer—it allows her to do virtually any task a laptop computer would do.[52] Her iPhone receives both her work emails and her personal emails in one mailbox.[53] Her email accounts have calendars that sync her personal and professional events.[54] She also can send and receive texts.[55] Text messaging is a major avenue for communicating with her friends and family, but she sometimes uses texts to communicate with customers and coworkers. Ironically, her least-used feature on the iPhone is her phone, though she still uses it for both personal and professional calls, all of which are documented in a detailed call log and voicemail box.[56]

Apps form one of the biggest functions of her iPhone. She uses Twitter, Facebook, Instagram, and LinkedIn apps, which automatically connect to her social media accounts.[57] She has Google Maps, which she uses for personal navigation as well as for directions to client meetings.[58] Her Uber and Lyft apps let her get rides when she needs them for work or personal reasons.[59]

Her iPhone has a camera and stores hundreds or thousands of photographs and videos. She also has apps that connect to her photos and videos saved in the cloud or shared with others, such as Shutterfly and YouTube.[60] Most of these are personal photographs and videos, but she occasionally has photos and videos of products or professional events that she attends. Pandora and Spotify supply her soundtrack all day

---

52. *See Why There's Nothing Quite like iPhone*, APPLE, *https://www.apple.com/iphone/why-theres-iphone/#hardware* (last visited Sept. 27, 2015).

53. *See iPhone Support, Mail, Contacts, and Calendars*, APPLE, https://support.apple.com/en-us/HT201320 (last visited Sept. 27, 2015).

54. *Id.*

55. *See iPhone Support, Phone, Message, and Facetime*, APPLE, https://www.apple.com/support/iphone/messages/ (last visited Sept. 27, 2015).

56. *Id.*

57. *See Why There's Nothing Quite like iPhone*, *supra* note 52; *see also* Steven Tweedie, *The 13 Best Social Networking Apps*, BUSINESS INSIDER (Oct. 14, 2014, 6:18 PM), http://www.businessinsider.com/the-best-social-networking-apps-for-iphone-android-and-windows-phone-2014-10.

58. *See Google Maps for Android*, GOOGLE, http://www.google.com/intl/en_us/mobile/maps/ (last visited Sept. 27, 2015).

59. *See* LYFT, https://www.lyft.com/ (last visited Sept. 27, 2015); UBER, https://www.uber.com/ (last visited Sept. 27, 2015).

60. *See* SHUTTERFLY, http://www.shutterfly.com/mobile/?esch=1 (last visited Sept. 27, 2015); YOUTUBE, http://www.youtube.com/yt/devices/ (last visited Sept. 27, 2015).

long.[61] Her Kindle app lets her access her entire digital library, including business publications.[62] Her fitness apps help her track her sleep habits and activity throughout the day.[63] Most of her shopping is done via Amazon, and her Amazon app[64] gives her easy access to her entire order history. She occasionally uses Tinder[65] to find dates.

Other apps help her stay productive on the go. She has a dictation and voice memo app for making shopping lists or keeping business notes after a client meeting.[66] She uses a scanner app to scan and save documents using her phone's camera; Dropbox[67] lets her access and edit personal and professional files stored on the cloud; Skype[68] lets her video conference and message on the run; and her banking apps help her track her personal finances as well as business expenses.[69]

Her smartphone creates a digital record of her communications and other activities. It contains personal information about texts, phone calls, physical locations, and photographs that blend her personal and professional life. Although most of her app data is stored in the cloud, her smartphone nonetheless creates some record of app activity as well. Quite simply, her iPhone is a portal to a complete, intimate portrait of her entire life.

The sheer volume of information stored in an employee's personal device increases the amount of messages and other content that may fall within the ambit of civil discovery. The ease with which we create and store data, coupled with the increased reliance on smartphone features, means that BYOD policies will increase the frequency of smartphone discovery in business disputes.[70]

---

61. *See, e.g.*, PANDORA, http://www.pandora.com/ (last visited Sept. 27, 2015); SPOTIFY, https://www.spotify.com/us/free (last visited Sept. 27, 2015).

62. *See Kindle App*, AMAZON, www.amazon.com/gp/kindle/pc (last visited Sept. 27, 2015).

63. *See, e.g.*, ENDOMONDO, https://www.endomondo.com/about (last visited Sept. 27, 2015).

64. *See Amazon App for iPhone*, AMAZON, http://www.amazon.com/gp/feature.html?docId=1000291661 (last visited Sept. 27, 2015).

65. *See* TINDER, http://www.gotinder.com/faq (last visited Sept. 27, 2015).

66. *See* Kirk McElhearn, *Beyond Siri: Dictation Tricks for the iPhone and iPad*, MACWORLD (Sept. 23, 2013, 3:30 AM), http://www.macworld.com/article/2048196/beyond-siri-dictation-tricks-for-the-iphone-and-ipad.html.

67. *See Dropbox for iPhone*, DROPBOX, https://www.dropbox.com/iphoneapp (last visited Sept. 27, 2015).

68. *See Skype for iPhone*, SKYPE, http://www.skype.com/en/download-skype/skype-for-iphone/ (last visited Sept. 27, 2015).

69. *See* Lance Davis, *Best iPhone Personal Finance Apps*, BANKRATE, http://www.bankrate.com/finance/personal-finance/best-iphone-personal-finance-apps-1.aspx (last visited Sept. 27, 2015).

70. *See* Philip J. Favro, *Getting Serious: Why Companies Must Adopt Information Governance Measures to Prepare for the Upcoming Changes to the Federal Rules of Civil Procedure*, 20 RICH.

Both social media accounts and smartphones are becoming the subject of civil discovery attempts, and the rules must adequately protect against overly broad discovery of these digital data compilations.

III. CIVIL DISCOVERY GENERALLY

Pretrial civil discovery allows the court and litigants to assess the truth before trial, in an effort to promote fairness and avoid surprise in the adversarial process.[71] Cases are to be resolved without undue cost or delay.[72] Rules 26 through 37 of the Federal Rules of Civil Procedure allow parties to "narrow and clarify the basic issues between the parties" by learning relevant facts through discovery.[73] Parties are expected to exercise good faith and produce all non-privileged, responsive materials in their possession, custody, or control based on their own review first, before granting access to the opposing party.[74] If relevant information is withheld from the court and litigants, a miscarriage of justice may occur.[75]

Thus, the Federal Rules of Civil Procedure were created to allow for liberal access to information before trial—but within limits. Courts are given broad discretion to define the scope, limits, and mechanics of discovery in a given case.[76] Recognized limits on civil discovery include embarrassment, burden, expense, harassment, or prejudice.[77] The Rules also protect against *disproportionate* discovery.[78] Indeed, the 2015 amendments to Rule 26 emphasize proportionality as an additional limit on the scope of discovery. By enumerating these limits, the Federal Rules acknowledge that overly broad access to personal information may

---

J.L. & TECH. 5, 2 (2014).

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

72. FED. R. CIV. P. 1.

73. CHARLES ALAN WRIGHT ET AL., 8 FEDERAL PRACTICE AND PROCEDURE § 2001 (3d ed. 2015); *see also* FED. R. CIV. P. 26–37.

74. *See* FED. R. CIV. P. 26; Rachel K. Alexander, *E-Discovery Practice, Theory, and Precedent: Finding the Right Pond, Lure, and Lines Without Going on a Fishing Expedition*, 56 S.D. L. REV. 25, 43–44 (2011) (describing how the "good faith" system of discovery can be implemented effectively in the digital age).

75. *See Hickman*, 329 U.S. at 507.

76. Crawford–El v. Britton, 523 U.S. 574, 598 (1998). The Supreme Court recognized that courts have tremendous latitude in defining the scope and managing the mechanics of discovery, including permitting plaintiff to conduct only focused depositions of the defendant at first and limiting the subject matter to fact development before allowing other, broader discovery. *Id.* at 600. Under Rule 26, "[t]he trial judge can therefore manage the discovery process to facilitate prompt and efficient resolution of the lawsuit . . . ." *Id.* at 599.

77. *See* FED. R. CIV. P. 26(c).

78. *See* FED. R. CIV. P. 26(b)(2)(iii).

also taint the judicial process.

This section will address the historical development of the discovery rules, including overlaps between the limits placed on civil discovery and the concern for individual privacy. It will also address the ways the rules have adapted to deal with the challenges of electronically stored information (ESI) in particular, as well as the 2015 amendments highlighting the need for proportionality.

A. Historical Development of the Federal Rules

Before the 1930s, federal civil procedure required highly technical pleadings with little or no opportunity to discover the facts underlying the case.[79] Federal courts generally followed state rules of procedure, which differed greatly in the amount and types of discovery devices permitted.[80] This landscape created uncertainty and inconsistency in the civil litigation process, which many viewed as an obstacle to justice and that resulted in a call for reform.[81] Thus, the Federal Rules of Civil Procedure were first developed in 1938 in an effort to add transparency and fairness to the litigation process.[82]

But even at that time, lawyers, judges, and academics disagreed about the scope of discovery that should be permitted in civil trials.[83] Some of the lead drafters of the Federal Rules believed that pleadings should be simplified while discovery should be made more expansive.[84] Others expressed concern about discovery abuses, blackmail, excessive costs—and even invasions of privacy.[85]

Despite the debate over the scope of discovery, the initial rules ultimately allowed for broad discovery with little judicial intervention.[86] For the first time, a uniform federal procedure was enacted that allowed a

---

79. CHARLES ALAN WRIGHT ET AL., 8 FEDERAL PRACTICE AND PROCEDURE § 2001 (3d ed. 2015).

80. *See* Conformity Act of 1872, ch. 255, §§ 5–6, 17 Stat. 196, 197; Steven N. Subrin, *Fishing Expeditions Allowed: The Historical Background of the 1938 Federal Discovery Rules*, 39 B.C. L. REV. 691, 719 (1998) (describing the limited and inconsistent discovery mechanisms available under various state laws as surveyed by Ragland in *Discovery Before Trial*).

81. Subrin, *supra* note 80.

82. *Id.*

83. *Id.*

84. Notably, Charles Clark, the dean of Yale Law School and reporter for the Advisory Committee, advocated for less technical pleading requirements while Edson Sunderland, an expert in pretrial discovery, supported broad and open pretrial discovery. *See* Subrin, *supra* note 80, at 710.

85. Subrin, *supra* note 80, at 717.

86. *Id.* at 735; *see also* Hickman v. Taylor, 329 U.S. 495, 499 (1947).

broader discovery scope than any single state allowed.[87] This new discovery scheme contemplated pleadings that gave only general notice of the claims and issues while new, expansive discovery devices allowed for broader inquiries into the facts. To protect against some of the concerns expressed by critics, the rules also allowed for judicial intervention or protective orders.[88] Thus, even though the new rules created the most open discovery system ever seen in the US (and arguably abroad),[89] drafters and proponents still perceived the rules as protecting against the proverbial "fishing expedition[]."[90]

Understandably, some early decisions applying the 1938 Federal Rules entertained arguments about privacy harms resulting from invasive discovery. For example, one court noted that it was within the court's sole discretion to deny discovery that is an oppressive and "undue invasion of privacy."[91] Other courts also noted that, while discovery rules are meant to promote justice and should be liberally construed, "they cannot be liberally construed in contravention of inhibitions respecting unreasonable searches and seizures or the invasion of the right of privacy."[92]

The 1938 rules' shift from very limited to broad discovery is expressly recognized in the Supreme Court's 1947 decision in *Hickman v. Taylor*.[93] In that case, the Court noted that the discovery rules "are to be accorded a broad and liberal treatment. No longer can the time-honored cry of 'fishing expedition' serve to preclude a party from inquiring into the facts underlying his opponent's case."[94] Yet, even with

87. Subrin, *supra* note 80. *See also* Linda S. Mullenix, *Lessons from Abroad: Complexity and Convergence*, 46 VILL. L. REV. 1, 24 (2001) (noting that "American federal discovery provides for more liberal discovery than any other legal system in the world").

88. Subrin, *supra* note 80, at 719–20.

89. *See* Geoffrey C. Hazard, Jr., *From Whom No Secrets Are Hid*, 76 TEX. L. REV. 1665, 1665 (1998).

90. *Id.* at 1684 (citing William D. Mitchell's 1937 testimony).

91. Conn. Importing Co. v. Cont'l Distilling Corp., 1 F.R.D. 190, 193 (D. Conn. 1940). There, the court rejected an argument that tax returns were privileged but noted that it could have entertained an argument about invasion of privacy:

> [o]f course, the amount of protection properly required against an undue invasion of privacy will rest largely on the discretion of the court. But here the defendant, in Paragraph (f) of its motion, has designated just what documents it seeks to inspect; the plaintiff on a noticed hearing has had opportunity to protest against any oppressive invasion of its privacy. No such protest has been made; the only objection raised has been the claim of privilege. Furthermore, the plaintiff has itself put certain aspects of its income in issue. Thus it is scarcely entitled to the protection which in another case the court would afford to some defendant sued, say, by a commercial competitor. *Id.*

92. State *ex rel.* Cummings v. Witthaus, 219 S.W.2d 383, 386 (Mo. 1949).

93. 329 U.S. 495, 507 (1947).

94. *Id.*

its sweeping language about the broad scope of discovery, *Hickman* nonetheless recognized that courts have judicial discretion to limit discovery:

> [e]xamination into a person's files and records, including those resulting from the professional activities of an attorney, must be judged with care. It is not without reason that various safeguards have been established to preclude unwarranted excursions into the privacy of a man's work. At the same time, public policy supports reasonable and necessary inquiries.[95]

Ultimately, the Court exercised its discretion to prevent discovery of attorney work-product.[96]

Although several amendments occurred in the decades that followed, this basic approach to discovery remained unchanged for nearly half a century. By the 1970s, however, judges, scholars, and lawyers were lamenting the abusive nature of the civil discovery process.[97] Citing over-broad, costly, and oppressive tactics by counsel, critics began to advocate for greater limits on the amount and scope of discovery. By the 2000s, outcries about the cost and burden of civil discovery were common. Many judges and lawyers noted that discovery abuse was rampant and reforms were needed.[98] The sheer volume of discovery occurring in some cases prompted more concerns over the Federal Rules' broad discovery scheme. At the same time, however, other commentators noted that discovery costs are exaggerated by many, and that outcries about discovery abuses are not supported by reality.[99]

In 2000 the Federal Rules were amended to tighten the scope of discovery from what is relevant to the *subject matter* of the action to information that is relevant to the *claim or defense* of any party.[100] Under this revision, information relevant to the subject matter of the action is only discoverable upon a showing of good cause. Further, the

---

95. *Id.* at 497.

96. *Id.* at 514.

97. Judge Milton Pollack, *Discovery—Its Abuse and Correction*, 80 F.R.D. 219, 220 (1979).

98. *Changing the Rules: Will Limiting the Scope of Civil Discovery Diminish Accountability and Leave Americans Without Access to Justice Before the Subcomm. on Bankr. and the Courts of the Comm. of the U.S. S.*, 113th Cong. 42–43 (2013) (statement of Arthur R. Miller, University Professor, New York University School of Law).

99. Linda S. Mullenix, *Discovery in Disarray: The Pervasive Myth of Pervasive Discovery Abuse and the Consequences for Unfounded Rulemaking*, 46 STAN. L. REV. 1393, 1407 (1994); Linda S. Mullenix, *The Pervasive Myth of Pervasive Discovery Abuse: The Sequel*, 39 B.C. L. REV. 683, 684 (1998); Jack B. Weinstein, *What Discovery Abuse? A Comment on John Setear's The Barrister and the Bomb*, 69 B.U. L. REV. 649, 653–54 (1989).

100. FED. R. CIV. P. 1 advisory committee's notes (2000 Amendments).

Supreme Court in its 2007 decision in *Twombly* recognized and criticized discovery abuse and tightened the pleading requirements under Rule 8.[101] Thus, even though the Federal Rules did away with fact-specific pleadings, *Twombly* made clear that "[f]actual allegations must be enough to raise a right to relief above the speculative level."[102] Discovery as a whole was coping with the realities of its own immense scope and perceived cost—and evolving as a result.

1. The 2006 Amendments

The discovery landscape changed dramatically with the advent of electronically stored information (ESI), and the Federal Rules were amended in 2006 to address some of the challenges created by the scope and nature of discovery in the digital age.[103] The amendments expressly confirmed that ESI is part of the ambit of discoverable information, required that litigants confer and consider ESI-related discovery issues early on in the course of the litigation, and imposed some preservation requirements.[104]

Most significantly, however, the 2006 amendments addressed the issues of cost and burden associated with the broad range of data available in electronic forms. The new rules allowed for cost-shifting and other considerations and created a two-step analysis for what ESI must be produced based on the ease of access to it.[105] First, data that is deemed "reasonably accessible" should be produced like any other information: the party or witness should produce all relevant, non-privileged information after conducting their own review.[106] But under the 2006 amendments, a different, second step exists for data that is not reasonably accessible. If data must be restored or recreated at great cost, it is presumptively undiscoverable.[107] In order to overcome the presumption against discoverability, good cause must be shown.[108] The

101. *See* Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007).

102. *Id.* at 555.

103. *See* FED. R. CIV. P. 26 advisory committee's notes (2006 Amendments); Julia M. Ong, Note, *Another Step in the Evolution of E-Discovery: Amendments of the Federal Rules of Civil Procedure Yet Again?*, 18 B.U. J. SCI. & TECH. L. 404, 414 (2012).

104. FED. R. CIV. P. 26 advisory committee's notes (2006 Amendments) ("Rule 26(a)(1)(B) is amended to parallel Rule 34(a) by recognizing that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses.").

105. *See* FED. R. CIV. P. 26(b)(2)(B).

106. *Id.*

107. *Id.*

108. *Id.*

advisory notes to the Federal Rules list several factors considered before discovery of inaccessible data is permitted, including assessing the importance of the information sought and of the issues in the litigation.[109] Thus, for information that is not reasonably accessible, discovery is expressly limited to specific requests for important, responsive information in certain instances.[110]

The two-pronged approach to ESI discovery is notable for its emphasis on burden and cost over the basic presumption of liberal and broad discovery. The 2006 amendments try to account for the sheer volume of ESI that may exist in a case and provide at least some level of protection against undue cost or burden.[111] At the same time, as noted by at least one scholar, the 2006 amendments also encourage quick-peek and clawback agreements, which enable parties to see otherwise non-discoverable data.[112] In this way, the ESI amendments shift the balance from protecting parties and witnesses from overly broad discovery to allowing access to even more data.[113] At a minimum, ESI is meant to be equally discoverable as other, more traditional forms of discovery but with some limits based on cost and burden. Nonetheless, ESI presents unique challenges and burdens for screening out private, non-discoverable content. It also creates a unique privacy issue because of the detailed and aggregate nature of some large data sets.

2. The 2015 Amendments

The 2015 amendments[114] to the Federal Rules of Civil Procedure emphasize, reorder, and add to the proportionality factors. The concept of proportionality is mentioned in relation to several rules—from the scope of discovery to preservation duties. Most notably, the revised Rule

---

109. FED. R. CIV. P. 26 advisory committee's notes (2006 Amendments) (defining the seven factors as "(1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive, information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources").

110. *See* FED. R. CIV. P. 26(b)(2)(B).

111. *Id.*

112. Rory Bahadur, *Electronic Discovery, Informational Privacy, Facebook and Utopian Civil Justice*, 79 MISS. L.J. 317, 329 (2009).

113. *Id.* (arguing that the ESI rules obliterate informational privacy).

114. The 2015 Amendments are expected to take effect in December 2015. *Federal Rules of Civil Procedure Supreme Court Order*, SUPREME COURT OF THE UNITED STATES (Apr. 29, 2015), http://www.supremecourt.gov/orders/courtorders/frcv15_5h25.pdf.

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."[115] Several factors are considered to determine proportionality:

> 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.[116]

These factors, and proportionality in general, are not a new addition to the rules.[117] Some of the proportionality factors first appeared in the rules in the 1983 amendment. They existed to protect against "disproportionate discovery" and to allow judges to discourage "discovery overuse."[118] Their purpose was to avoid unduly burdensome or expensive discovery when considering the needs of the case, the amount in controversy, and the importance of the issues at stake.[119] From the beginning, proportionality was meant to serve as a limit on civil discovery itself.[120] Two additional proportionality factors were added in 1993[121] and, once again, the committee notes emphasized that proportionality should limit civil discovery: "the revisions in Rule 26(b)(2) [proportionality factors] are intended to provide the court with broader discretion to impose additional restrictions on the scope and extent of discovery[.]"[122] Despite the Committee's express intent to make proportionality a limit on discovery, courts seemed to under-utilize the proportionality factors. In 2000, the Committee added a cross-reference to the proportionality factors to Rule 26(b)(1), again in an effort "to emphasize the need for active judicial use of subdivision (b)(2) [proportionality factors] to control excessive discovery."[123]

Thus, the 2015 amendments make three major changes as to proportionality of civil discovery: (1) move the proportionality factors to

---

115. FED. R. CIV. P. 26(b)(1) (2015 Prospective Amendments).

116. *Id.*

117. *See* Judicial Conference Committee Summary, *supra* note 3, at Rules App'x B-5; *see also* Thomas Y. Allman, *Local Rules, Standing Orders, and Model Protocols: Where the Rubber Meets the (E-Discovery) Road*, 19 RICH. J.L. & TECH. 8, 73 (2013) (describing local initiatives to make e-discovery more fair and affordable).

118. FED. R. CIV. P. 26 advisory committee's notes (1983 Amendments).

119. *Id.*

120. *See id.*

121. The existing two factors were also moved to a different subpart of Rule 26.

122. *See* FED. R. CIV. P. 26 advisory committee's notes (1993 Amendments).

123. *See* FED. R. CIV. P. 26 advisory committee's notes (2000 Amendments).

a more prominent placement within Rule 26, (2) reorder the existing proportionality factors to make "importance of the issues at stake" the first factor, rather than leading with the amount in controversy, and (3) add a final factor of "the parties' relative access to relevant information."[124] Critics of these changes felt that they favor defendants, allow for too much subjectivity and flexibility, will result in blanket "proportionality" objections to civil discovery requests, and require a multi-factor test that places too great a burden on the court.[125] Additionally, some critics felt that proportionality already exists in discovery, making these changes unnecessary.[126]

Even with the renewed emphasis on proportionality in the 2015 amendments, the proportionality test itself largely focuses on economic concerns. Indeed, the "burden or expense" that the court weighs against the needs of the case are largely *financial* burdens.[127] Critics of the 2015 amendments have pointed out that the proportionality test may be abused by large corporate litigants who will shield otherwise discoverable information on economic grounds alone.[128] Although some view discovery as financially burdensome and overly broad, others have pointed out that arguments as to undue cost are exaggerated and result in an unfair advantage to large corporate interests.[129] Further, some have noted that non-pecuniary considerations should also be taken into account when weighing the proportionality factors.[130]

---

124. *See* Judicial Conference Committee Summary, *supra* note 3, at Rules App'x B-8.

125. *Id.* at Rules App'x B-5.

126. *Id.*

127. *See id.*

128. *See* Stephen B. Burbank, *Proportionality and the Social Benefits of Discovery: Out of Sight and Out of Mind?*, 34 REV. LITIG. __ (forthcoming 2015) (warning that courts should not privilege costs over the benefits of litigation or monetary considerations over variables that are not as easily quantified).

129. *See* Emery G. Lee III & Thomas E. Willging, *Defining the Problem of Cost in Federal Civil Litigation*, 60 DUKE L.J. 765, 779–80 (2010); Emery G. Lee III & Thomas E. Willging, NATIONAL CASE-BASED CIVIL RULES SURVEY: PRELIMINARY REPORT TO THE JUDICIAL CONFERENCE ADVISORY COMMITTEE ON CIVIL RULES 27–33 (2009), http://www.fjc.gov/public/pdf.nsf/lookup/dissurv1.pdf/$file/dissurv1.pdf (median costs of discovery, including attorney's fees, are less than four percent of defendants' reported stakes); *see also* Danya Shocair Reda, *The Cost-and-Delay Narrative in Civil Justice Reform: Its Fallacies and Functions*, 90 OR. L. REV. 1085, 1116–23 (2012).

130. 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) (Principle 5 states that "[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) (explaining the dangers of over-emphasizing monetary factors alone in the proportionality analysis); 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) (arguing that proportionality may still be used as a limit in non-monetary or low-value cases); Jordan

Other changes in the 2015 amendments further clarify the limits that exist on overly broad discovery. These changes include streamlining the language in Rule 26(b)(1), which describes discoverable matters, and removing "subject-matter discovery" in favor of confining discovery to the parties' claims and defenses, absent a showing of good cause.[131] Notably, the amendments also replace "reasonably calculated to lead" to admissible evidence with the statement that "[i]nformation within this scope of discovery need not be admissible in evidence to be discoverable."[132] This change clarifies that "reasonably calculated" was never intended to define the scope of discovery.[133] Further, Rule 26 now makes clear that allocation of expenses may be included in protective orders, without intending to make cost-shifting a common practice.[134] The 2015 amendments also emphasize increased cooperation among the parties[135] and greater judicial oversight of the discovery process.[136]

As a whole, the 2015 amendments take into account the sheer volume of data that exists in many cases and attempt to create additional boundaries to the scope of discovery. Most notably, the Federal Rules will now require more careful consideration of the proportionality of discovery.

B. Relevance, Proportionality, and Protective Orders

Even with 2015 amendments to the Federal Rules, civil discovery, as a general proposition, still broadly encompasses all relevant information. Information is relevant if it "'bears on' or might reasonably lead to information that 'bears on' any material fact or issue in the action."[137] Because relevance is a broad concept, it is difficult to apply in the

---

M. Singer, *Proportionality's Cultural Foundation*, 52 SANTA CLARA L. REV. 145, 149 (2012) ("disproportionate discovery is caused not by abuse of attorney discretion, but by a breakdown of the core values and cultural norms that typically animate civil litigation"); Gordon W. Netzorg & Tobin D. Kern, *Proportional Discovery: Making It the Norm, Rather Than the Exception*, 87 DENV. U. L. REV. 513, 529 (2010) (advocating for proportionality to be the default, threshold rule for defining the scope of discovery, including the use of non-monetary factors in the proportionality analysis); Leah M. Wolfe, Comment, *"The Perfect is the Enemy of the Good": The Case for Proportionality Rules Instead of Guidelines in Civil E-Discovery*, 43 CAP. U. L. REV. 153, 189 (2015) (noting that the Sedona Principles support judicial consideration of any nonmonetary factor when determining proportionality-based limits of discovery).

131. *See Judicial Conference Committee Summary*, *supra* note 3, at Rules App'x B-9.

132. *Id.*

133. *Id.* at Rules App'x at B-10.

134. *Id.* at Rules App'x at B-10–11.

135. FED. R. CIV. P. 1 advisory committee's notes (2015 Amendments).

136. *See id.*

137. Dongguk Univ. v. Yale Univ., 270 F.R.D. 70, 72–73 (D. Conn. 2010).

abstract, and instead should be grounded in particular facts and circumstances of each case.[138] Fishing expeditions and requests for unfettered discovery are disallowed.[139] Rather, discovery requests must seek specific, relevant material and must be stated with "reasonable particularity."[140]

Proportionality, as first established in the 1983 amendments, already serves as a backstop to overly broad discovery and promotes "fair and efficient operation of discovery rules."[141] Proportionality can limit discovery even when discovery requests are otherwise reasonably calculated to lead to admissible evidence:

> [a]fter 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, i.e., that there is no other juncture in the pretrial period when there would be a clearly happier balance between the benefit derived from and the burdens imposed by the particular discovery effort.[142]

Thus, courts possess the power to limit the scope of discovery to meet the needs of the case and should take proportionality into account. However, the proportionality requirement does not "obligate courts to conduct a detailed balancing of the enumerated factors" in every case.[143] Instead, proportionality serves as an additional limit and tool for active judicial management of the discovery process.[144]

---

138. *See id.* at 73.

139. *See, e.g.*, Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007) (dismissing a complaint to protect antitrust defendants from potentially burdensome pretrial discovery). Although the court's majority opinion did not identify the complaint as such, Justice Stevens wrote that the majority regarded plaintiff's complaint as a "fishing expedition." *Id.* at 577 (Stevens, J., dissenting); *see also* Bissessur v. Ind. Univ. Bd. of Trs., 581 F.3d 599, 604 (7th Cir. 2009) ("Allowing this case to proceed absent factual allegations that match the bare-bones recitation of the claims' elements would sanction a fishing expedition costing both parties, and the court, valuable time and resources.").

140. FED. R. CIV. P. 34(b)(1)(A) (a discovery request "must describe with reasonable particularity each item or category of items to be inspected").

141. *Dongguk*, 270 F.R.D. at 73.

142. *In re* Convergent Techs. Sec. Litig., 108 F.R.D. 328, 331 (N.D. Cal. 1985).

143. *In re* Cooper Tire & Rubber Co., 568 F.3d 1180, 1194 (10th Cir. 2009).

144. *See id.*; *see also* The Sedona Conference®, *The Sedona Conference® Commentary on Proportionality in Electronic Discovery*, 14 Sedona Conf. J. 155, 158 (Conor R. Crowley et al. eds.) (2013) (discussing the origins of proportionality, providing examples of its application, and proposing principles to guide courts, attorneys, and parties).

Despite the flexibility of the proportionality factors, cases applying the proportionality test mainly focus on financial burden.[145] But even financial burden is difficult to quantify in some cases, as clear ratios between the cost of discovery and the value of the underlying claim cannot be assessed.[146] Additionally, other factors expressly contemplate non-financial consideration, such as the importance of the issues at stake in the litigation. This factor implicates broader societal values that are not subject to mathematical calculation.[147] Thus, the proportionality analysis necessarily incorporates non-monetary considerations, such as vindication of personal or private values,[148] even though the expense of discovery is the main focus of the proportionality inquiry in many cases.

In addition to proportionality-based limits, the rules allow courts to issue protective orders for good cause in order to protect against "annoyance, embarrassment, oppression, or undue burden or expense."[149] Protective orders are an additional tool available for courts to prevent discovery abuses.[150] The good cause standard requires particular facts demonstrating potential harm, and not on conclusory allegations.[151] The party seeking the protective order must show a particular need for protection, rather than broad allegations of harm.[152] Further, the harm must be significant.[153] Nonetheless, harms such as embarrassment, if particularly serious, can be grounds for good cause.[154]

---

145. *See, e.g.*, Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 364 (D. Md. 2008) (noting that discovery might be excessive in relation to the value of the plaintiffs' claims). Nonetheless, at least one case has expressly considered nonmonetary burdens when limiting discovery. *See* Hunter v. Ohio Indem. Co., No. C 06-3524, 2007 WL 2769805, at *1 (N.D. Cal. Sept. 21, 2007) ("the burden of a deposition on Ms. Jansen, who has virtually no knowledge of any issues specific to the coverage at issue, and is caring for a spouse with a life-threatening illness, would be inhumane as well as unproductive.").

146. *See id.*

147. *See* Jonah B. Gelbach & Bruce H. Kobayashi, *The Law and Economics of Proportionality in Discovery*, Univ. of Pa. Law Sch. Legal Scholarship Repository, Paper No. 1521, at 5–6 (2014), http://scholarship.law.upenn.edu/faculty_scholarship/1521.

148. *See Judicial Conference Committee Summary*, *supra* note 3, at Rules App'x B-42.

149. FED. R. CIV. P. 26(c)(1).

150. *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 34–36 (1984).

151. *See, e.g.*, Anderson v. Cryovac, Inc., 805 F.2d 1, 7 (1st Cir. 1986) (protective order properly used to restrict press access to discovery in environmental tort case). By analogy, courts restrict similar public access to pretrial criminal hearings because the interest in a fair trial and privacy outweigh the public's right to access. *Id.* at 11 (citing *In re* Globe Newspaper Co., 729 F.2d 47 (1st Cir. 1984)).

152. *See* Cipollone v. Liggett Grp., Inc., 785 F.2d 1108, 1121 (3d Cir. 1986).

153. *Id.*

154. *Id.*; Jonathan M. Redgrave et al., *Understanding and Contextualizing Precedents in E-Discovery: The Illusion of Stare Decisis and Best Practices to Avoid Reliance on Outdated Guidance*, 20 RICH. J.L. & TECH. 8, 40 (2014) (noting that protective orders may not suffice to protect individual privacy interests).

As a whole, courts can limit discovery due to undue burden and expense under the proportionality limits, and can use protective orders as another method by which to mitigate the harm of overly burdensome discovery.[155] As with discovery in general, courts are given wide discretion to fashion protective orders to address the wide range of harms contained in a particular case.[156] Thus, protective orders may be used for reasons beyond the enumerated ones.[157]

The rules have evolved to adapt to the modern realities of litigation and technological advancements over time, and the 2015 amendments appear to continue the trend of limiting the broad scope of civil discovery. In particular, proportionality, relevance, and protective orders serve as major tools for judges in managing discovery's scope. Nonetheless, the law must continue to adapt to the realities of new technology and privacy implications of massive digital data compilations and modern data collection.[158]

IV. THE INTERSECTION OF PRIVACY LAW AND CIVIL DISCOVERY IN THE DIGITAL AGE

The very existence of large digital data compilations and potential access to them in discovery implicate privacy concerns. Indeed, privacy harm impacts fundamental values of a free society, such as freedom of speech, association, and expression.[159] Generally, the advent of social media and smartphones has triggered a re-examination of existing privacy law principles.[160] The digital age has only exacerbated the challenges of creating principled and effective privacy protections. New technology encourages (or even forces) people to expose traditionally private spheres to public view and to share more personal information

---

155. *See* Dongguk Univ. v. Yale Univ., 270 F.R.D. 70, 73 (D. Conn. 2010) ("With regard to the 'undue burden and expense' provision, Rule 26(c) operates in tandem with the proportionality limits set forth in Rule 26(b)(2).").

156. *Id.* ("The text of Rule 26(c) is construed liberally to include a wide range of potential harms not explicitly listed.").

157. *See id.*

158. *See* Jonathan M. Redgrave et al., *Understanding and Contextualizing Precedents in E-Discovery: The Illusion of Stare Decisis and Best Practices to Avoid Reliance on Outdated Guidance*, 20 RICH. J.L. & TECH. 8, 6 (2014).

159. *See* Woodrow Hartzog, *The Value of Modest Privacy Protections in a Hyper Social World*, 12 COLO. TECH. L.J. 333, 345–46 (2014); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 611 (2014).

160. *See, e.g.*, Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165, 167 (2012); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1124 (2013).

than ever before.[161] But as society adjusts to a new world of over-sharing, the current state of the law facilitates an erosion of privacy rights through its incomplete and ineffective treatment of modern privacy concerns. Nonetheless, new theories of privacy are emerging in light of the privacy harms we now face, and some of those theories can inform (and improve) the civil discovery process.

The term "privacy" itself is vague and imprecise, and the U.S. legal system struggles to define adequate privacy protections in many different contexts. A comprehensive body of "privacy law" does not exist, and instead privacy protection draws on different sources of law and notions of harm.[162] This results in an unclear patchwork of statutes or constitutional protections that create significant gaps and inconsistencies.[163]

In the civil discovery context, privacy harms may seem less severe than in other areas, such as Fourth Amendment law. Nonetheless, while the need for open access to information in civil litigation justifies some intrusion, privacy harms cannot be completely ignored simply because a civil case is pending. Rather, even civil discovery has limits—limits that necessarily draw on important privacy-based principles.

This section will provide an overview of privacy law, including information privacy, physical autonomy, private spaces, and cell phones; and the emerging "mosaic theory" of privacy. It will also explain privacy's role in civil discovery, both as to established categories of privacy protection and as to cases addressing social media and smartphone discovery.

A. Overview of Privacy Law

Scholars have attempted to divide and categorize the types of privacy rights recognized under various sources of U.S. law. These divisions include "states" of individual privacy (such as solitude, intimacy, and anonymity),[164] categories of substantive law (tort law, Fourth Amendment law, First Amendment law, and state constitutions, for

---

161. Dr. Shlomit Yanisky-Ravid, *To Read or Not to Read: Privacy Within Social Networks, The Entitlement of Employees to a Virtual "Private Zone," and the Balloon Theory*, 64 AM. U. L. REV. 53, 55 (2014) (noting that people increasingly must rely on modern technology like smartphone apps and social media to communicate with others).

162. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 481 (2006).

163. *See, e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 208 (1992); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999).

164. ALAN F. WESTIN, PRIVACY AND FREEDOM 31–32 (1967).

example),[165] and spaces or activities protected (such as physical space, personal choices, and personal information).[166] Other scholars have honed in on the privacy *harm* that may occur.[167]

Taken as a whole, no clear definition of "privacy" exists and, not surprisingly, no cohesive privacy law has emerged to date either. Nonetheless, as relevant to civil discovery, three general concepts of privacy rights become particularly important: (1) the right to control one's personal information, (2) the right to physical autonomy and protection against intrusion into one's private sphere, including smartphones or cell phones, and (3) the emerging "mosaic theory" of privacy rights.

1. Information Privacy

Information privacy involves protecting against the collection and use of personal information. Like many theories of privacy, information privacy can be difficult to define and overlaps with other concepts or substantive areas of law. Nonetheless, the interest in keeping information about oneself private—both in its creation and use—is an important concept to consider within the broader framework of civil discovery.

A patchwork of substantive law serves as the main mode of protecting information privacy. For example, tort law provides a remedy when private facts are publicized or when there is an intrusion upon one's seclusion.[168] Other torts, like defamation, breach of confidentiality, infliction of emotional distress, and related dignitary torts protect one's reputation or sense of autonomy.[169] Property rights may protect information privacy, such as through conversion and trespass claims.[170] Contract law may be used to ensure confidentiality of

165. Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1335 (1992).

166. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202–03 (1998). Professor Kang refers to these three concepts as decisional, spatial, and informational privacy. *Id.*

167. *See, e.g.*, Solove, *supra* note 162, at 564; M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1162 (2011); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 885 (2003).

168. Scholars cite a famous law review article by Samuel D. Warren and Louis D. Brandeis as the origin of modern privacy torts. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). At least four distinct privacy torts emerged from this article, including (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light, and (4) appropriation. *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

169. *See* Prosser, *supra* note 168, at 398.

170. *See* Solove, *supra* note 162, at 552.

information within certain contractual relationships.[171] Even criminal law includes some protection against misappropriation and misuse of one's personal information, such as through criminal penalties for wiretapping and identity theft.[172]

In addition to the common law, several state and federal statutes create a patchwork of narrow laws protecting specific bits and pieces of information. Examples include:

- Fair Credit Reporting Act, governing the use and disclosure of certain financial information;[173]
- Children's Online Privacy Protection Act, protecting personal information of minors;[174]
- Stored Communications Act, preventing web service providers from disclosing information to third parties without consent;[175]
- Family Educational Rights and Privacy Act, protecting school records;[176]
- Video Privacy Protection Act, protecting video rental information;[177]
- Telephone Consumer Protection Act, limiting telemarketing;[178]
- Health Insurance Portability and Accountability Act, protecting medical information;[179] and
- The Federal Wiretapping Act, prohibiting the interception of certain communications.[180]

171. *See id.* at 529.

172. *See, e.g.*, Federal Wire Tap Act, 18 U.S.C. § 2516 (2012) *amended by* Electronic Communications Act of 1986, Pub. L. No. 99-508 (1986).

173. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2012); Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2012); Video Privacy Protection Act, 18 U.S.C. § 2710 (2012); Telecommunications Act of 1996, 47 U.S.C. § 222 (2012); Cable Communications Policy Act, 47 U.S.C. § 551 (2012).

174. Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (2012).

175. Stored Communications Act, 18 U.S.C. § 2701 (2012).

176. Family Educational Rights and Privacy Act, 20 U.S.C. § 1221 (2012).

177. Video Privacy Protection Act, 18 U.S.C. § 2710 (2012).

178. Telephone Consumer Protection Act, 47 U.S.C. § 227 (2012).

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

180. Federal Wiretapping Act, 18 U.S.C. § 2516 (2012), *amended by* Electronic Communications Act of 1986, Pub. L. No. 99-508 (1986); Robert A. Pikowsky, *The Need For*

This list is but a few examples. Dozens of other state and federal laws limit the collection and use of personal information, but in narrowly defined circumstances. As demonstrated by this web of statutory provisions, U.S. law has evolved in a piecemeal fashion, providing little comprehensive privacy protection. At the same time, the very existence of so many piecemeal information privacy statutes indicates that we value protecting information privacy enough to place privacy-based limits on the use of personal information in certain contexts and categories.[181]

In addition to the common law and statutory examples, Constitutional law provides another source of possible protection of information privacy. The First Amendment protects one's right to speak anonymously and protects against forced disclosure of one's associations.[182] The Fourth Amendment's protections against unreasonable search and seizure also border on information privacy, such as protecting phone conversations on a public pay phone.[183]

Most notably, the Fifth Amendment's substantive due process protections may include protecting one's personal matters from disclosure. In *Whalen v. Roe*,[184] the court examined the constitutionality of a New York state statute that required the state to collect personal information about patients who are prescribed certain drugs.[185] Although the statute was ultimately upheld as constitutional, the Supreme Court noted that a privacy interest exists in "avoiding disclosure of personal matters."[186] However, the Court stopped short of defining an express constitutional right to information privacy.[187] Similarly, in *Nixon v. Administrator of General Services*,[188] the Court acknowledged a privacy interest in "avoiding disclosure of personal matters" but rejected any such concern as to matters of public interest concerning a public official.[189] Subsequently, in *NASA v. Nelson*,[190] the Supreme Court once

---

Revisions to the Law of Wiretapping and Interception of Email, 10 MICH. TELECOMM. & TECH. L. REV. 1, 39 (2003).

181. *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003).

182. *See* U.S. CONST. amend. I.

183. *See* Katz v. United States, 389 U.S. 347, 358 (1967).

184. 429 U.S. 589, 591 (1977); *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977).

185. *Whalen*, 429 U.S. at 591.

186. *Id.* at 599.

187. *Id.* at 605–06.

188. 433 U.S. 425, 457 (1977).

189. *Id.* at 457, 455–58 (holding that an act requiring retention and access to presidential records is not an unconstitutional invasion of former President Nixon's privacy rights).

again seemed to recognize a constitutional right to information privacy but fell short of defining or enforcing such a right. There, the Court "assume[d], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*"[191] and instead noted that statutory protections applied (but were not violated).[192] Thus, the Court upheld as constitutional background-check questionnaires that were required as part of government employment.[193]

Even though these cases did not enforce a constitutional right of information privacy, they indicate that some type of constitutional limits on the collection and use of personal information may exist. At least one state's constitution goes even further to protect information privacy. California's constitution contains a fundamental right to privacy that applies to both state actors and private individuals.[194] This constitutional provision has even been applied to nongovernmental entities to limit the scope of civil discovery.[195]

Although information privacy is developing as a distinct aspect of privacy law, constitutional protection remains undefined and vague. Statutory provisions provide some protection, but the web of laws that govern this area is complex and incomplete. These existing privacy laws may be inadequate in protecting individuals against overly intrusive disclosure of personal information.

2. Physical Autonomy, Private Spaces, and Cell Phones

The U.S. Constitution also creates privacy-based protections for physical autonomy and against government intrusion into physical spaces. Physical autonomy involves the fundamental right to make decisions about one's body. Examples include the decision to terminate a pregnancy,[196] the right to marital privacy,[197] and the right to private sexual autonomy.[198] Physical autonomy relies on a fundamental right to

190. 562 U.S. 134 (2011).

191. *Id.* at 138.

192. *See id.* at 159 ("In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy.") (citing *Whalen*, 429 U.S. at 605).

193. *Id.*

194. *See* CAL. CONST. art. 1, § 1.

195. Hill v. Nat'l Collegiate Athletic Ass'n., 865 P.2d 633, 641 (Cal. 1994).

196. Roe v. Wade, 410 U.S. 113, 154 (1973).

197. Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (decision to procreate); Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (contraception use).

198. Lawrence v. Texas, 539 U.S. 558, 578 (2003).

privacy under the U.S. Constitution and serves as a limit on government intrusion into these private decisions and activities.

Similarly, the U.S. Constitution creates privacy-based protections against intrusion into one's physical space, such as one's home and private papers.[199] Fourth Amendment law applies in the specific context of government intrusion into private spheres, and prohibits unreasonable searches and seizures by law enforcement, without first showing probable cause. At its core, the Fourth Amendment prohibits governmental "fishing expedition" searches by requiring a warrant or a specific exception to the warrant requirement. Additionally, warrants must be particularized, describing what will be searched and for what specific evidence. Searches that incidentally capture irrelevant information or that extend to information about innocent third parties may also violate the Fourth Amendment.[200]

Although the Fourth Amendment protects against unlawful search and seizure into these physical spaces, it has considerable limitations. These limitations include the reasonable expectation of privacy standard and the third-party disclosure rule. Generally, in order for Fourth Amendment protection to apply, the person must have a reasonable expectation of privacy.[201] This expectation must be objectively reasonable and not merely subjective.[202] Additionally, disclosure of private information to third parties undermines any argument that an objectively reasonable expectation of privacy exists.[203]

In the digital age, these limitations can prove fatal for attempts to apply privacy protection to most content transmitted electronically, given that an internet service provider, website, or other third party receives and transmits content.[204] Further, interactive "social" tools like

---

199. *See* U.S. CONST. amend. IV.

200. *See* Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1460–62 (1996) (explaining how innocent third parties may have greater privacy rights, but how they have the least incentive or fewest procedural mechanisms to enforce their Fourth Amendment privacy rights); Winston v. Lee, 470 U.S. 753, 766 (1985) (noting that a heightened standard of reasonableness may apply when the privacy intrusion of the search is more severe). Electronic surveillance methods increase the likelihood that innocent third party information is captured in a search. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 18 (2013) ("the production of cell-site location information has resulted in significant breaches of innocent third parties' privacy rights.").

201. *See* Katz v. United States, 389 U.S. 347, 360–61 (1957) (Harlan, J., concurring) (expectation of privacy must not only be subjective, but also objectively reasonable).

202. *Id.*

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

204. *See* Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*,

Facebook are premised on sharing,[205] so expectations of privacy to communications and content on social media websites may be seen as objectively *un*reasonable.[206]

Nonetheless, in the Fourth Amendment context, courts have recognized that using social media websites' privacy settings is relevant in determining whether a reasonable expectation of privacy exists. In *United States v. Meregildo*,[207] the court examined whether probable cause is needed before law enforcement can search private Facebook content.[208] The court noted that public postings are not protected by the Fourth Amendment, but "postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected."[209] Further, some commentators have noted that, while there is no reasonable expectation to privacy in social media posts generally, certain private posts should be afforded some protection based on the specific type of data that is involved.[210] Privacy also must be viewed in the context of society.[211] Because privacy is subject to broad and imprecise definitions, it is best viewed in relation to the harm that may be caused to an individual.[212] At the same time, privacy law must adapt to the new realities of people living their lives online.[213]

---

66 HASTINGS L.J. 183, 227 (2014).

205. For example, Facebook makes clear that its mission is to provide a platform for sharing and connecting with others: "Founded in 2004, Facebook's mission is to give people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them." *About Facebook*, FACEBOOK, https://www.facebook.com/facebook/info?tab=page_info (last visited Sept. 22, 2015).

206. Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010).

207. 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (holding that the Fourth Amendment was not violated when law enforcement received private social media information from a Facebook "friend" of the defendant).

208. *Id.*

209. *Id.* at 525.

210. Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 242, 246–47 (2012).

211. *See* Solove, *supra* note 162, at 482–84 (attempting to develop a new way of looking at privacy based on harms created by various privacy problems).

212. *Id.* at 486–88.

213. *See* Teri Dobbins Baxter, *Low Expectations: How Changing Expectations of Privacy Can Erode Fourth Amendment Protection and a Proposed Solution*, 84 TEMP. L. REV. 599, 599–600 (2012) ("[T]echnology has . . . brought about significant cultural shifts. One prominent example is the way that people, particularly young people, socialize and become socialized."); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011) ("[A] future is nearly upon us that will make it impossible to preserve the privacy even of traditional Fourth Amendment bastions, such as the home, without considering the intertwined effects of technological and social change."); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 511 (2005) (arguing for a strict and narrow construction of reasonable

Smartphones further complicate the analysis. The Supreme Court recently acknowledged that new technology and easy access to vast amounts of digital content is testing the traditional Fourth Amendment analysis of privacy interests. In particular, the Court in *Riley v. California*[214] made clear that searches of cell phone content require a warrant, even when the phone is seized incident to a lawful arrest.[215] The Court compared smartphones (which it refers to as "cell phones") to mini computers that "place vast quantities of personal information literally in the hands of individuals" and acknowledged that serious privacy concerns exist when cell phone content is accessed by law enforcement.[216] Indeed, unlike traditional, physical objects, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[217] The Court detailed how a modern cell phone now contains thousands of pieces of information, including pictures, videos, call logs, text messages, internet browsing history, and calendar entries.[218] If in physical form, this level of detailed, portable content would never be carried around by a person, yet cell phones allow easy access to an entire digital archive of one's life.[219]

The Court described at length the privacy implications of cell phone content:

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip

---

expectation of privacy so that the law can adapt to new technologies); Stephen E. Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431, 433 (2013) (noting a positive trend toward doing away with a strict third party doctrine).

214. 134 S. Ct. 2473 (2014).

215. *Id.* at 2493.

216. *Id.* at 2486–89.

217. *Id.* at 2488–89.

218. *See id.* at 2489.

219. *See id.* at 2489–90; *see also* Charles E. MacLean, *But Your Honor, a Cell Phone is not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L. Rev. 37, 57 (2012) ("Cell phones are more like extensive computers than wallets.").

> of paper reminding him to call Mr. Jones; he would not carry a record of all of his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[220]

Thus, the Court acknowledged the unique and comprehensive data compilation contained in a modern cell phone. Citing Justice Sotomayor's concurrence in *United States v. Jones*,[221] the Court also noted how cell phone content can even reveal historic location information that can convey a minute-by-minute account of one's specific movements.[222] Taken as a whole, the content on one's cell phone rivals the level of intimate details stored in one's house, and a cell phone can hold the key to cloud-based data as well.[223] Access to this amount of information burdens privacy rights.

In sum, the Court recognized a privacy concern unique to new technology like cell phones: some Fourth Amendment protection is needed for the archive of personal details—from mundane to intimate—of one's life contained in an easily accessible digital format.[224] The challenge of new technology cannot be addressed by merely analogizing to physical records; rather, a rule is needed to address the privacy concerns surrounding cell phones in particular.[225] The Court also noted that a standard based on the reasonable belief that a cell phone will contain relevant evidence is unworkable, given the sheer volume of data contained on a cell phone.[226] In essence, police could always find some sort of potential evidence, so such a standard "would in effect give 'police officers unbridled discretion to rummage at will among a person's private effects.'"[227] Ultimately, the Court treated digital searches as unique and established a warrant requirement for law enforcement accessing cell phone content—even incidental to arrest.[228]

Although *Riley* recognized the unique privacy implications of warrantless searches of cell phone content, traditional Fourth Amendment principles provide little protection of digital data compiled through electronic means over time. While statutory law provides

---

220. *Id.* at 2489.
221. 132 S. Ct. 945 (2012).
222. *See Riley*, 134 S. Ct. at 2490.
223. *Id.* at 2491.
224. *Id.* at 2490.
225. *Id.* at 2493.
226. *Id.* at 2492.
227. *Id.* at 2492 (citing Arizona v. Gant, 556 U.S. 332, 345 (2009)).
228. *Id.* at 2493.

narrow slivers of restrictions on its use and collection,[229] electronic compilations of public information are given little privacy protection because of the third-party disclosure rule or the reasonable expectation of privacy. Yet scholars have urged—and courts have begun to recognize—that traditional notions of privacy may be inadequate to address current and emerging technologies.

3. The Mosaic Theory of Privacy

The "mosaic theory" is an emerging concept in Fourth Amendment law that redraws the lines between public and private. The mosaic theory stands for the proposition that traditionally public information, when collected over time and viewed in the aggregate, should be afforded some privacy protection because of the detailed mosaic of one's life these bits of information paint.[230] In other words, new technology allows us to capture so many individual details of public life that, when viewed as a whole, invade one's privacy.

To date, courts applying the Fourth Amendment have not fully embraced mosaic theory, but several opinions indicate the potential viability of a mosaic approach to privacy. In *United States v. Maynard*,[231] the D.C. Circuit considered GPS monitoring that tracked a suspected drug dealer's public movements for 28 days and compiled over 2,000 pages of data. There, the court noted that these movements, even though public, would never be observed by a stranger in their entirety.[232] Instead, the degree of monitoring and scope of information collected was only possible by technological means.[233] Further, the unique, thorough compilation of electronic data collected revealed "habits and patterns that mark the distinction between a day in the life and a way of life."[234]

The *Maynard* case was appealed to the Supreme Court as *United*

229. *See, e.g.*, Wireless Communications and Public Safety Act, 47 U.S.C. § 222 (2012) (safeguarding access to cell phone location information).

230. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012). The government used a mosaic theory argument to block Freedom of Information Act requests to computerized summaries, such as FBI "rap sheets." *See, e.g.*, United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 780 (1989). Now, that same notion of privacy in large compilations of public data is being used to prevent the government from collecting this information in the first place. *See infra* notes 234–36 and accompanying text.

231. 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

232. *Id.* at 560.

233. *Id.* at 562.

234. *Id.* at 558; *see also* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009); United States v. Graham, 796 F.3d 332, 344–47 (4th Cir. 2015).

States v. Jones.[235] There, Justice Sotomayor seemed to accept a mosaic theory approach to privacy in her concurrence.[236] In particular, Justice Sotomayor's concurrence recognized that electronic compilations of non-private data, as a whole, deserve some sort of protection given the sheer scope of information they convey about the person.[237]

The *Jones* majority opinion focused on whether the placement of the device was a search and held that an unconstitutional search occurred when the device was placed on the car that was parked in a private driveway.[238] Notably, the majority avoided the issue of whether placing the device without the trespass would be constitutional. The Court noted that, although visual surveillance and tailing over a four-week period may be constitutional, "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[239]

But Justice Sotomayor's concurrence expanded on this question and noted that evolving technological advancement may also alter societal expectations of privacy.[240] Thus, even if no trespass or other physical intrusion had occurred, use of the GPS tracking device may still amount to a constitutional violation.[241] Sotomayor observed that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about . . . familial, political, professional, religious, and sexual associations."[242] Compiling this comprehensive personal data—though not "private" data—may constitute an invasion of privacy when viewed in the aggregate.[243] Indeed, gaining access into this "quantum of intimate information about any person" crosses the boundaries of what may be reasonable.[244] Thus, Sotomayor called into question the lack of reasonable expectations of privacy to aggregated public data, noting that she would "ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more

235. 132 S. Ct. 945 (2012).
236. *Id.* at 954–57 (Sotomayor, J., concurring).
237. *Id.*
238. *Id.* at 950–53 (majority opinion).
239. *Id.* at 954.
240. *See id.* at 954–55 (Sotomayor, J., concurring).
241. *Id.* at 955.
242. *Id.*
243. *Id.* at 955–56; *see also* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009); United States v. Graham, 796 F.3d 332, 344–47 (4th Cir. 2015).
244. *Jones*, 132 S. Ct. at 956.

or less at will, their political and religious beliefs, sexual habits, and so on."[245]

Sotomayor also took into consideration the fact that this aggregate of data may be voluntarily communicated to third parties and called for a rethinking of the third-party disclosure rule: "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[246]

The mosaic theory may be difficult to apply in the Fourth Amendment context. For example, Professor Orin Kerr has identified serious limitations and challenges of applying the mosaic theory to Fourth Amendment search and seizure requirements.[247] In particular, Fourth Amendment law has always hinged on viewing each step individually—sequentially and scene-by-scene—to determine if a search occurred as to a particular act.[248] In contrast, mosaic theory looks at the entirety of numerous individual acts retrospectively to determine if the surveillance as a whole constitutes a search.[249] The departure from the scene-by-scene analysis requires a post hoc reexamination of activity that, individually, may have passed constitutional muster. Further, no standard of reasonableness exists as to mosaic searches, no remedies have been defined, and no guidance exists as to permissible durations and scales of mosaic searches. Thus, the practical implication is that law enforcement is given little guidance as to when lawful activity morphs into an unconstitutional "mosaic" search and may struggle in applying this new, unprecedented mosaic approach.[250]

Despite these criticisms, mosaic theory can be a tool when looking at whether an existing digital data compilation should be handed over in civil discovery. At the very least, this theory, by analogy, can support a more limited production and disaggregation of data, in an effort to

---

245. *Id.*; *see also* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring)).

246. *Jones*, 132 S. Ct. at 957; *Weaver*, 909 N.E.2d at 1199; *Graham*, 796 F.3d at 344–47; *but see In re* United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc).

247. Kerr, *The Mosaic Theory*, *supra* note 230, at 346–50.

248. *Id.* at 315–17 (Kerr refers to this as "sequential" approach).

249. *Id.* at 313.

250. *Id.* at 344. Although Professor Kerr argues against a mosaic theory approach to the Fourth Amendment, he nonetheless notes that traditional privacy doctrines have been outpaced by new technology: "[c]hanging technology can outpace the assumptions of existing precedents, and courts may need to tweak prior doctrine to restore the balance of privacy protection from an earlier age." *Id.* (noting that longstanding methods of interpreting the Fourth Amendment already include "equilibrium-adjustment" in the wake of shifting societal needs).

mitigate some of these privacy concerns.

B. Privacy's Role in Civil Discovery

The constitutional and statutory principles that provide a framework of privacy law in the U.S. do not expressly limit civil discovery under the Federal Rules of Civil Procedure. Indeed, the Fourth Amendment protects against *government* intrusion into private spaces, and civil discovery among private parties is not limited by the Fourth Amendment *per se*.[251] Nonetheless, some scholars maintain that the Fourth Amendment should be an express limit or (at the very least) guiding principle for court-ordered discovery in civil cases.[252] Several courts already look to broader constitutional principles when exercising their discretion in civil matters, noting that discovery, if proper, also comports with constitutional protections.[253] Most notably, privacy-based arguments are being made in a variety of civil cases, and courts analogize to Fourth Amendment or other privacy concepts when resolving discovery disputes.[254] Thus, general privacy law principles are important for crafting meaningful boundaries in the civil discovery context. Several parallels can be drawn between the principles underlying the Federal Rules of Civil Procedure and privacy law and, by recognizing the intersection of these two areas of law, courts can revive or expand important privacy-based limits on civil discovery.

1. Established Categories of Privacy Protection in Civil Discovery

Overly broad civil discovery violates certain implied rights of the party or witness that draw on broader privacy concepts, such as the right to be free from harassment and embarrassment.[255] But as a general

---

251. *See, e.g.*, Doe v. Senechal, 725 N.E.2d 225, 231 (Mass. 2000) (noting that Fourth Amendment does not apply to civil litigation among private parties); Jeana K. Reinbold, *Reconciling a Debtor's Right to Privacy with a Chapter 7 Trustee's Duties*, 33-OCT AM. BANKR. INST. J. 18, 18 (Oct. 2014) (noting that the Fourth Amendment may apply to trustees, who function as private parties acting as agents for the government).

252. Chad DeVeaux, *A Tale of Two Searches: Intrusive Civil Discovery Rules Violate the Fourth Amendment*, 46 CONN. L. REV. 1083, 1104 (2014) (proposing that Fourth Amendment applies to court-ordered civil discovery); *see also* Jordana Cooper, *Beyond Judicial Discretion: Toward a Rights-Based Theory of Civil Discovery and Protective Orders*, 36 RUTGERS L.J. 775, 776 (2005).

253. *See, e.g.*, Ambassador Coll. v. Goetzke, 260 S.E.2d 27, 29–30 (Ga. 1979) (Hill, J., concurring); Grober v. Dep't of Revenue, 956 P.2d 1230, 1234 n.8 (Alaska 1998); Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 350 (2000).

254. *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 654 (N.Y. Sup. Ct. 2010).

255. *See* FED. R. CIV. P. 26(c).

matter, the discovery rules permit broad discovery with little differentiation between public and private content. As noted by the Supreme Court in *Seattle Times v. Rhinehart*,[256]

> [t]he rules do not differentiate between information that is private or intimate and that to which no privacy interests attach. Under the Rules, the only express limitations are that the information sought is not privileged, and is relevant to the subject matter of the pending action. Thus, the Rules often allow extensive intrusion into the affairs of both litigants and third parties.[257]

Nonetheless, some privacy-protection tools already exist within the rules, and the rules as a whole contemplate broad discretion by courts.

Although litigants may seek out all relevant information,[258] discovery requests cannot create undue burden, embarrassment, or harassment.[259] Courts do not allow fishing expeditions that demand broad and unfettered access to data and documents without regard to its relevance.[260] Discovery should be used to find details, not to cast a wide net to fish for potential claims.[261] As a result, discovery requests must be specific and stated with reasonable particularity, and the need for discovery must be balanced against the burden or embarrassment that producing it creates.[262] These limits—particularly those based on notions of harassment, embarrassment, and burden—imply a privacy-related right that should not be infringed upon through overly broad discovery.

Therefore, courts have the power and discretion to limit the scope of discovery itself. Even though relevant information is generally discoverable, courts can disallow discovery of even relevant information when countervailing concerns warrant such a limit. Thus, information that is otherwise relevant may still be excluded altogether from discovery, thereby protecting broader categories of data from any

256. 467 U.S. 20 (1984).

257. *Id.* at 30.

258. *See id.*

259. *See* FED. R. CIV. P. 26(c); FED. R. CIV. P. 26(g)(1)(B); FED. R. CIV. P. 26 advisory committee's notes (1970 Amendments).

260. *See, e.g.*, Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007) (dismissing a complaint to protect antitrust defendants from potentially burdensome pretrial discovery). Although the court's majority opinion did not identify the complaint as such, Justice Stevens wrote that the majority regarded plaintiff's complaint as a "fishing expedition." *Id.* at 577 (Stevens, J., dissenting).

261. *Id.* at 560 n.6 ("Discovery is used to find the details.").

262. The standard for protective orders states that the court "may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." FED. R. CIV. P. 26(c). Further, Rule 34 states that a discovery request "must describe with reasonable particularity each item or category of items to be inspected." FED. R. CIV. P. 34(b)(1)(A).

disclosure at all.[263]

In addition to the court's discretion to define the scope of discovery, the Federal Rules have also been limited by express privacy protection, such as through the work product doctrine and the attorney-client privilege.[264] Narrow categories of information, like tax returns[265] and trade secrets,[266] have also been shielded from discovery on privacy grounds.

Once private information is deemed to be within the scope of discovery, courts have multiple options to help protect privacy or confidentiality, including *in camera* review, the sealing of documents, and redaction of personal information.[267] Protective orders are an important mechanism for protecting privacy.[268] Rule 26(c) expressly permits courts to use protective orders in the discovery process, both as "'blanket' protective orders" covering a broad swath of information in the litigation or narrow protective orders as to particular materials.[269] Although open disclosure of court records is an important consideration, that access must be balanced against individual privacy interests.[270] Protective orders thus "recognize that parties engaged in litigation do not sacrifice all aspects of privacy or their proprietary information simply because of a lawsuit"[271] and provide a modicum of privacy protection. Nonetheless, alleging privacy interests, without more, will not suffice to establish good cause for obtaining a protective order.[272]

Privacy-based limits are already built into the existing civil discovery process, and the renewed emphasis on proportionality further highlights the courts' ability to limit discovery. Throughout the history of the

263. Crawford–El v. Britton, 523 U.S. 574, 598 (1998).

264. Hickman v. Taylor, 329 U.S. 495, 499 (1947); *see also* Bahadur, *supra* note 112 (describing these as part of a realm of information privacy that is protected under the Federal Rules of Civil Procedure, which attempt to achieve equilibrium between truth and privacy, but he argues ESI discovery has eliminated the practical restrictions privacy-based limits created in discovery and, instead, access to justice and fairness will be increased if all privacy limits are done away with, including privilege).

265. *See, e.g.*, Wiesenberger v. W. E. Hutton & Co., 35 F.R.D. 556, 557 (S.D.N.Y. 1964).

266. *See, e.g.*, Julius M. Ames Co. v. Bostitch, Inc., 235 F. Supp. 856, 857 (S.D.N.Y. 1964).

267. *See* Guerra v. Bd. of Trs. of Cal. State Univs. & Colls., 567 F.2d 352, 355 (9th Cir. 1977) (confidentiality of university personnel records); *see also* CHARLES ALAN WRIGHT ET AL., 8A FEDERAL PRACTICE AND PROCEDURE § 2043 (3d ed. 2015).

268. *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 31 (1984).

269. *See* United Nuclear Corp. v. Cranford Ins. Co., 905 F.2d 1424, 1427 (10th Cir. 1990).

270. *In re* Mirapex Prods. Liab. Litig., 246 F.R.D. 668, 673 (D. Minn. 2007).

271. *Id.*

272. *See, e.g.*, Koster v. Chase Manhattan Bank, 93 F.R.D. 471, 481 n.18 (S.D.N.Y. 1982) (good cause not established when defendant bank made conclusory assertion that its employees would be harmed without a protective order).

Federal Rules of Civil Procedure, an implicit tension between open access to information and privacy existed. This tension continues to exist today as courts grapple with large swaths of data that, in the aggregate, reveal unprecedented amounts of personal information about people. Evolving notions of privacy, particular as to aggregated digital data compilations, may help courts fashion fair limits on overly intrusive discovery. To date, however, few cases rely on privacy-based considerations as a factor in determining the scope of civil discovery of digital data compilations.

2. Social Media Discovery

Social media accounts are a primary example of cases where litigants rely on privacy-based arguments to combat overly broad discovery. But courts have taken inconsistent and at times unfair approaches to discovery of social media content, giving little credence to privacy-based limits to discovery.

Although social media data is a form of ESI, the 2006 amendments addressing ESI discovery predate the social media boom. In the same year the 2006 amendments were made, Twitter was founded; Facebook first expanded beyond college campuses; and MySpace was the industry leader (though MySpace was only three years old at the time). Needless to say, social media's popularity, functionality, and ubiquity has grown in unprecedented ways since 2006, and it is safe to assume that the ESI discovery amendments did not specifically consider social media and its unique ability to compile detailed personal information. Courts seem to struggle with finding a fair, consistent approach to social media discovery and wholly reject most privacy concerns. The result is broad social media discovery in many cases.

a. Different Approaches to Social Media Discovery Generally

A social media account, like Facebook, contains highly detailed personal information, archived and aggregated over time. Generally, courts take three predominant approaches to social media discovery: (1) a "factual predicate" approach that looks to what the public account content shows before granting access to privacy-protected contents; (2) a presumption of complete discovery with few limits; or (3) a "reasonable particularity" approach that tries to narrow discovery to specific claims and issues in the litigation.

First, under a "factual predicate" approach, courts require the party seeking discovery to show a factual predicate based on publicly available

social media data before allowing access to any private content.[273] In other words, courts will deny access to any social media content without the party seeking discovery showing a publicly available post that establishes a factual predicate.

For example, in *Romano v. Steelcase Inc.* the court allowed broad discovery of the plaintiff's Facebook page after she alleged that she suffered debilitating neck and back injuries and loss of enjoyment in life from an injury caused by defendant's faulty chair.[274] The plaintiff had a profile photo on Facebook in which she was smiling on vacation in Florida that was visible to the public—including to opposing counsel.[275] The photo clearly contradicted her claim that she could not leave the house and engage in any physical activity, and defense counsel used it as factual predicate to support discovery of the private portions of the Facebook page.[276] Specifically, defendants requested "authorizations to obtain full access to and copies of Plaintiff's current and historical records/information on her Facebook and MySpace accounts."[277] The court allowed the defendant's complete request and permitted discovery of current and prior (even deleted) items on the private portions of the plaintiff's Facebook and MySpace pages under state rules that parallel the Federal Rules.[278] The court reasoned that the plaintiff's claim placed her physical condition, as well as her enjoyment of life, at issue in the litigation, therefore broad social media discovery was warranted.[279] No limits based on the relevance of particular posts or as to date ranges were included in the court's order.[280]

In contrast, another court in a similar case disallowed all social media discovery under the factual predicate approach.[281] In *Tompkins v. Detroit Metropolitan Airport*, the plaintiff alleged physical injuries from a slip-and-fall accident at the Detroit airport, claiming loss of enjoyment

---

273. Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 653–54 (N.Y. Sup. Ct. 2010).

274. *Id.* at 653.

275. *Id.* at 654.

276. *Id.* at 653–54.

277. *Id.* at 653.

278. *Id.* at 657.

279. *Id.*; *see also* Keller v. Nat'l Farmers Union Prop. & Cas. Co., No. CV 12-72-M-DLC-JCL, 2013 WL 27731, at *4 (D. Mont. Jan. 2, 2013) (adopting a factual predicate approach similar to that in *Romano*); Palma v. Metro PCS Wireless, Inc., 18 F. Supp. 3d 1346, 1348 (M.D. Fla. 2014) (no factual predicate shown in Fair Labor Standards Act case, where plaintiff's physical condition not at issue); Doe v. Rutherford Cty., Tenn., Bd. of Educ., No. 3:13-0328, 2014 WL 4080159, at *3 (M.D. Tenn. Aug. 18, 2014) (Plaintiff's public Twitter post sufficient for an evidentiary threshold justifying broad discovery of Plaintiff's private social media posts on multiple sites).

280. *See Romano*, 907 N.Y.S.2d at 657.

281. Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 388–89 (E.D. Mich. 2012).

of life among other injuries.[282] The defendant sought discovery of the private portions of the plaintiff's Facebook page, relying on plaintiff's public postings that showed her standing with friends at a birthday party while holding a small dog.[283] The court rejected the discovery requests under the *Romano* approach.[284] Specifically, the court noted that plaintiff never claimed to be unable to engage in all physical activity, and standing at a party and holding a small dog (which the court opined must weigh less than five pounds) did not undermine plaintiff's injury claims.[285] The court even noted that, while public photos of the plaintiff golfing or horseback riding might have created a factual predicate, the less rigorous activities depicted in the actual photos did not.[286] Thus, the court denied defendants' request for discovery of the private Facebook content.[287]

This factual predicate approach places too great an emphasis on what the user chose to leave public. It ignores the fact that, even without publically visible content, the privacy-setting protected material may still be highly relevant.[288] On the other hand, the factual predicate approach also may lead to overly broad access to private content once the factual predicate has been established. In some cases, courts have granted "complete and unfettered access" to the entire account without establishing any parameters on what must be produced.[289] Thus, a single public photo may throw open the doors to an entire Facebook account, for example. As a whole, the factual predicate approach results in inconsistent or unfair results.[290]

Second, some courts seem to employ a presumption of complete discovery of all social media contents and create few, if any, limits on what must be produced. In some instances, courts even order litigants to produce or exchange their login and password information, thus granting broad and unrestricted access to everything in the social media

282. *Id.* at 387.

283. *Id.* at 388–89. The defendant also relied on a surveillance video of the plaintiff pushing a shopping cart. *Id.* at 389.

284. *Id.*

285. *Id.* at 388–89.

286. *Id.* at 389.

287. *Id.* at 387.

288. *See id.*; *see also* 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, 887–88 (2013) (criticizing different approaches courts take to social media discovery).

289. McPeak, *supra* note 288, at 928.

290. *Id.* at 887–88.

account.[291] Password exchanges are particularly disturbing because they can impact third-party rights, such as allowing the opposing counsel to see the "friend-only" content for the account holder's contacts or receiving real-time, irrelevant content in a live stream.[292]

Courts taking this complete-access approach seem to make no attempts to define the scope of relevant data in social media accounts. For example, in *Gallion v. Gallion*, a family law case,[293] the court ordered counsel to exchange their clients' passwords for Facebook and dating websites, apparently because the husband suspected that his wife made comments relevant to her feelings for their children and to infidelity on the social media sites.[294] Again, the court created no limits on what data within the accounts was discoverable.[295]

Similarly, in *McMillen v. Hummingbird Speedway, Inc.*,[296] the court ordered the plaintiff, a racecar driver, to hand over his MySpace and Facebook passwords to defense counsel in his personal injury suit after only a minimal relevance showing.[297] In that case, defendants were granted broad discovery of the social media accounts because the public portions of the account showed the plaintiff fishing and attending a Daytona 500 race.[298] The court did not address whether these activities directly contradict plaintiff's injury claims but noted that the plaintiff may have posted other information about travel or activity that could undermine his case.[299]

These cases illustrate how, under this second, complete-access approach, courts allow unfettered review of all of the social media

---

291. *Id.* at 887.

292. For example, Facebook's policies prohibit disclosing one's password to anyone else. *See Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last visited Sept. 8, 2015); *see also* Brian Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps In Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 17 (noting how cell-site location information implicates third-party privacy rights).

293. No. FA114116955S, 2011 WL 4953451 (Conn. Super. Ct. Sept. 30, 2011).

294. *Id.* at *1; *see also* Kashmir Hill, *Judge Orders Divorcing Couple to Swap Facebook and Dating Site Passwords*, FORBES (Nov. 7, 2011, 9:42 AM), http://www.forbes.com/sites/kashmirhill/2011/11/07/judge-orders-divorcing-couple-to-swap-facebook-and-dating-site-passwords/.

295. *Gallion*, 2011 WL 4953451, at *1 (modifying its order to clarify that only counsel and not the parties themselves may receive the other's password, and neither party may post messages pretending to be the other).

296. No. 113–2010 CD, 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010) (granting motion to compel under state rules that mirror the Federal Rules).

297. *Id.* at *4; *see also* Largent v. Reed, No. 2009-1823, 2011 WL 5632688, at *7 (Pa. Ct. Com. Pl. Nov. 8, 2011).

298. *McMillen*, 2010 WL 4403285, at *4.

299. *Id.* at *3–4.

account contents after little or no relevance showing. This approach likely encompasses data that is not only irrelevant but otherwise wholly unrelated to the claims and issues in the litigation.[300] Forced password disclosures also impact third-party rights and provide overly intrusive aspects to all facets of a live social media account.

Third, under a "reasonable particularity" approach, courts attempt to define the scope of discovery based on the specificity of the discovery request and the potential relevance of the information sought.[301] This approach tries to create more meaningful limits based on the reasonable particularity of the request, but courts still struggle with drawing meaningful boundaries.[302] Nonetheless, under this approach, courts tend to recognize that relevance should be the threshold inquiry, even as to social media discovery.[303]

Some courts using the reasonable particularity approach make more of an effort to define what is relevant in a social media account. For example, in *EEOC v. Simply Storage Management*[304] the court held that data marked *private* on social media websites is nonetheless discoverable if it may be relevant to a claim or defense.[305] That case involved an employment discrimination suit in which plaintiffs claimed they were victims of sexual harassment and sex discrimination.[306] The defendants sought broad discovery of plaintiffs' social media pages, including all photographs or videos and copies of complete profiles, and certain third-party app information.[307] The court noted that the Federal Rules support broad discovery and encompass all relevant data, regardless of the form

---

300. Scholars have criticized the broad and unfettered access courts give litigants to social media accounts. *See, e.g.*, Bruce E. Boyden, *Oversharing: Facebook Discovery and the Unbearable Sameness of Internet Law*, 65 ARK. L. REV. 39, 58–59 (2012) (asserting that such broad access is inconsistent with the rules of civil procedure and invades privacy without sufficient cause); Aviva Orenstein, *Friends, Gangbangers, Custody Disputants, Lend Me Your Passwords*, 31 MISS. C. L. REV. 185, 223–24 (2012) (recommending a rebuttable presumption regarding the authenticity of social media accounts when litigants are asked to hand over passwords).

301. *See, e.g.*, EEOC v. Simply Storage Mgmt., 270 F.R.D. 430, 434–35 (S.D. Ind. 2010).

302. *Id.* at 434.

303. *Id.*

304. *Id.* at 430.

305. *Id.* at 434.

306. *Id.* at 432.

307. *Id.* (explaining that defendants specifically sought "[a]ll photographs or videos posted by [plaintiffs] or anyone on [their] behalf on Facebook or MySpace from April 23, 2007 to present" as well as copies of plaintiffs' "complete profile on Facebook and MySpace (including all updates, changes, or modifications to [the] profile[s]) and all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, details, blurbs, comments, and applications (including, but not limited to, 'How well do you know me' and the 'Naughty Application') for the period from April 23, 2007 to the present").

that data takes.[308] The court also recognized that discovery is subject to some limits and cannot be unreasonably cumulative, duplicative, burdensome, or expensive.[309] It noted that these limits must be balanced against "the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues."[310]

With this general framework in mind, the court in *Simply Storage* applied the basic principles of discovery to social media content.[311] It clarified that "the simple fact that a claimant has *had* social communications is not necessarily probative of the particular mental and emotional health matters at issue in the case."[312] Instead, only limited social media content can be sought, even though severe emotional distress is alleged.[313] The court analogized "private" social media content to email and noted that only those communications that are relevant should be produced.[314] But ultimately, the court articulated the scope of relevant discovery in very broad terms:

> [A]ny profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and [social networking site] applications for [plaintiffs] for the period from [date of incident], through the present 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.[315]

Thus, although the *Simply Storage* court refused to allow disclosure of an entire social media account, it also drew a wide net of what content is discoverable under the relevance standard.[316] The resulting order

---

308. *Id.* at 433 (citing FED. R. CIV. P. 26).

309. *Id.* (citing FED. R. CIV. P. 26(b)(2)(C)(i)).

310. *Id.* (quoting FED. R. CIV. P. 26(b)(2)(C)(iii)).

311. *Id.* at 434.

312. *Id.* at 435.

313. *Id.* at 435–36 (explaining that "[a]llegations of depression, stress disorders, and like injuries do not automatically render all SNS communications relevant").

314. *Id.* at 435.

315. *Id.* at 436.

316. *Id.* at 434–36 (stating that social networking site content is not shielded from discovery just because it is "locked" or "private" and that such content must be produced when it is relevant to a claim or defense in the case); *see also* Caputi v. Topper Realty Corp., No. 14-CV-2634, 2015 WL 893663, at *8 (E.D.N.Y. Feb. 25, 2015) ("the Court . . . declines to give Defendants complete access to Plaintiff's Facebook account for the purpose of identifying photographs, postings or private messages that may appear inconsistent with someone experiencing emotional distress. Rather, Defendants are entitled to a sampling of Plaintiff's Facebook activity for the period November 2011 to November 2013, limited to any 'specific references to the emotional distress [Plaintiff] claims she

remains very broad, and the court noted that it cannot draw boundaries in the level of specificity that the litigants would desire.[317] Indeed, because social media contains so much personal information, broad discovery requests for social media account data often touch upon issues in the litigation—from piecing together facts to impeachment evidence and proof of damages.

Because discovery requests for social media content often meet a basic standard of relevance,[318] the court in *Simply Storage* attempted to create a more meaningful, narrow scope of discovery.[319] Specifically, the court limited its holding to cases involving more than "garden variety emotional distress claims,"[320] as the analysis hinged instead on allegations of "severe emotional distress, including post-traumatic stress disorder."[321] Despite the court's attempt to limit broad discovery to cases of severe emotional distress, other cases involving "garden variety emotional distress claims" still take as broad an approach as *Simply Storage*.[322]

Taken as a whole, the cases addressing social media discovery take an inconsistent and often times broad approach that often results in complete access to a social media account. Some courts make little effort to create meaningful boundaries and instead allow, without adequate justification, whole-cloth discovery in many cases.

b. Privacy Arguments in Social Media Discovery Cases

Regardless of which approach courts take to social media discovery, the cases often reject privacy-based arguments as a limit to social media discovery. Instead, courts emphasize that social media accounts cannot

---

suffered' in the Complaint, and any 'treatment she received in connection [there]with.'").

317. *Id.* at 436.

318. FED. R. CIV. P. 26(b)(1). The 2015 amendments will modify this rule to define the scope of discovery as information "relevant to any party's claim or defense and [is] proportional to the needs of the case." FED. R. CIV. P. 26(b)(1) (2015 Prospective Amendments). Nonetheless, even under the revised rule, social media content will often meet the relevance standard.

319. *Simply Storage Mgmt.*, 270 F.R.D. at 434.

320. *Id.* at 437.

321. *Id.*

322. *See, e.g.*, Mailhoit v. Home Depot U.S.A., Inc., 285 F.R.D. 566, 571–73 (C.D. Cal. 2012) (severe emotional distress claim warranted broad social media discovery but included a limit based on a relevant time period); Robinson v. Jones Lang LaSalle Ams., Inc., No. 3:12-cv-00127-PK, 2012 WL 3763545, at *1–2 (D. Or. Aug. 29, 2012) (social media discovery limited to content that reflects "work-related emotions"); Reid v. Ingerman Smith LLP, No. CV 2012–0307 (ILG) (MDG), 2012 WL 6720752, at *2–3 (E.D.N.Y. Dec. 27, 2012) (allowing discovery as broad as that in *Simply Storage* but apparently without allegations of severe emotional distress).

be protected as "private" by the very nature of this new medium.[323] Further, the privacy controls on social media websites are complicated, unreliable, and ever-changing, making it difficult to create meaningful and trustworthy limits based on these unique features of social media accounts.[324]

Many privacy-based arguments usually fail in social media discovery cases. First, some litigants have argued for a "social network site privilege" or exception, which understandably has been flatly rejected by courts.[325] It is clear that no "social network site privilege" should exist, and several courts expressly hold that social media cannot be subject to any sort of privilege as an exception to discoverability.[326] In *McMillen*, a Pennsylvania court rejected arguments that some form of "social network site privilege" should be created to protect confidential and private messages sent through Facebook.[327] According to the *McMillen* court, social networking websites may be used by some people to convey confidential and personal information to another user, but any expectation to privacy in such communications is unreasonable due to the very nature and purpose of these websites.[328] Further, the user who receives a communication via a social media account can easily disseminate it to others, which also deteriorates the private nature of the communication.[329] The *McMillen* court quoted Facebook's own privacy policy to emphasize further the lack of privacy protections guaranteed by the site[330] and noted that, if users want to keep communications private, they should have chosen another form of communication.[331] But like many other decisions, the *McMillen* court failed to make any distinction between Friends-only posts and direct one-on-one communications via

323. Social media websites exist to share, and sites like Facebook make clear in their terms that they are designed to facilitate connections and sharing with others. *See About Facebook*, *supra* note 205.

324. *See Facebook's Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (stating the Facebook user "will not share your password (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account"); *see* McPeak, *supra* note 288.

325. *See, e.g.*, McMillen v. Hummingbird Speedway, Inc., No. 113–2010 CD, 2010 WL 4403285, at *4 (Pa. Ct. Com. Pl. Sept. 9, 2010); Trail v. Lesko, No. GD-10-017249, 2012 WL 2864004 (Pa. Ct. Com. Pl. July 3, 2012).

326. *See McMillen*, 2010 WL 4403285 at *4.

327. *Id.* at *3.

328. *Id.* at *2.

329. *Id.*

330. *Id.* at *2–3.

331. *Id.* at *3–4 ("[N]o person choosing MySpace or Facebook as a communications forum could reasonably expect that his communications would remain confidential, as both sites clearly express the possibility of disclosure.").

the messaging or chat features, nor did it consider the full scope of data available via a social media account. Ultimately, the court ordered the plaintiff to provide his user name and password to his Facebook and MySpace accounts.[332]

Other privacy-based concerns have also been rejected by courts. In *Romano*, for example, the plaintiff argued that private social media data should be afforded some protection from discovery.[333] The court expressly looked to Fourth Amendment jurisprudence, noting that an email or other writing is not private once shared with another person.[334] Thus, the expectation of privacy is not reasonable once information is transmitted to others.[335] The *Romano* court noted that social media websites exist to facilitate sharing, and a plaintiff cannot be allowed to hide behind self-selected privacy settings to shield otherwise discoverable information from the defendant.[336]

In general, courts lump all social media together and rely heavily on the simple definition of social media as a tool for sharing and not secrecy.[337] However, in *Trail v. Lesko*, the court acknowledged that granting a party broad access to the private portion of a social media account is intrusive and can result in access to a great deal of personal information that is unrelated to the litigation.[338] Further, the court noted that a state rule of procedure prevented discovery that may be embarrassing, such as social media content.[339] Nonetheless, the court reasoned that the intrusiveness that results is minimal, given that the account-holder already chose to share social media information voluntarily with numerous Friends.[340] Thus, the court held that when discovery is likely to yield relevant information that is not available

---

332. *Id.* at *4; *see also* Trail v. Lesko, No. GD-10-017249, 2012 WL 2864004 (Pa. Ct. Com. Pl. July 3, 2012) (rejecting social media privilege argument because no "constitutional right to privacy or any common law or statutory privileges" apply).

333. Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 651–52 (N.Y. Sup. Ct. 2010).

334. *Id.* at 655–56.

335. *Id.* at 656 ("Users would logically lack a legitimate expectation of privacy in materials intended for . . . public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient . . . the e-mailer would be analogous to a letter-writer whose expectation of privacy ordinarily terminates upon delivery . . . ." (quoting United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004))).

336. *Id.* at 655.

337. *See id.* at 653–54.

338. Trail v. Lesko, No. GD-10-017249, 2012 WL 2864004, at *28–29 (Pa. Ct. Com. Pl. July 3, 2012).

339. *Id.*

340. *Id.* at 29 ("[O]n a scale of 1 (the lowest) to 10 (the greatest), the intrusion from most *Facebook* discovery is probably at a level of 2.").

elsewhere, the intrusion posed is not unreasonable.[341]

Other cases give some consideration to privacy-based concerns. In *Appler v. Mead Johnson & Co., LLC*, the plaintiff in an employment case requested the complete download file from Facebook for two of defendants' employees. The court noted that the broad request for the entire download file, which includes content not available to the public, implicates privacy interests.[342] Thus, the court acknowledged that even private social media content is discoverable, but limited discovery to content that is relevant to plaintiff's mental and emotional states, which are factual issues in the litigation.[343] Notably, the court balanced the relevancy of the requested discovery against the privacy burden, and concluded that limited social media discovery of defendants' employees' Facebook pages is permissible.[344]

These cases, for the most part, give little consideration to the fact that privacy settings create some distinction between public and private content, which may affect how users perceive their intended audiences.[345] But under many cases addressing social media civil discovery issues, the user's desired level of sharing means very little, and broad discovery of social media data appears to be common. The current case law on social media discovery does not adapt privacy considerations to the changing nature of our online activity.[346]

3. Smartphone Discovery

Smartphones and similar computing devices serve a dual personal and professional purpose for many users, especially in light of the rise of BYOD policies at workplaces. The result is that personal and professional content is comingled on one personally-owned device. The effect of this commingling may be profound: employers must determine how they control and back up professional data on personal devices in

341. *Id.*

342. Appler v. Mead Johnson & Co., LLC, No. 3:14-CV-166-RLY-WGH, 2015 WL 5615038, at *4 (S.D. Ind. Sept. 24, 2015).

343. *Id.*

344. *Id.*; *see also* Nucci v. Target Corp., 162 So. 3d 146, 153 (Fla. Dist. Ct. App. 2015) (allowing broad discovery of Plaintiff's Facebook photographs because she "has but a limited privacy interest, if any, in pictures posted on her social networking sites.").

345. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012).

346. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); *see also* Solove, *supra* note 162; Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12 (2011) (comparative examination of different privacy schemes in relation to social media).

order to collect and preserve content for litigation purposes.[347] Additionally, discovery of content on these devices may encompass irrelevant, highly personal information of both litigants and employees who are not parties to the litigation.

As a starting point, content contained on personal devices generally is not beyond the scope of discovery in a business dispute. Rather, employers may be under a duty to preserve and produce relevant information that exists on employees' personal devices when used for a work-related purpose. In *Passlogix, Inc. v. 2FA Technologies, LLC*[348] the defendant was sanctioned for failing to preserve 143 written communications made on an employee's personal device, including emails, text messages, and Skype messages.[349] The court held that the communications were relevant to the breach of contract claim at issue and rejected defendant's argument that it was under no duty to preserve communications that occurred on an employee's personal device.[350] Thus, the employee's personal device contents were not shielded from discovery.[351]

Even though smartphone contents are discoverable, courts give some consideration to confidentiality and privacy concerns. For example, in *Bakhit v. Safety Marking, Inc.*[352] the court looked at a request to image and retrieve data from a cell phone, including phone call and text records in an employment discrimination case.[353] There, the court noted that the scope of discovery includes a right to electronically stored information, but that this right is '"counterbalanced by a responding party's confidentiality or privacy interests.'"[354] Direct access to records of this nature is not granted as a matter of course, and the requesting party must provide adequate justification for the discovery sought.[355] Thus, the court in *Bakhit* rejected the request, even though it sought relevant

347. *See* The Sedona Conference®, Commentary, *The Sedona Conference® Commentary on Information Governance*, 15 SEDONA CONF. J. 125, 129 (Conor R. Crowley et al. eds.) (2014).

348. 708 F. Supp. 2d 378, 416 (S.D.N.Y. 2010).

349. *Id.*

350. *Id.*

351. *See, e.g.*, Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Secs., 685 F. Supp. 2d 456, 486 (S.D.N.Y. 2010) *abrogated on other grounds by* Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135 (2d Cir. 2012) (employer had duty to produce emails and documents on employee personal devices); Koosharem Corp. v. Spec Pers., LLC, No. 6:08-583-HFF-WMC, 2008 WL 4458864, *2 (D.S.C. Sept. 29, 2008) (same).

352. Civ. No. 3:13CV1049 (JCH), 2014 WL 2916490 (D. Conn. June 26, 2014).

353. *Id.* at *1.

354. *Id.* at *2 (quoting Genworth Fin. Wealth Mgmt., Inc. v. McMullan, 267 F.R.D. 443, 446 (D. Conn. 2010)).

355. *Id.*

content: "[a]lthough the information plaintiffs seek may be relevant to their claims, on the current record, the Court finds that the request as framed is overly broad and too intrusive for this stage of discovery."[356] The court further supported its decision by citing to *Riley* and "[t]he implication of the individual defendants' privacy interest in the data stored on their cell phone."[357] As a result, discovery of potentially relevant cell phone content was denied due in part to the privacy concerns such broad discovery raises.

Other courts tackling these novel challenges also seem to recognize the privacy implications of broad personal device discovery. For example, in *Han v. Futurewei Technologies, Inc.*[358] the court considered a motion to compel a broad search of a former employee's personal computing device in her employment discrimination claim.[359] During the initial disclosure phase of the litigation, the employer-defendant's computer forensics firm discovered that the plaintiff copied, removed, and deleted files from a company-issued laptop.[360] As a result, the employer-defendant suspected theft of confidential and proprietary company information through transfer of that content to the plaintiff's personal device.[361]

Even though the employer-defendant in *Han* had not filed a counterclaim yet, it sought broad, expedited discovery of all content on plaintiff's personal computers and devices.[362] As part of the discovery attempt, the employer-defendant suggested a protocol involving a forensic firm imaging and capturing all of plaintiff's personal computer content for search-term review and other analysis.[363] The plaintiff objected to this broad discovery, noting that "her personal computer contains attorney-client privileged communications, attorney work product, and information in which she has a strong privacy interest, including correspondence with friends and family, online banking information, and other private data and passwords."[364] The court found that the requested discovery was not necessary or justified, as the employer-defendant had not established that the plaintiff was acting

356. *Id.*
357. *Id.* at *3.
358. No. 11-CV-831-JM (JMA), 2011 WL 4344301 (S.D. Cal. Sept. 15, 2011).
359. *Id.* at *1.
360. *Id.*
361. *Id.* at *1, *4.
362. *Id.*
363. *Id.* at *1–2.
364. *Id.* at *2.

maliciously or at risk of destroying evidence.[365] Nor could the employer-defendant point to a policy that prohibited the transfer or deletion of company content from work or personal devices.[366] Instead, the court noted that the plaintiff may have been merely "cleaning up" a work laptop when she returned it after transferring or deleting work-related material.[367] Thus, the employer-defendant failed to support its broad discovery attempts as to personal computers that may store work-related data.[368] Additionally, the court expressed concern over the potential access to privileged or private content on the employee's personal computer, noting that broad access to the plaintiff's personal information is unduly burdensome.[369]

As more employers adopt BYOD policies, business disputes will involve broad attempts at discovery of smartphone or other personal device contents. While these devices are not shielded from discovery, the scope of discovery must account for the unique privacy implications that arise because of the comingling of personal and professional data. Further, smartphones and personal devices will continue to expand in functionality and will archive even more highly personal details over time, making broad attempts at civil discovery even more intrusive. Courts will have to weigh privacy concerns when defining discovery's parameters.

V. DEVELOPING PRIVACY-BASED LIMITS TO CIVIL DISCOVERY OF DIGITAL DATA COMPILATIONS

The Federal Rules of Civil Procedure, throughout their evolution, have struggled to balance open access to information with countervailing concerns that are rooted in privacy-based principles. At the same time, privacy law as a whole struggles to adapt to the quickly-evolving technological landscape. As our capacity to create, store, and access vast archives of personal information increases, the law's ability to cope with

365. *Id.* at *6.

366. *Id.* at *4.

367. *Id.*

368. *Id.*

369. *Id.* at *5; *see also In re* Petition of John W. Danforth Grp., Inc., No. 13-MC-33S, 2013 WL 3324017, at *3 (W.D.N.Y. July 1, 2013) (denying request to copy contents of plaintiff's personal smartphone in employment discrimination case under FED. R. CIV. P. 27 because there was insufficient showing that the evidence would otherwise be destroyed or lost before Rule 26 discovery commenced); *see also* Redgrave, *supra* note 154 at 41–42 (discussing at least seven factors courts consider when weighing individual privacy concerns in electronic communication files against an organization's legitimate business interests).

novel privacy implications decreases. The result is incomplete protection against new privacy harms, particularly in the context of civil discovery.

As digital data compilation, storage, and access evolves, the underlying principles of civil discovery nonetheless form a solid foundation for balancing privacy concerns against the need for open access to information in an adversarial civil litigation system. The existing rules, particularly with the 2015 amendments, already provide the mechanisms by which to unearth the limiting principles necessary for recalibrating the scope of discovery. Courts already have the discretion to limit the scope of discovery based on the needs of the case and should utilize the proportionality test in Rule 26 to balance the privacy burden of overly invasive discovery against the needs of the case. Through the proportionality test, balance can be achieved, and the rules will not be outpaced by technological change.

A. Privacy-Based Considerations Are Necessary and Proper

Privacy-based limits on civil discovery of large digital data compilations are necessary to protect individuals from being forced to hand over the thorough archive of their lives contained in the private portion of a social media account or on a smartphone. Although individual content alone may not be "private," the aggregate of data—as a whole—is too broad and detailed to warrant complete discovery in many cases. In essence, the data contained in these digital compilations, when viewed together, paint a detailed mosaic of one's personal life. Access to the entire mosaic should not be granted without adequate justification.

Throughout its history, the Federal Rules of Civil Procedure have balanced the need for open access to information against countervailing limiting principles that, in essence, are rooted in notions of privacy. Even at the time of the rules' adoption, critics noted the intrusiveness of the new discovery regime.[370] The rules have always excluded irrelevant content from the ambit of discovery and shunned discovery attempts that harass, embarrass, or burden others. As the rules evolved, courts expressly carved out specific privacy-based limits, such as attorney-work product or protection of trade secrets. It is within this framework—of striving for a balance between access and privacy protection—that the rules continue to grow and evolve through the 2015 amendments.

Even though the 1938 rules intentionally opened up otherwise

370. *See* Subrin, *supra* note 80 and accompanying text.

personal information to discovery in civil litigation, no one at that time could have anticipated the vast scope of data that would be accessed in modern cases.[371] Electronically stored information, in general, can involve millions of pages of emails, documents, files, and other information. Social media accounts offer multiple functions and aggregate daily activity over time. Smartphones, as noted in the *Riley* case, hold more personal information than an individual could ever carry with them in non-digital form.[372] Quite simply, the world of information has changed. And civil discovery once again must strike a balance.

The 2006 amendments, in addressing ESI specifically, recognized the need for meaningful limits on electronic discovery due to the sheer volume of data now available. Although critics and scholars differ about the actual costs and burdens of discovery,[373] the rules nonetheless have responded to the digital age by accounting for the impact of large digital archives of information. Now, the 2015 amendments to Rule 26 signal a renewed emphasis on proportionality and striking a balance: discovery, at its core, must be proportional to the needs of the case.

At the same time, privacy law in general struggles to adapt to the boom of digital information and its implications on individual privacy rights. While no comprehensive privacy protection exists for social media accounts and personal data on smartphones, privacy law nonetheless is trending towards protecting digital data compilations in some way. In the Fourth Amendment context, for example, some privacy interests have been recognized in cell phones[374] and in privacy-setting protected portions of social media accounts.[375] Additionally, the mosaic theory of the Fourth Amendment may be gaining ground as an additional consideration for privacy protection. Vast digital data compilations may be composed of individual, non-private pieces of information but, when viewed in the aggregate, they paint a detailed picture that is highly personal and subject to some sort of privacy protection. Although problematic in a Fourth Amendment context, mosaic theory nonetheless may be shaping some court decisions about privacy-based limits on GPS tracking or other electronic surveillance.[376]

---

371. *See* Subrin, *supra* note 80.

372. Riley v. California, 134 S. Ct. 2473, 2489 (2014); *see also* Alex Kozinski, *Essay: The Two Faces of Anonymity*, 43 CAP. U. L. REV. 1, 13 (2015) (noting how "surprisingly little trivial information" could reveal a lot about a person, such as an anonymous blogger's identity).

373. *See supra* Part III.A.I.

374. *See Riley*, 134 S. Ct. at 2485.

375. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012).

376. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 954 (2012).

As a whole, traditional privacy law principles may be evolving to adapt to the digital age through recognition of privacy-based protections of digital data compilations.

Without question, civil discovery must allow for much broader intrusion into personal spheres than Fourth Amendment searches and seizures, for example. Parties may inject issues into civil litigation that necessitate prying into private documents and electronic information. But like Fourth Amendment law, civil discovery rules must also account for the new technological landscape in which we now live. Even though our civil discovery system allows for broad discovery into relevant matters, limits do exist. Privacy law concepts should help define those limits in the digital age.

B. The Proportionality Analysis Should Consider Privacy Burdens

The Federal Rules have already equipped courts with the tools they need to craft meaningful limits to civil discovery of large digital data compilations, such as social media accounts and smartphone contents. Under the existing rules and the 2015 amendments, discovery must be "proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."[377] Under this test, even relevant information can be excluded if such discovery is *disproportionate*.[378]

In order to achieve proportionality, courts should (1) acknowledge the privacy concerns that exist with discovery of digital data compilations; (2) include burdens *on privacy* within the proportionality test; and (3) consider protective orders when granting broad access to digital data compilations.

First, courts should recognize that a valid privacy concern exists when a party seeks access to a digital data compilation. This privacy concern is similar to that which underlies the mosaic theory of the Fourth

377. *See* FED. R. CIV. P. 26(b)(1) (proposed 2015), http://www.supremecourt.gov/orders/courtorders/frcv15_5h25.pdf.

378. In social media discovery, courts should also strive to provide a narrow definition of relevance in order to prevent overly broad discovery. *See* Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 910 (2013) (criticizing different approaches courts take to social media discovery).

Amendment: when viewed as a whole, a digital data compilation contains individual bits of information that reveal the intimate details of one's thoughts, feelings, activities, associations, and public movements. This level of detailed information should be afforded some privacy protection, even though each piece of information does not fit neatly into traditional notions of privacy. In other words, the mosaic painted by these small pieces of information should be shielded from civil discovery in some instances.

Thus, courts should be mindful of the personal mosaic that is revealed when a party is granted access to all privacy-setting protected portions of a social media account or smartphone data. Most cases do not justify the intrusiveness of whole-cloth disclosure of the entire digital data compilation. Even though most of the individual pieces of data in these examples may not be considered "private" when analyzed alone, the aggregate of data should not be handed over until the privacy harm of broad discovery is considered.[379] By recognizing the invasiveness of whole-cloth discovery of digital data compilations, courts can begin to disaggregate content and carve out appropriate boundaries for production.

Second, after recognizing that broad discovery of digital data compilations may implicate privacy concerns, courts should take privacy burdens into account when determining the proportionality of discovery. Under the proportionality test, the "burden" of discovery usually looks to economic costs and financial burden.[380] Although financial burdens are important, nothing in the Federal Rules limits this consideration to finances alone. Indeed, a purely economic inquiry is not possible in many cases, as the value of the claim may be difficult to determine and the actual costs of the discovery is unknown.[381] Thus, an economic-only approach nonetheless leads to imprecise calculations. Further, the cost of storing and producing digital data compilations continues to decline, and companies like Facebook empower account-holders to easily access a downloaded version of their entire account.[382] Structuring the law

379. Further, while Mosaic Theory has considerable limitations in the Fourth Amendment context, many of those limits are not an issue in its adaptation in the civil discovery context. *See* Kerr, *supra* note 230.

380. *See In re* Convergent Techs. Sec. Litig., 108 F.R.D. 328, 331–32 (N.D. Cal. 1985).

381. *See* Jonah B. Gelbach & Bruce H. Kobayashi, *The Law and Economics of Proportionality in Discovery*, UNIV. OF PA. LAW SCH. LEGAL SCHOLARSHIP REPOSITORY, Paper No. 1521 (Oct. 20, 2014), http://scholarship.law.upenn.edu/faculty_scholarship/1521.

382. *See Downloading Your Info*, FACEBOOK, https://www.facebook.com/help/131112897028467/ (last visited Sept. 8, 2015) (describing how to download a zip file of one's entire Facebook account).

around merely financial considerations would be short-cited given the pace at which new technology evolves.

Additionally, the proportionality factors already look to some non-pecuniary considerations, such as the importance of the issues at stake in the action. And, as some have noted, other nonmonetary factors should be considered within the proportionality analysis.[383] These factors necessarily involve public policy considerations, societal values, and other principles that cannot be easily quantified. Therefore, courts already balance a variety of concerns—beyond monetary ones—when applying the proportionality test. It follows that privacy-based concerns can also be taken into account when determining proportionality.

Thus, when balancing the needs of the case and the likely benefit of discovery against its burden or expense, *privacy* burdens should be considered as well. In many cases, disclosure of a complete, detailed mosaic of one's personal life is too burdensome on individual privacy interests and is not justified by the needs of the case or is not outweighed by the likely benefit of discovery. A social media account or smartphone may contain highly personal details about the individual, and revealing this information must meet the rules' proportionality threshold.

For example, a personal injury victim may place her physical condition or general emotional state at issue, but such claims do not support complete access to all portions of the plaintiff's private social media account. Rather, the private portions of the social media account should be disaggregated into component parts: timeline status updates, photographs, items uploaded by third parties that merely tag the plaintiff, one-on-one messages, geolocation data, and other items should be considered separately. Additional parameters may rely on date ranges, the parties to a communication, and specific subject matter of each component part. Similarly, a demand for the entire smartphone contents for an employee in a business dispute may be disproportionate given the privacy invasion such discovery poses, particularly if the employee is not a party to the suit. Disaggregation should be considered to prevent unnecessary, disproportionate privacy invasions.[384]

---

383. *See supra* note 130 & accompanying text.

384. As an additional illustration of this point, a social media account or smartphone may reveal that an individual uses a dating app. While dating apps may be relevant in divorce cases, for example, they may be too revealing in a personal injury case, as even the type of app chosen by the individual can touch on highly intimate personal information. *Compare* GRINDR, http://grindr.com/learn-more (an "all-male location-based social network . . . [to] find a new date, buddy, or friend") (last visited Sept. 27, 2015), *with* CHRISTIAN MINGLE, http://www.christianmingle.com/ (last visited Sept. 27, 2015) ("the largest online dating site created specifically for single Christians . . . looking for a friend, romantic partner, or spouse").

In other cases, more severe and precise claims of injuries may support broader discovery into a party's digital data compilations. Severe emotional distress claims and debilitating, permanent physical injuries may justify broader discovery in a personal injury case over garden-variety emotional harm or general pain and suffering.[385] Nonetheless, a forced password disclosure is never proportional. Forcing litigants to hand over their passwords allows complete, unfettered access to all portions of a social media account, regardless of time frame, subject matter, or intended audience. This approach also impedes the privacy rights of third parties who granted access to their own private information to the account-holder only and not to the account-holder's adversaries in litigation.[386] Even cases that justify broad discovery of digital data compilations must stop short of forced password disclosures.

Lastly, as an additional measure of protection, courts should use protective orders to protect some social media or smartphone contents that are handed over in discovery. The "good cause" standard already protects against particularized, serious harm, including embarrassment.[387] By extension, good cause may exist when discovery of large portions of digital data compilations amounts to an invasion of privacy. The highly personal details contained in such a compilation should, at the very least, be shielded from public access. Protective orders are an additional mechanism by which to protect privacy in this new digital discovery landscape, and courts should recognize that the good cause standard can be met through showing privacy-based harms.

Achieving proportional privacy means that the privacy invasion in some cases may outweigh the likely benefits of the discovery. Non-pecuniary burdens are a necessary consideration as a limit to civil discovery and an important aspect of the proportionality analysis. With the addition of privacy burdens, the proportionality test can serve as a mechanism for preventing overly broad discovery of digital data compilations.

VI. CONCLUSION

Large digital data compilations contain bits and pieces of personal information that, when looked at as a whole, create a detailed mosaic portrait of one's life. Discovery of these compilations runs the risk of

385. *See* EEOC v. Simply Storage Mgmt., Inc., 270 F.R.D. 430, 435 (S.D. Ind. 2010).

386. *See supra* note 200 & accompanying text.

387. *See, e.g.*, Cipollone v. Liggett Grp., Inc., 785 F.2d 1108, 1121 (3d Cir. 1986).

invading individual privacy rights. As a result, meaningful protection against overly broad civil discovery is needed. The Federal Rules, throughout their development, have balanced broad discovery against countervailing principles that, at their core, recognize some privacy-based limits. In the 2015 amendments, the rules will emphasize the need to limit discovery based on proportionality: even relevant information is not discoverable if discovery is not proportional to the needs of the case. Although the proportionality analysis traditionally focuses on financial burden of the discovery, *privacy* burden should also be a factor. By recognizing the non-pecuniary burden on privacy that discovery poses, courts can use the Federal Rules to effectively address the challenges created by new technology.