The Privacy Paradox in Discovery

ABSTRACT

Allyson Haynes Stuart[*]

US citizens enjoy strong protection against criminal searches pursuant to the Fourth Amendment, but they must produce a diary entry from a bedroom drawer or a text message to a romantic partner if it is relevant to a civil case and not privileged. The reason for this paradox, long a mystery to outsiders, is a complex mixture of history and culture. Understanding the paradox is particularly important now. In the absence of any other check on discovery, federal and state courts have relied on persuasive sources to protect privacy in pretrial practice, none of which are reflected in the discovery rules. The Supreme Court gutted one of those sources, the federal constitutional right to privacy, in Dobbs. *At the same time, technological advancements and increasingly intrusive discovery requests push the boundaries of the rules. It is time to strengthen individual privacy rights in the context of civil discovery requests that implicate intimate and even incriminating details.*

The early history of discovery rules in the federal system shows no intent that parties to a civil lawsuit waive any privacy rights they might otherwise possess. Rather, the breadth of discovery—intended to prevent secrecy before trial—resulted from grafting equity procedures onto legal claims without retaining equitable guardrails. As technology changed the discovery landscape from designated paper documents to broad categories of electronic databases, broad disclosure became akin to a constitutional right. While digital invasions of privacy were a primary issue for legislative protection and Fourth Amendment concern, no concomitant change occurred in the discovery rules. Instead, courts protected against discovery into private matters by reference to persuasive privacy laws and by use of protective orders, which are increasingly ineffective.

This Article proposes a revision to the civil discovery rules that would give explicit protection to information when it is subject to a reasonable expectation of privacy. The revolution initiated by the broad

---

[*] Professor of Law, Charleston School of Law.

The author wishes to thank Skye E. Martin and Rachel M. Rittelmann for their valuable research assistance, and her colleague Paul E. Lund for his thoughtful comments.

discovery rules did not result in transparency and justice but instead provided tools for abuse. Simply because sensitive information housed in a database or on the cloud is potentially relevant to broad issues in litigation does not mean that it should be presumptively discoverable. Instead, courts should require production only based on a showing of substantial need. Given the erosion of constitutional protection in Dobbs *and its intimations for other rights, the legal system must prevent the use of broad discovery to harass, embarrass, and deter access to the courts.*

TABLE OF CONTENTS

I. INTRODUCTION: CIVIL INVASIONS OF PRIVACY

If the government wants access to an individual's personal correspondence, it must seek a warrant showing probable cause for the

commission of a crime.[1] Whether the correspondence is a handwritten letter, an email, a text message, or a direct message on social media, the government cannot require disclosure from the individual without the request adhering to certain parameters. Specifically, a judge must find that the warrant describes with particularity the items sought and does not violate the Fourth Amendment's prohibition against unreasonable searches.[2] A private party, however, can demand any of these types of correspondence from an individual or third party without a court order based solely on relevance to litigation.[3] The owner of the correspondence could be a party to the litigation or a third party recipient of a subpoena.[4] The scope is limited only by the low bar of relevance to a party's claim or defense and does not necessarily have to be admissible at trial.[5] This Article probes the basis for this broad waiver of privacy rights based solely on the filing of a complaint.

Discovery implicates privacy in myriad ways.[6] Common discovery requests include personal communications such as email, text messages, and third party messaging applications;[7] social media, which can reveal personal connections and group affiliation;[8] wearable

1. Boyd v. United States, 116 U.S. 616, 622 (1886) ("[A] compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the fourth amendment to the constitution.").

2. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

3. *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 30 (1984) ("The 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.").

4. Chazin v. Lieberman, 129 F.R.D. 97, 98 (S.D.N.Y. 1990) (declining to quash subpoena of nonparty banks where defendants' privacy interest in materials did not outweigh plaintiff's right to pursue the relevant material).

5. Fed. R. Civ. P. 26(b)(1); Fed. R. Civ. P. 45(e).

6. This Article uses the term "privacy" to refer generally to a person's right to determine what personal information she will share with others. Professors Daniel J. Solove and Paul M. Schwartz refer to this as "information privacy," as contrasted with "decision privacy" dealing with freedom to make decisions about a person's body and family. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (6th ed. 2018).

7. *See* Daniel Black & Jodi Daniels, *Here Today, Gone Today: Managing Third-Party Messaging Apps in a New Regulatory Environment*, JDSUPRA (June 20, 2023), https://www.jdsupra.com/legalnews/here-today-gone-today-managing-third-9844251/ [perma.cc/R45Y-2HLX] (discussing explosion in use of apps like WhatsApp, Signal, Snapchat, Telegram, and WeChat after the worldwide pandemic).

8. *See* Gordon v. T.G.R. Logistics, Inc., 321 F.R.D. 401, 403–04 (D. Wyo. 2017) (noting intrusiveness of request for extensive social media information); *see also* Allyson Haynes Stuart, *Privacy in Discovery After* Dobbs, 26 VA. J.L. & TECH. 4, 19 (2023) (describing groups on Facebook

devices, which can disclose medical information;[9] and other data from smartphones, including location tracking and health applications.[10] Defendants seek GPS and location services data from workers' cell phones to construct a timeline of their working hours.[11] Personal injury plaintiffs are asked for all their Fitbit data, dating site photographs, and other social media posts.[12] Sexual harassment defendants often seek a decade's worth of plaintiffs' medical and mental health history.[13] Parties may also be required to produce employment records, job applications, personnel files, school records, transcripts, and tax returns.[14] Attorneys warn potential parties that litigation in general may result in exposure of their marital status, work history, current employment, criminal convictions, drug and alcohol history and usage, mental health issues, and prior medical conditions.[15] The subjects of discovery are as broad as an attorney's imagination and are bound only by the requirement that information sought be relevant to a party's claim or defense.

This Article examines the adoption of the Federal Rules of Civil Discovery ("the Rules") to discern the justification for the broad scope of pretrial access to information in the hands of parties and nonparties alike. Not surprisingly, the original purposes for broad discovery diverge greatly from modern practice. As technology and the internet have upended the means of communication, including the quantity of generated data and the pervasive nature of surveillance culture across technological mediums, Fourth Amendment doctrine has largely kept pace by protecting the right to privacy as to data even when shared with

---

related to pregnancy, sexual orientation, sexually-transmitted disease, and sexual abuse); Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995, 1000 (2013) (discussing an instance in which sexual preferences were revealed inadvertently based on Facebook group membership).

9. *See* Allyson Haynes Stuart, *A Right to Privacy for Modern Discovery*, 29 GEO. MASON L. REV. 675, 710–12 (2022) [hereinafter *Modern Discovery*].

10. *Id.* at 706–07, 716–17.

11. Crabtree v. Angie's List, Inc., No. 1:16-cv-00877-SEB-JMD, 2017 WL 413242, at *1 (S.D. Ind. Jan. 31, 2017); *see also* Pendelton v. First Transit, Inc., Civ. No. 20-1985, 2020 WL 10787493, at *1 (E.D. Pa. July 10, 2020).

12. Spoljaric v. Savarese, 121 N.Y.S.3d 531, *1 (N.Y. Sup. Ct. 2020); *see also* Forman v. Henkin, 30 N.Y.3d 656, 659 (2018).

13. Sandoval v. Am. Bldg. Maint. Indus., 267 F.R.D. 257, 262 (D. Minn. 2007).

14. *Id.*

15. *See* William K. Thayer, *Will 'Discovery' Invade My Right to Privacy?*, SCHAUERMANN THAYER INJ. L. (Apr. 1, 2019) (warning potential personal injury plaintiffs that they may be required to answer questions about their marital status, work history and current employment, criminal convictions, drug and alcohol history and usage, mental health issues, and prior medical conditions, and may be required to produce employment records, applications for jobs, personnel files, school records and transcripts, and tax returns).

third parties.[16] In contrast, parties' data searches in civil courts require only the filing of a complaint, with limited restrictions on intrusive requests.[17] Broad discovery has generated decades of complaints, but the Rules' revisions have focused on cost and delay, not privacy.[18]

Concurrently, the privacy risks implicated by data collection have expanded. With the Supreme Court's decision in *Dobbs*[19] and the ensuing state laws criminalizing or attaching civil liability to aiding, abetting, and obtaining an abortion,[20] reproductive health information and location data are not only private but also potentially incriminating.[21] Other privacy rights are in peril as well, including the constitutional right to confidentiality that has underpinned many courts' discretionary protection of discovery.[22]

In response to these emergent privacy concerns, this Article argues that privacy deserves prominent protection in the Federal Rules and that the traditional use of protective orders and confidentiality agreements is insufficient. First, potential litigants are harmed when their personal information is generally regarded as discoverable even if a court agrees to protect against production.[23] These harms include loss of autonomy and chilling meritorious litigation when a potential plaintiff fears the privacy consequences of bringing her claim. Second, problems arise when discovery is required to be disclosed—despite limitations on further dissemination—including the risk of inadvertent disclosure. The more places that sensitive information resides, the greater the risk of accidental revelation. Finally, judges may revise protective orders in the same or subsequent litigation, after a party has relied on those protections in agreeing to produce sensitive information.[24] Protective orders do not govern nonparties or other

16. *See infra* Section II.E.

17. *See* Fed. R. Civ. P. 26(b)(1).

18. *See infra* Section II.C.

19. Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 301 (2022).

20. *See Privacy in Discovery After* Dobbs, *supra* note 8, at 8.

21. *Dobbs*, 597 U.S. 215 at 301.

22. *See infra* Section IV.A.

23. *See infra* Section IV.A.

24. Lambright v. Ryan, 698 F.3d 808, 826 (9th Cir. App. 2012) ("We affirm the portion of the district court's May 4, 2010 order excluding non-privileged materials from the coverage of its protective order, but we hold that it erred in holding that: (1) the protective order applied only to privileged materials produced after its issuance; (2) the privileged materials introduced at the evidentiary hearing were no longer covered by the protective order because Lambright failed to move to seal the evidentiary hearing; and (3) the materials identified by Lambright as privileged were not protected because he failed to support his assertion of privilege by submitting written justifications to the district court. We therefore vacate those portions of the order pertaining to the numbered clauses supra. On remand, the district court shall allow Lambright an opportunity to support his assertions of privilege as to materials that he identified as protected by the attorney-

courts. Instead, privacy protections should be explicit limitations on the scope of discovery, like protections given to attorney work product.[25]

Part I delves into the history of discovery in the United States to discern the original basis for allowing broad discovery without concern for privacy interests. It charts the expansion of information in the digital age and the evolution of rights to privacy against changes in discovery rules. Part II addresses the reasons discovery has maintained its broad scope even in light of its abuse. The problems broad discovery raises are more important than ever, as current Supreme Court doctrine erodes traditional sources of privacy protection historically relied upon by lower courts in the context of protective orders. Part III argues that protective orders and confidentiality provisions are insufficient to ameliorate this issue because they fail to factor privacy into the discovery calculus and because protective orders can be overcome in the same or subsequent litigation. Part IV explains that situating privacy as an express factor in determining the scope of discovery is a necessary start to ending civil invasions of privacy and proposes language to amend the Federal Rules of Civil Procedure (FRCP). Part V briefly concludes.

I. THE HISTORY OF PRIVACY IN DISCOVERY

The history of broad civil discovery in the United States begins with the adoption of the FRCP in 1937.[26] Before that, discovery rules were a patchwork among the states and federal courts with little pretrial disclosure.[27] The Field Code, which had been adopted in about half the states, resembled English common law procedure in eliminating equitable bills of discovery and interrogatories as well as severely limiting motions to produce documents and requests for admission.[28] Where equity proceeding applied, "judges performed very

client, work product, and Fifth Amendment privileges, and shall determine which materials fall within a privilege and are thus covered by the protective order.").

25. *See infra* Section II.B.

26. The Rules were adopted in 1937 and went into effect in 1938. Fed. R. Civ. P. 26; George Shepherd, *Failed Experiment: Twombly, Iqbal, and Why Broad Pretrial Discovery Should be Further Eliminated*, 49 IND. L. REV. 465, 469 (2016) [hereinafter *Failed Experiment*].

27. *See id.* at 469 ("Although some state courts offered isolated discovery opportunities, no state combined them together as did the FRCP. Moreover, many of the state provisions that did exist could not take effect because courts held that federal provisions with no discovery occupied the field, precluding application of the state provisions.").

28. Stephen N. Subrin, *How Equity Conquered Common Law: The Federal Rules of Civil Procedure in Historical Perspective*, 135 PENN. L. REV. 909, 936–37, 939 (1987) [hereinafter *Equity Conquered*].

much as they did in passing on the necessity for a search warrant."[29] Courts largely believed that broad requests for discovery not bound by a court's finding of good cause violated the Fourth Amendment.[30]

In opposition to seemingly unnecessary procedural technicalities and a "sporting theory of justice,"[31] the drafters of the new Rules aimed to reduce or eliminate impediments to finding the truth. The new Rules were to be "scientific, flexible and simple."[32] They would require "each party . . . to lay all his cards upon the table, the important consideration being who has the stronger hand, not who can play the cleverer game."[33] The new discovery rules were rightly seen as revolutionary in expanding the role of pretrial discovery in their zeal to eliminate secrecy before trial.[34] Now, all possible discovery tools would be available in all types of cases.[35]

One little-noted concern of the new discovery provisions was the inordinate power they gave parties and courts to invade the privacy of others. Edson R. Sunderland, credited with drafting the discovery components of the new Rules, engineered this new landscape by

---

29. ALAN WESTIN, PRIVACY AND FREEDOM 334 (1967) (quoting Justice Story as saying "courts of equity will restrain a party from making a disclosure of secrets communicated to him in the course of a confidential employment. And it matters not, in such cases, whether the secrets be secrets of trade, or secrets of title, or other secrets of the party important to his interests.").

30. *See* Red Star Labs. Co. v. Pabst, 194 N.E. 734, 735 (1935) ("We have uniformly held that before an order can be entered under [section 9 of the Evidence Act] there must be good and sufficient cause shown upon reasonable notice, and that the evidence sought to be obtained is pertinent to the issues in the case. The order in this case was general and not limited to the production of documents relevant and pertinent to the issues. It was violative of the constitutional rights of appellant to be secure against unreasonable search and seizure of his papers and effects, as guaranteed him by the Fourth Amendment to the Federal Constitution, and section 6 of article 2 of the State Constitution."); Shell Oil Co. v. Superior Ct. of L.A. Cnty., 292 P. 531, 531 (Cal. Ct. App. 1930) ("The affidavit further shows, through its length, that it is a mere "fishing device," as contended for by petitioner. Being a fishing device, it is in direct violation of the constitutional immunity against unlawful searches and seizures.").

31. Roscoe Pound, *The Causes of Popular Dissatisfaction with the Administration of Justice*, 40 AM. L. REV. 729, 736 (1906) ("A no less potent source of irritation lies in our American exaggerations of the common law contentious procedure. The sporting theory of justice, the 'instinct of giving the game fair play,' as Professor Wigmore has put it, is so rooted in the profession in America that most of us take it for a fundamental legal tenet." The idea that procedure must be contentious "leads to sensational cross-examinations 'to affect credit,' which have made the witness stand 'the slaughter house of reputations.'").

32. *Equity Conquered*, *supra* note 28, at 959.

33. Edson R. Sunderland, *Discovery Before Trial Under the New Federal Rules*, 15 TENN. L. REV. 737, 739 (1939).

34. *Id.* at 738.

35. Stephen N. Subrin, *Fishing Expeditions Allowed: The Historical Background of the 1938 Federal Discovery Rules*, 39 B.C.L. REV. 691, 719 (1998) [hereinafter *Fishing Expeditions*] ("[A]t the time Sunderland drafted what became the federal discovery rules, no one state allowed the total panoply of devices." and the federal rules "eliminated features of discovery that in some states had curtailed the scope of discovery and the breadth of its use.").

importing equity discovery provisions into law cases while eliminating the protections rendering equity remedies extraordinary.[36] This allowed for invasive discovery procedures in all cases without the guardrails inherent in equity practice, which included limited jurisdiction and complex pleading requirements.[37]

During the 1938 hearings of the Senate Committee on the Judiciary, one lawyer pointed out that, in equity, "courts were never intended to be given power over the person of a plaintiff or defendant, except where the parties are not dealing at arms length, or where one has an unfair advantage given by the law."[38] In contrast, law cases did not implicate "the tremendous powers of the chancelor and dangers of abuse."[39] Because of those risks, safeguards applied to actions in equity court allowing them to proceed only if necessary to avoid irreparable injury.[40] Equity was seen as a drastic action only available if legal remedies were not adequate.[41] Having the full artillery of equity discovery rules available in ordinary contract or personal injury cases was predicted to wreak havoc.[42]

Despite these early objections, the Rules were adopted, along with their extraordinary ability to make "vast intrusions on the rights of privacy of individuals."[43] Relatively few have challenged the Rules on a Fourth Amendment basis, even though discovery searches are enforced by government action through court order.[44]

---

36. *See id.* at 715.

37. *See* GEORGE RAGLAND, JR., DISCOVERY BEFORE TRIAL 6 (1932).

38. *Rules of Civil Procedure for the U.S. District Courts: Hearings Before the United States Senate Committee on the Judiciary, Subcommittee on S.J. Res. 281*, 75th Cong. 44 (1938) [hereinafter *Rules Hearings*] (statement of Challen B. Ellis, Member of the Bar, Washington, D.C.); *see also Equity Conquered*, *supra* note 28, at 999 (quoting a lawyer as stating, "[h]eretofore the theory has been that a case may be submitted at one time through the medium of open testimony and in open court, except in the infrequent instances in which depositions are used. Now, by a kind of inquisition conducted under rule 26, interrogatories under rule 33, discovery under rule 34, and admission of facts under rule 36, together with the consequences imminent under rule 37, there is left little further to be done.").

39. *Rules Hearings*, *supra* note 39, at 46.

40. *Id.*

41. *Id.*

42. *Id.* at 47.

43. *Fishing Expeditions*, *supra* note 35, at 732–34.

44. *See* Chad DeVeaux, *A Tale of Two Searches: Intrusive Civil Discovery Rules Violate the Fourth Amendment*, 46 CONN. L. REV. 1083, 1096 n.84 (2014); Jordana Cooper, *Beyond Judicial Discretion: Toward a Rights-Based Theory of Civil Discovery and Protective Orders*, 36 RUTGERS L.J. 775, 818–19 (2005). *But see* DeVeaux, *supra* at 1090 (arguing that "to pass constitutional muster, document production orders seeking private papers should be premised on a showing of probable cause"); John Swanson, *Privacy Limitations on Civil Discovery in Federal and California Practice*, 17 PAC. L. J. 1, 10 (1985) ("[T]he logical way to deal with the problem [of privacy

Over the ensuing eighty years, drafters have revised the Rules on numerous occasions.[45] Only once, in 1970, did the drafters consider changes to protect litigants' privacy.[46] Since then, despite vast technological advancement—including the rise of computerized databases, the internet, and global information gathering—the amendments to the discovery rules have not addressed privacy.[47] The next Section further discusses the history of the Rules' revisions against the backdrop of privacy risks resulting from changes in culture and technology.

A. Early Focus on Depositions and "Blackmail": The 1930s

Early references to concern for privacy rights in civil discovery focused on depositions and the publication of details of those examinations in newspapers.[48] In 1932, lawyer and researcher George Ragland compiled "field studies" of the discovery practices of all the states as well as the federal and English provisions in his book, *Discovery Before Trial*. This work would prove extremely influential to Sunderland in drafting the federal discovery rules.[49] Ragland quoted lawyers in several states who complained of parties misusing depositions to gain advantages over litigants in cases, such as seduction under promise of marriage, divorce proceedings, and alienation of affection.[50] There, depositions were threatened and taken "for blackmailing purposes," and "newspapers were full of salacious details disclosed by" those examinations.[51] Professor Stephen Subrin also recounts early fears of Rule opponents that "unsavory plaintiffs' lawyers would use discovery to 'blackmail' corporations and their

---

limitations on discovery] is to extend the Fourth Amendment law of search and seizure to cover 'searches' through discovery by private litigants of their opponents and third parties.").

45. *E.g.*, FED. R. CIV. P. 26 ("As amended Dec. 27, 1946, eff. Mar. 19, 1948; Jan. 21, 1963, eff. July 1, 1963; Feb. 28, 1966, eff. July 1, 1966; Mar. 30, 1970, eff. July 1, 1970; Apr. 29, 1980, eff. Aug. 1, 1980; Apr. 28, 1983, eff. Aug. 1, 1983; Mar. 2, 1987, eff. Aug. 1, 1987; Apr. 22, 1993, eff. Dec. 1, 1993; Apr. 17, 2000, eff. Dec. 1, 2000; Apr. 12, 2006, eff. Dec. 1, 2006; Apr. 30, 2007, eff. Dec. 1, 2007; Apr. 28, 2010, eff. Dec. 1, 2010; Apr. 29, 2015, eff. Dec. 1, 2015.").

46. *See infra* Section III.B. One exception is the provision in Fed. R. Civ. P. 5.2 for redaction of personally identifiable information like social security numbers from filings with the court.

47. *See infra* Section III.C.

48. *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 34–35 (1984) ("[D]iscovery by depositions and interrogatories has a significant potential for abuse" and "[t]here is an opportunity, therefore, for litigants to obtain – incidentally or purposefully – information that not only is irrelevant but if publicly released could be damaging to reputation and privacy.").

49. GEORGE RAGLAND, JR., DISCOVERY BEFORE TRIAL (1932).

50. *Id.* at 31.

51. *Id.*

officers."[52] Of course, this concern for newspapers' publication of private facts dovetails with the emerging right to privacy that Samuel Warren and Louis Brandeis discuss in their influential 1890 article, *The Right to Privacy*.[53] Warren and Brandeis too complained of newspapers publishing gossip, which had become a "trade."[54] They warned that details of sexual relations were broadcast in the papers' columns, attaining "the dignity of print."[55] Modern advancements like printing and photography further contributed to the invasion of individuals' privacy.[56] Some of this same "gossip" came from deposition questions.[57] Further evidence of the concern for misuse of the deposition power is the fact that the original Rules only included a provision for protective orders in the context of depositions.[58] Subdivision (b) of Rule 30 gave the court broad discretion as to the parameters of a deposition, including its location, its scope, and who could be present at the time.[59] The Rule provided for sealing the deposition or specified documents that were "to be opened as directed by the court."[60] Finally, the Rule provided that the court "may make any other order which justice requires to protect the party or witness from annoyance, embarrassment, or oppression."[61]

This 1937 language—protection from annoyance, embarrassment, or oppression—echoes the sentiments of lawyers at the time concerned about newspapers' misuse of depositions.[62] It remains the language of protection orders today, now part of Rule 26(c), applicable to all discovery.[63]

Ragland's field studies quote two almost identical state provisions that—unlike the Federal Rules—included explicit procedures for claims of privacy as to documents.[64] Upon request for a

52. *Equity Conquered*, *supra* note 28, at 978.

53. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); E.L. Godkin, *The Rights of the Citizen IV. To His Own Reputation*, SCRIBNER'S, July 1890, at 58, 66 ("The chief enemy of privacy in modern life is that interest in other people and their affairs known as curiosity, which in the days before newspapers created personal gossip.").

54. Warren & Brandeis, *supra* note 53, at 196.

55. *Id.*

56. *See id.*

57. *See* RAGLAND, *supra* note 49, at 31.

58. Hubert Dee Johnson, *Depositions, Discovery, and Summary Judgments Under the Proposed Uniform Federal Rules*, 16 TEX. L. REV. 191, 196 (1938).

59. *See id.*

60. *Id.*; FED. R. CIV. P. 30(b) (1937).

61. Johnson, *supra* note 58, at 196.

62. *See id.*; RAGLAND, *supra* note 49, at 31.

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

64. RAGLAND, *supra* note 49, at 351–52, 390.

"book, paper, writing[,] or document," Ohio and Wyoming allowed a "party in possession" thereof to argue that the dossier, or part of it, "is of mere private interest, or of such character that it ought not to be produced, or an inspection or copy allowed or taken."[65] Either party could file a motion, and the court could "direct a private examination of it by a master."[66] Ragland does not otherwise mention these privacy provisions or the use of a master, although he expresses disapproval of bringing matters to the already "overburdened" court.[67] This could suggest that Ragland opposed the use of a master or other court intervention in discovery. In any event, the original federal discovery rules contained no privacy protection.[68]

B. Attorney Work Product and Confidential Commercial Information: 1940–1970

By the 1950s, the revolution of the discovery rules was underway.[69] Amendments in 1946 eliminated the leave of court

---

65. *Id.* at 351–52 (quoting Ohio law); 390 (quoting Wyoming law).

66. *Id.* Historically, the term "master" descended from the common law "master in chancery," appointed as an assistant to the court, with authority to take depositions and perform other duties. *See* Samuel L. Bray, *The System of Equitable Remedies*, 63 UCLA L. REV. 530 (2016); JOHN G. HENDERSON, CHANCERY PRACTICE WITH ESPECIAL REFERENCE TO THE OFFICE AND DUTIES OF MASTERS IN CHANCERY, REGISTERS, AUDITORS, COMMISSIONERS IN CHANCERY, COURT COMMISSIONERS, MASTER COMMISSIONERS, REFEREES, ETC. 35–38 (1904).

67. RAGLAND, *supra* note 49, at 132 ("[T]he theory that the right to discovery is within the discretion of the court and that each case has its peculiar status as regards discovery, serves as an invitation for needless presentation of disputes to an already overburdened court.").

68. *See id.* at 193. One additional area of privacy in pretrial discovery noted by Ragland was in the context of a person's physical examination. Some states allowed a court to require a plaintiff suing for personal injury to submit to a physical examination by a physician selected by the court. Ragland stated,

> [i]t is of great facility in determining the exact nature, extent and probable duration of the injury in personal injury cases that the defendant be allowed to have an examination of the plaintiff by a competent physician. On the other hand, it is necessary that the examination be so conducted and supervised that no abuse or unnecessary violation of the rights of personal privacy may be allowed.

Id. at 191. Similarly, he cites a number of cases where courts find that "the discovery of truth and prevention of fraud is so necessary in administering justice in personal injury cases that the slight inroad on the right of personal privacy must be tolerated and that the courts have inherent power to allow physical examinations." *Id.* at 192. Many states provide that a female is entitled to be examined by a physician of her own sex. *Id.* Interestingly, Ontario allowed the physician to examine but not to question the person. A court explained that, "[t]o permit the plaintiff to be physically examined in a sufficient invasion of his personal rights without giving the surgeon the right to hold an inquisition on him.'" *Id.* at 193.

69. *See Fishing Expeditions*, *supra* note 35, at 738 ("By the end of the first decade after the Federal Rules became law, many courts were routinely giving the discovery provisions the full scope the drafters had intended.").

requirement for taking depositions and broadened the overarching scope of discovery to include otherwise inadmissible evidence, "which [was projected to] lead to the discovery of [admissible] evidence."[70] The Supreme Court approved the broad scope of discovery in the 1947 case *Hickman v. Taylor*, where it noted the new discovery provisions' "vital role in the preparation for trial" allowing the parties "to obtain the fullest possible knowledge of the issues and facts before trial."[71] That decision recognized a privacy right in discovery, but it was the right of attorneys to protect the fruits of their labor from their opponents:

> In performing his various duties, . . . it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. . . . Were [the attorney's work product] open to opposing counsel on mere demand, much of what is now put down in writing would remain unwritten. . . . The effect on the legal profession would be demoralizing.[72]

Thus, the Court upheld the "general policy against invading the privacy of an attorney's course of preparation" without a showing of necessity.[73] *Hickman* ensured the adversary process by protecting against disclosure of the attorney's research, thought processes, or opinions.[74] At the same time, the right to discovery appeared to diverge from any Fourth Amendment limitation as the Court embraced party-driven, broad civil searches.[75]

In the meantime, lower courts were protecting privacy in the context of confidential commercial information, like trade secrets and financial records.[76] For example, in *Lauer v. A/S Meyers Tankrederi*, the US District Court for the Eastern District of Pennsylvania denied discovery of financial information, noting that "[t]he institution of a personal injury suit by one who never asked to be hurt in the first place does not constitute probable cause for the issuance of a search warrant into his personal financial affairs."[77] A showing of good cause was

---

70. FED. R. CIV. P. 26(a) advisory committee's note to 1946 amendment.

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

72. *Id.* at 510–11.

73. *Id.* at 512.

74. *See* Wayne D. Brazil, *The Adversary Character of Civil Discovery: A Critique and Proposals for Change*, 31 VAND. L. REV. 1295 (1978).

75. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994) ("[T]he Fourth Amendment applies equally to civil and criminal law enforcement. Its text speaks to all government searches and seizures, for whatever reason.").

76. *See* Richland Wholesale Liquors, Inc. v. Joseph E. Seagram & Sons, Inc., 40 F.R.D. 480, 482–83 (D.S.C. 1966) (requiring a "compelling need" for the discovery of financial records); Serv. Liquor Distribs. v. Calvert Distillers Corp., 16 F.R.D. 344, 347 (S.D.N.Y. 1954) ("Certain items from those documents may be relevant, but this is no reason for giving the plaintiff a roving commission to get not merely those items but also all the details of a business that may have no relevancy to the lawsuit, but which would be delectable nuggets of information for a competitor.").

77. Lauer v. A/S Meyers Tankrederi, 39 F.R.D. 334, 335 (E.D. Pa. 1966).

necessary to avoid "a dangerous and unwarranted incursion into the financial privacy of personal injury plaintiffs."[78] While the Rules had broadened discovery, courts instinctively protected personal information like financial records.[79]

In turn, when the Rules were next revised in 1970, they provided for the work product protection recognized in *Hickman* and the possibility for protective orders shielding commercial and financial privacy interests.[80] On the other hand, while Rule 34 had originally required court approval and a showing of "good cause" to obtain documents, the Rule was amended to omit those requirements.[81] Instead of limits to production under Rule 34, courts were encouraged to continue using protective orders if production threatened exposure of trade secrets or other confidential material.[82] As the advisory committee noted, this change "reflect[ed] existing law," whereby "courts ha[d] not given trade secrets automatic and complete immunity against disclosure, but have in each case weighed their claim to privacy against the need for disclosure."[83]

These were small tweaks in light of the significant changes that had occurred by then in technology and privacy law.[84] The mid-60s saw increased concerns about electronic eavesdropping, data surveillance, computerization, and the increased collection and processing of personal information.[85] In 1966, the Freedom of Information Act (FOIA)

---

78. *Id.*

79. *See id.*; *Richland*, 40 F.R.D at 483*; Serv. Liquor*, 16 F.R.D. at 347.

80. *See* FED. R. CIV. P. 26(c)(1)(G) (providing for a protective order "requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way"). This provision is important too because corporations have been found not to have rights to privacy. United States v. Morton Salt Co., 338 U.S. 632 (1950).

81. In fact, some courts had recognized that document requests necessitated a higher burden than other types of discovery. *See* Hickman v. Taylor, 153 F.2d 212 (3d Cir. 1945), *aff'd*, 329 U.S. 495 (1947) (noting that the good cause requirement for document production is "a difference in language in these Rules which we think must be given attention"). Other courts apparently disregarded it outside the context of trial preparation materials. *See* FED. R. CIV. P. 26(c) advisory committee's note to 1970 amendment ("With respect to documents not obtained or prepared with an eye to litigation, the decisions, while not uniform, reflect a strong and increasing tendency to relate 'good cause' to a showing that the documents are relevant to the subject matter of the action."); *see also* Geoffrey C. Hazard, Jr., *From Whom No Secrets Are Hid*, 76 TEX. L. REV. 1665, 1686 (1998) [hereinafter Hazard, *Secrets*] (requirements of court approval and good cause "were omitted on the ground that they had become needless formalities because court had come to grant discovery requests as a matter of routine").

82. *See* FED. R. CIV. P. 34 advisory committee's note to 1970 amendment ("Protection may be afforded to claims of privacy or secrecy or of undue burden or expense under what is now Rule 26(c) (previously Rule 30(b)).").

83. FED. R. CIV. P. 26(c) advisory committee's note to 1970 amendment.

84. *See* WESTIN, *supra* note 29, at 206.

85. *See id.* at 173.

was passed to give the public access to information federal government agencies had collected.[86] Other legislative acts included the Wiretap Act,[87] the Bank Secrecy Act,[88] and the Fair Credit Reporting Act.[89] Privacy scholar Alan Westin warned that "the increased collection and processing of information for diverse public and private purposes, if not carefully controlled, could lead to a sweeping power of surveillance by government over individual lives and organizational activity."[90] A contemporaneous article by Roy N. Freed, a legal authority on computers, warned that companies' legal opponents would demand their computer records, thereby "conduct[ing] far more effective 'fishing expeditions' than previously."[91]

The Supreme Court brought Fourth Amendment doctrine into the technology age in *Katz v. United States*.[92] In determining that the government had conducted a search when it electronically surveilled the defendant's phone conversation in a telephone booth, the Court made clear that technology should not erode Fourth Amendment principles: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[93] Physical trespass was no longer key to the analysis, as the Fourth Amendment protects "people, not places," and "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[94] Justice Harlan's famous concurrence articulated the two-part test that became fundamental: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[95]

In addition, the Court recognized a newfound constitutional right to privacy in certain zones of intimacy.[96] In *Griswold v. Connecticut*, the Court found that a Connecticut law criminalizing the

---

86. *Id.* at 386.

87. 18 U.S.C. § 2510.

88. 12 U.S.C. § 3401.

89. 15 U.S.C. § 1681.

90. WESTIN, *supra* note 29, at 173.

91. *Id.* at 301 (quoting Roy N. Freed, *Your Computer – Witness for the Prosecution?*, MGMT. REV. (1962)).

92. *See* 389 U.S. 347, 348 (1967).

93. *Id.* at 351.

94. *Id.* at 351, 359.

95. *Id.* at 361.

96. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

provision of contraception violated a married couple's constitutional right to privacy.[97] Justice Douglas recognized the relationship as "within the zone of privacy created by several fundamental constitutional guarantees," including the First, Fourth, and Fourteenth Amendments.[98] Years later, the Court would extend this privacy right to a woman's decision to terminate a pregnancy.[99] None of these advances in privacy law were transported into the discovery rules, where broad requests remained rampant. As discussed below, these Supreme Court protections now too have been severely curtailed.

C. Weapons of Mass Discovery—Decades of Abuse: 1970–1990

After 1970, backlash mounted against the breadth and misuse of civil discovery.[100] While discovery had become "central to American litigation," by this time, there was also "very broad opposition to the liberality of discovery."[101] Amendments in 1980 counseled parties to attempt resolving disputes themselves and, if necessary, to seek the intervention of the court.[102] Three years later, the advisory committee acknowledged those changes were insufficient, as "[e]xcessive discovery and evasion or resistance to reasonable discovery requests" continued to be significant.[103] The committee recognized that advocates were using discovery as "tactical weapons rather than to expose the facts and illuminate the issues."[104] Their solution was to impose an attorney signature requirement and sanctions under Rule 37 to deter and punish misconduct, and to require a discovery conference under 26(f).[105] The amendments also introduced the first express proportionality limitation to the Rules' scope, including consideration of whether a discovery request would be unduly burdensome or expensive in light of the amount in controversy, the needs of the case, limitations on the parties' resources, and the importance of the issues at stake in the litigation.[106] While a goal of the amendments was to encourage judges to be

97. *See id.*
98. *Id.*
99. Roe v. Wade, 410 U.S. 113, 153 (1973).
100. FED. R. CIV. P. 26(f) advisory committee's note to 1980 amendments.
101. Richard L. Marcus, *Discovery Containment Redux*, 39 B.C. L. REV. 747, 751 (1998).
102. FED. R. CIV. P. 26(f) advisory committee's note to 1980 amendments.
103. *Id.*
104. *Id.*
105. 85 F.R.D. 521; 97 F.R.D. 165.
106. FED. R. CIV. P. 26(b)(1) (1983).

aggressive in deterring over-discovery, they were not particularly effective in doing so.[107]

Against this backdrop, the country also saw further striking developments in its privacy law. The 1989 Supreme Court case *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press* illustrates the extent to which privacy had become part of the country's lexicon.[108] The case considered whether one of the exemptions to the right of disclosure under FOIA covered information gathered in an FBI "rap sheet," an official record of arrests and prosecutions.[109] Congress included two privacy exemptions to FOIA in 1966 amendments that otherwise required government agencies to make its records available upon request.[110] The exemption at issue in this case allowed the government to withhold records compiled for law enforcement purposes "to the extent that the production . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[111] The primary argument against disclosing the contents of the rap sheets was that the individual items of information were otherwise public knowledge on record at local courthouses or police stations—a condition termed "practical obscurity."[112]

In deciding what Congress meant by "personal privacy," the Court noted that the question implicated what it had recognized in *Whalen v. Roe* as "the individual interest in avoiding disclosure of personal matters."[113] The government's argument that there was no such interest in events that had been previously disclosed to the public was a "cramped notion of personal privacy."[114] The Court cited, among other sources, Warren and Brandeis' 1890 law review article, Alan Westin's book, *Privacy and Freedom*, and Webster's Dictionary in discussing the importance of the individual's control over information about himself. The fact that information may have been disclosed to others does not deprive it of all privacy; instead, it is "the degree of dissemination" and "the passage of time" that mattered in determining a privacy right at common law. Here, the "compilation of otherwise

---

107. Richard L. Marcus, *Retooling American Discovery for the Twenty-First Century: Toward A New World Order?*, 7 TUL. J. INT'L & COMP. L. 153, 162 (1999) [hereinafter *Retooling American*].

108. U.S. Dep't of Just. v. Reporters Comm. For Freedom of the Press, 489 U.S. 749, 751 (1989).

109. *Id.* at 757.

110. 5 U.S.C. §§ 552(b)(6), 552(b)(7)(C).

111. § 552(b)(7)(c).

112. *Reporters Comm. For Freedom of Press*, 489 U.S. at 760–62.

113. *Id.* at 762 (citing Whalen v. Roe, 429 U.S. 589, 598–600 (1977)).

114. *Id.* at 762–63.

hard-to-obtain information" did not alter "the privacy interest implicated by disclosure of that information."[115]

The Court noted the "web of federal statutory and regulatory provisions that limits the disclosure of rap-sheet information," as intending to protect the subjects' privacy as well as a "recognition of the power of compilations to affect personal privacy."[116] Finally, the Court acknowledged the implications for privacy represented by compiled computerized data banks, an impetus for the passage of the Privacy Act of 1974.[117] This led to the determination that "[t]he privacy interest in a rap sheet is substantial" based in no small part on the length of time "that in today's society the computer can accumulate and store information."[118] *Whalen* itself had noted "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[119]

Despite the prominence of privacy in Supreme Court decisions and legislation during these decades, civil litigation continued to enable "the power for the most massive invasion into private papers and private information . . . to anyone willing to take the trouble to file a civil complaint."[120] Professor Samuel Rifkind raised this anomaly in 1976, noting that "[a] foreigner watching the discovery proceedings in a civil suit would never suspect that this country has a highly-prized tradition of privacy enshrined in the Fourth Amendment."[121] Few others seemed to recognize the paradox of broad civil discovery despite strong constitutional privacy rights.

D. ESI and Proportionality: 1990–2015

The rise of the internet in the 1990s was the next tremendous catalyst for change in methods of communication as well as accompanying concerns about privacy.[122] The decade saw a flood of

115. *Id.* at 763.

116. *Id.* at 764.

117. *Id.* at 764–65.

118. *Id.* at 764.

119. Whalen v. Roe, 429 U.S. 589, 605 (1977).

120. Samuel H. Rifkind, *Are We Asking Too Much of Our Courts?*, *in* THE POUND CONFERENCE: PERSPECTIVES ON JUSTICE IN THE FUTURE 51, 61 (A. Leo Levin & Russell R. Wheeler eds. 1979).

121. *Id.*

122. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701 (Congress describing the opportunities and dangers presented by electronic communication).

legislation to protect email privacy,[123] drivers' privacy,[124] health insurance privacy,[125] children's online privacy,[126] and financial records privacy.[127] Again, the advisory committee took note of the problem, stating in 1993 that "[t]he information explosion of recent decades has greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument for delay or oppression."[128] By the 2000s, data breaches had become an epidemic, and global positioning system (GPS) devices and smartphones were widespread.[129] The iPhone debuted in 2007.[130] Social media also began to proliferate with the launch of Friendster, MySpace, and LinkedIn in the early 2000s.[131] Facebook launched in 2004 and became the dominant social media platform by 2008.[132] All of these new data repositories became the subjects of discovery demands as litigants sought cell phone data, online search history, location data, and passwords to social media accounts.[133]

As in 1980 and 1983, subsequent discovery reform efforts did not address privacy concerns.[134] Amendments focused instead on reducing

123. *Id.* §§ 7701–7713.

124. Drivers' Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725.

125. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936; 45 C.F.R. § 164.

126. Children's Online Privacy Protection Act of 1998,15 U.S.C. §§ 6501–06, 16 C.F.R. § 312.

127. Gramm-Leach-Bliley Act, Pub. L. No. 106–102, Stat. 1338 (1999).

128. Fed. R. Civ. P. 26(b) advisory committee note to 1993 amendment.

129. *See* Chimdi Nwosu, *Visualizing the 50 Biggest Data Breaches From 2004-2021*, THE VISUAL CAPITALIST (June 1, 2022), https://www.visualcapitalist.com/cp/visualizing-the-50-biggest-data-breaches-from-2004-2021/ [perma.cc/TQ5U-JSPF].

130. Kevin Urrutia, *When Did Social Media Become Popular*, VOY (Feb. 9, 2024), https://voymedia.com/when-did-social-media-become-popular/#google_vignette [perma.cc/CBY2-2EZE].

131. *Id.*

132. *Id.*; *see also* Esteban Ortiz-Ospina, *The Rise of Social Media*, OUR WORLD IN DATA (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media [https://voymedia.com/when-did-social-media-become-popular/#google_vignette].

133. *See* Allyson Haynes Stuart, *Finding Privacy in a Sea of Social Media and Other E-Discovery*, 12 NW. J. TECH. & INT. PROP. 149, 152–53 (2014).

134. In 1993, the rules added two additional proportionality factors—"whether the burden or expense of those proposed discovery outweighs its likely benefit" and "the importance of the proposed discovery in resolving the issues;" numerical limits on depositions and interrogatories; and an initial disclosure duty limited by an ability to opt out. FED. R. CIV. P. 26 advisory committee note to 2015 amendment. Again, the drafters stressed the discretion of the court to impose restrictions on "scope and extent of discovery." FED. R. CIV. P. 26 advisory committee's note to 1993 amendment. In 2000, a sentence was added to 26(b)(1) reminding that the proportionality provisions of 26(b)(2) apply to all discovery, parties were no longer allowed to opt out of mandatory disclosures, and relevance was confined to the parties' claims or defenses, not to the "subject matter." FED. R. CIV. P. 26 advisory committee's note to 2000 amendment.

costs and delay largely by increasing cooperation, judicial management, and proportionality.[135] The amendments in 2006 and 2015 in particular dealt with the explosion in electronic discovery.[136] While electronically stored information (ESI) was already common by 2006, primarily in the form of email and computer databases, the Rules were amended to provide specifically for the production of ESI and the consideration of reasonably usable forms of production.[137] The Rules also included protections against privilege waiver and limitations on sources that are not reasonably accessible.[138] These changes were intended to encourage cooperation and lessen the costs and delay of lengthy document review.[139]

The most recent amendment in 2015 returned the proportionality factors to Rule 26(b)(1), ensuring that those factors function as prominent limitations on the scope of discovery.[140] The amendments also changed Rule 37(e) to limit sanctions for spoliation of ESI, addressing a split among circuits.[141] The Advisory Committee stressed the need for "continuing and close judicial involvement in the cases that do not yield readily to the ideal of effective party management."[142] Once again, the Rules left out any explicit reference to privacy, and continued to rely on judicial management to stem abuse.

E. Supreme Court Developments: 2012–2022

While the Rules focused on limiting the costs and delays engendered by modern data, Fourth Amendment doctrine focused on the substance of the data vast technology could generate.[143] Most

135. *See* Paul W. Grimm, *Are We Insane? The Quest for Proportionality in the Discovery Rules of the Federal Rules of Civil Procedure*, 36 REV. LITIG. 117, 129–30 (discussing the 2010 Duke Conference that evaluated the state of civil discovery and determined that "cooperation and proportionality" along with "sustained, active, hands-on judicial case management" were the key lessons).

136. FED. R. CIV. P. 26 advisory committee's note to 2006 & 2015 amendments.

137. FED. R. CIV. P. 34 advisory committee's note to 2006 amendment. Rule 34(b)(2)(D) and (E) specifically address objections to a request for production of ESI and the production of ESI in a form in which it is ordinarily maintained or otherwise reasonably usable.

138. *See* Zubulake v. UBS Warburg, 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

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

140. FED. R. CIV. P. 26 advisory committee's note to 2015 amendment. ("The present amendment restores the proportionality factors to their original place in defining the scope of discovery. This change reinforces the Rule 26(g) obligation of the parties to consider these factors in making discovery requests, responses, or objections.").

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

142. FED. R. CIV. P. 26 advisory committee's note to 2015 amendment.

143. *See* Riley v. California, 573 U.S. 373, 393–97 (2014) (describing how cell phones impact the Fourth Amendment analysis).

importantly, the nature of searches of GPS devices, smartphone data, and cell site location information led the Supreme Court to rethink the Fourth Amendment in relation to the third party doctrine and the expectation of privacy against pervasive surveillance.[144] In *United States v. Jones*, the Supreme Court found that the attachment of a GPS tracking device to an individual's vehicle and subsequent monitoring of that vehicle on public streets constituted a search within the meaning of the Fourth Amendment.[145] The majority opinion declined to decide whether the use of the GPS device to monitor the vehicle's movements would have violated the Fourth Amendment in the absence of physical trespass.[146] However, Justice Sotomayor's concurrence stated that such surveillance encompassing a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,"[147] does implicate a reasonable societal expectation of privacy.

Two years later, in *Riley v. California*, the Court found that the warrantless search of data stored on a suspect's cell phone incident to an arrest was unreasonable under the Fourth Amendment.[148] The search incident to arrest exception did not justify the search of digital data in addition to the physical phone itself.[149] Cell phone technology is distinct from previous subjects of Fourth Amendment jurisprudence, particularly in light of its storage capacity, which contains data by which "[t]he sum of an individual's private life can be reconstructed."[150]

The volume and intrusiveness of information in digital records also influenced the Supreme Court in its finding that the Government's actions in accessing historical cell phone records constituted a search under the Fourth Amendment.[151] The Court in *Carpenter v. United States* distinguished the gathering of cell-site location technology from ordinary surveillance or the gathering of traditional third party records because of the technology's "ability to chronicle a person's past movements through the record of his cell phone signals."[152] These

144. *See, e.g.*, United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring).

145. *See id.* at 402.

146. *See id.*

147. *Id.* at 417.

148. *See* Riley v. California, 573 U.S. 373, 401 (2014).

149. *See id.* at 385.

150. *Id.* at 394.

151. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

152. *Id.* at 2216, 2220. Of course, civil discovery too can uncover "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." In addition to cell phones, social media, health tracker data, and other information from devices connected to the Internet of Things (IoT) provide broad access to personal information. Lower courts have been

decisions effectively construe constitutional rights in light of unprecedented advancements in technology's scope.

By contrast, in 2022, the Supreme Court reversed fifty years of precedent in finding no constitutional right to privacy that would protect a person's right to an abortion.[153] While acknowledging that the Due Process Clause "has been held to guarantee some rights that are not mentioned in the Constitution," the Court stated that "any such right must be 'deeply rooted in this Nation's history and tradition' and 'implicit in the concept of ordered liberty'."[154] The right to abortion "does not fall within this category."[155] The Court's majority decision took pains to say it was limited to abortion and "does not undermine [other Due Process decisions] in any way."[156] Its reasoning, however, implicates other case law relying on the substantive due process right to privacy.[157] As the dissent stated, *Roe* and *Casey* have been linked for decades "to other settled freedoms involving bodily integrity, familial relationships, and procreation."[158] Specifically, the right to purchase and use contraception and the rights to same-sex intimacy and marriage "are all part of the same constitutional fabric, protecting autonomous decision-making over the most personal of life decisions."[159] While *Dobbs* purports to be inapplicable to "the right to shield information from disclosure,"[160] that right too is at risk.[161]

After *Dobbs*, twenty-one states have banned or restricted abortion in ways that would have violated *Roe*.[162] In Texas, private

---

influenced by these cases in the discovery context, protecting against broad examination of cell phones. *See* Henson v. Turn, Inc., No. 15-CV-01497-JSW (LB), 2018 WL 5281629, at *6 (N.D. Cal. Oct. 22, 2018); Bakhit v. Safety Marking, Inc., No. 3:13CV1049 (JCH), 2014 WL 2916490, at *3 (D. Conn. June 26, 2014).

153. *See* Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 225 (2022).

154. *Dobbs,* 597 U.S. at 216, 231.

155. *Id.*

156. *Id.* at 218; 346 (Kavanaugh, J., concurring in part) ("I emphasize what the Court today states: Overruling *Roe* does *not* mean the overruling of those precedents, and does *not* threaten or cast doubt on those precedents.").

157. *See id.* at 383.

158. *Id.* at 362 (Breyer, Sotomayor, and Kagan, JJ., dissenting) (citations omitted).

159. *Id.*

160. *Id.* at 223.

161. *See* NASA v. Nelson, 562 U.S. 134, 138 (2011) (rejecting employees' claim that NASA's investigation into their drug use violated their constitutional privacy interest in avoiding disclosure of personal matters: "assum[ing], without deciding that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon,*" any such right was not violated here); *id.* at 160 (Scalia, J., concurring) ("A federal constitutional right to 'informational privacy' does not exist."); *id.* at 169 (Thomas, J., concurring) ("No provision in the Constitution mentions such a right.").

162. Allison McCann, Amy Schoenfeld Walker, Ava Sasani, Taylor Johnston, Larry Buchanan & Jon Huang, *Tracking Abortion Bans Across the Country*, N.Y. TIMES (Jan. 8, 2024),

citizens can sue abortion providers and other individuals who assist patients seeking an abortion after about six weeks of pregnancy, in effect offering cash bounties for suing a person who has helped another obtain an abortion.[163] States impose criminal liability for aiding and abetting an abortion, making it a crime for any individual, whether a healthcare provider or not, to assist a pregnant person in getting an abortion.[164] For example, government agents in Nebraska used personal messages they obtained from Facebook to prosecute a mother for aiding her daughter in obtaining an unlawful abortion, in addition to prosecuting the daughter.[165]

In response to these developments, some states and the federal government have passed laws protecting medical data or data in general in an effort to protect against problematic use of medical information.[166] California expanded the scope of its Confidentiality of Medical Information Act to strengthen the protection of mental health information exchanged through digital health applications.[167] The Act prohibits health care providers from disclosing patient medical information without first obtaining written authorization from the individual.[168] The Biden administration has introduced rules that would protect certain health data from being used to prosecute clinicians and patients by prohibiting certain disclosures of personal health data that may be used "for a criminal, civil, or administration investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating lawful reproductive health care, or identifying any person for the purpose of initiating such an

---

https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html [perma.cc/N2Y5-2EY7].

163. *See* Texas Heartbeat Act, TEX. HEALTH & SAFETY CODE ANN. §§ 171.201–.212 (West 2021) ("An Act relating to abortion, including abortions after detection of an unborn child's heartbeat; authorizing a private civil right of action.").

164. *Human Rights Crisis: Abortion in the United States After Dobbs*, HUM. RTS. WATCH (Apr. 18, 2023), https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs#_ftn87 [perma.cc/9G3E-KQ4K].

165. Johana Bhuiyan, *Health Data Privacy Post-Roe: Can Our Information Be Used Against Us?*, THE GUARDIAN (June 24, 2023, 6:00 AM), https://www.theguardian.com/us-news/2023/jun/24/health-data-privacy-protection-roe-abortion-tech-laws [perma.cc/9WBV-EJ9Z].

166. *See id.*

167. *See California Expands the CMIA to Regulate Mental Health Digital Services*, BLANKROME (Oct. 18, 2022), https://www.blankrome.com/publications/california-expands-cmia-regulate-mental-health-digital-services#:~:text=California%20Governor%20Gavin%20Newsom%20signed,or%20online%20%E2%80%9Cmental%20health%20digital [perma.cc/ZZ5M-S8HA].

168. *See id.*

investigation or proceeding."[169] More general data protection laws have been passed across the country, providing for consumer access to their data and the ability to correct, delete, and limit processing of that data.[170] These laws and proposals go a long way in granting people access to and control over their own personal information, in addition to protecting against compelled disclosure of health care providers' medical records. The laws do not, however, constrict the ability of a litigant to seek information as part of a lawsuit if it is relevant. These developments warrant fresh analysis of discovery culture and its place in the US legal system.

III. WHY INVASIVE DISCOVERY PERSISTS

A. Discovery As Part of the System

The liberal nature of the US discovery rules is more than just a matter of their words. As Professor Geoffrey Hazard has noted, other common law countries have similar definitions of the scope of discovery.[171] Where the US rules diverge is in their interpretation, which is itself affected by liberal pleading rules,[172] the jury system,[173] and high standards for obtaining summary judgment.[174] Notably, *Conley v. Gibson*'s broad pleading standard has been supplanted by a plausibility standard articulated in *Iqbal* and *Twombly*.[175] While this development may affect the ability to obtain early dismissal in certain contexts, it will likely take more than a stricter pleading standard to

169. HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (Apr. 17, 2023) (to be codified at 45 C.F.R. § 160).

170. Theodore Augustinos, Alexander Cox & Brianna Dally, *U.S. State Privacy Laws: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, Virginia*, JD SUPRA (Dec. 12, 2023), https://www.jdsupra.com/legalnews/u-s-state-privacy-laws-california-4777943 [perma.cc/4HHB-TDAQ].

171. *See* Hazard, *Secrets*, *supra* note 81, at 1678.

172. *See* Samuel H. Rifkind, *Are We Asking Too Much of Our Courts?*, 15 JUDGES J. 43, 49 (1976) (tracing problems in discovery to "the liberalized requirements of pleading, heralded at the beginning of this century, which reduced the requirements of the petition and left for discovery the opportunity to define the facts and issues").

173. *See* Hazard, *Secrets*, *supra* note 81, at 1691.

174. *See* John Swanson, *Privacy Limitations on Civil Discovery in Federal and California Practice*, 17 PAC. L.J. 1, 7 (1985) (discussing recent developments in privacy law, including the Supreme Court's recognition of its constitutional status, and arguing that discovery should be reevaluated as well).

175. *See* George Shepherd, *Still a Failure: Broad Pretrial Discovery and the Superficial 2015 Amendments*, 51 AKRON L. REV. 817, 830–32 (2017); *Failed Experiment*, *supra* note 26, at 478.

change the ingrained belief in the desirability of broad discovery—what some have referred to as a "quasi-constitutional" institution.[176]

Professor Richard Marcus notes that broad discovery is a foundation for the efficient functioning of the US civil justice system.[177] Discovery is seen as essential to effective settlement discussions.[178] The party-driven nature of discovery is central to enabling overburdened court systems to manage cases.[179] Finally, the ability to obtain information through discovery is inherent in "satisfaction with the litigation process itself."[180]

In a more cynical view, the enduring discovery scope benefits the players who would otherwise be tasked with changing it. Professor George Shepherd has described the discovery rules as "a seventy-year experiment that has failed."[181] Broad discovery shifted the emphasis from trial to pretrial procedure and ushered in the billable hour.[182] Despite its revolutionary cost and harm, the system has not been changed due to the fact that "lawyers often benefit from discovery because it increases their incomes."[183] Indeed, Professor Subrin finds that lawyers' self-interest was part of the reason the broad discovery rules were adopted in the first instance:

> None of the most important legal constituencies had much to lose from the broad discovery provisions; in fact they had a good deal to gain. For lawyers the new Federal Rules generally, and broadened discovery in particular, opened new horizons. Plaintiffs' and defendants' lawyers had the ability to create new theories and defenses and to engage in extensive discovery, for which at least some of them would be paid by the hour.[184]

B. Cultural Views of Privacy

Scholars have also noted differences in attitudes toward privacy in the United States and other countries, a "cultural divide" where "protections of privacy are taken more seriously on the Continent than

---

176. *See Retooling American, supra* note 107, at 190–91, citing Geoffrey C. Hazard, *Discovery and the Role of the Judge in Civil Law Jurisdictions*, 73 NOTRE DAME L. REV. 1017, 1024 (1998).

177. *Id.* at 194.

178. *Id.*

179. *See id.* at 195.

180. *Id.* at 193–96.

181. *Failed Experiment*, *supra* note 26, at 466.

182. *See* George B. Shepherd & Morgan Cloud, *Time and Money: Discovery Leads to Hourly Billing*, 1999 U. ILL. L. REV. 91, 163 (1999) ("The expansion of discovery in the 1938 Federal Rules of Civil Procedure played a substantial role in leading the legal profession to switch from fixed-fee billing to hourly billing for all but contingency cases.").

183. *Failed Experiment*, *supra* note 26, at 481.

184. *Fishing Expeditions*, *supra* note 35, at 741.

in America, at least where civil proceedings are concerned."[185] In particular, the US legal system places much less importance on the confidentiality of business documents than its European counterparts.[186] Professor James Whitman has described the attitude of Americans toward privacy as driven by the concept of liberty, largely construed as liberty from the state.[187] In contrast, the European tradition views privacy as akin to "dignity."[188] This is consistent with US suspicion of document searches by the government and a strong belief in Fourth Amendment protection but little concern for private litigant discovery requests (even when coupled with government enforcement).[189]

The differences between US litigation and that in other countries produces a great deal of friction when foreigners encounter US discovery.[190] As Professor Hazard describes, document discovery in other countries "goes after what public and private officials regard as their most private thoughts, such that this kind of discovery, to them, resembles self-incrimination."[191] As the European Union in particular has tightened data privacy laws, the issue of US authorities conducting discovery of data residing outside the country has become a problem for litigants and for US business as well: "American law allows parties to rummage around in each other's records in a way that seems obnoxious and manifestly unacceptable to Europeans. The result, in recent decades, has been a seething little war over discovery."[192] The United States alone allows the invasive gathering of documents as a matter of course in litigation.

---

185. *Retooling American*, *supra* note 107, at 193; *see also* WESTIN, *supra* note 29, at 30.

186. *See Retooling American*, *supra* note 107, at 162 ("The European solicitude for the confidentiality of business information is particularly perplexing to Americans, for the debate in this country is whether such information is even eligible for a protective order which limits its use to the litigation at hand.").

187. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004) ("America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home.").

188. *See id.*

189. *See id.* at 1214.

190. *See* RESTATEMENT (THIRD) OF FOREIGN RELS. § 442 reporters' note 1 (1987) ("No aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction as the requests for documents in investigation and litigation in the United States."); *see* Karen A. Feagle, *Extraterritorial Discovery: A Social Contract Perspective*, 7 DUKE J. COMP. & INT'L L. 297, 299 (1997).

191. Hazard, *Secrets*, *supra* note 81, at 1675–76.

192. Whitman, *supra* note 188, at 1157.

C. The System Works?

While this Article criticizes the lax protection of privacy in civil discovery as compared to Fourth Amendment limitations on government searches, an argument exists that civil discovery requirements are at least as onerous as a criminal warrant's "reasonableness" test.[193] Admittedly, the stakes in civil disputes are lower than in criminal actions. In addition, many believe the use of protective orders and confidentiality provisions is sufficient protection for privacy.[194] Certainly, many decisions show that judges thoughtfully weigh privacy rights against the need for discovery under Rule 26(c).[195] Those decisions are part of a strong body of case law drawing on federal and state constitutional principles, legislation, and other persuasive sources to protect a variety of privacy interests in litigation.[196] But the fact remains that litigants are not required to make any showing of reasonableness prior to making discovery requests.[197] There is no particularity requirement as there is for a search warrant. Litigants continue to feel emboldened to make overbroad requests, leading to the cost and delay motions practice entails.[198] When motions practice ensues, judges have broad discretion to make discovery rulings and such decisions are typically unappealable until the case is over, when they are likely moot or harmless error.[199] Moreover, protective orders

193. *See* United States v. Int'l Bus. Mach. Corp., 83 F.R.D. 97, 103–04 (S.D.N.Y. 1979) (finding that, in the context of subpoenas issued in a civil antitrust case, "the fourth amendment if applicable would hold subpoenas in civil litigation to a standard of reasonableness no more rigorous than that imposed by rule 45(b)").

194. *See* Lee H. Rosenthal & Steven S. Gensler, *Proportionality and Privacy: The Privacy-Protection Hook in the Federal Rules*, 105 JUDICATURE 77, 78 (2021) ("Rule 26(c): The privacy hook we've been using and why it works").

195. *See* Lawson v. Love's Travel Stops & Country Stores, Inc., 2020 WL 109654, Civ. No. 1:17-CV-1266 (M.D. Pa. Jan. 9, 2020) (rejecting the plaintiffs' "invitation to require some sort of wholesale disclosure of a wide array of cellphone data," although it recognized that "a more narrowly tailored request, supported by a more specific showing of relevance, might be appropriate").

196. *See Modern Discovery*, *supra* note 9, at 678–84, 685–702.

197. *See* Bedora A. Sheronick, *Rock, Scissors, Paper: The Federal Rule 26(a)(1) "Gamble" in Iowa*, 80 IOWA L. REV. 363, 376 (1995).

198. *See* William K. Thayer, *"Will 'Discovery' Invade My Right to Privacy?"*, SCHAUERMANN THAYER INJ. L. (Apr. 1, 2019), https://www.stlaw.com/will-discovery-invade-my-right-to-privacy/ [perma.cc/34PA-DZNR] (warning potential personal injury plaintiffs that they may be required to answer questions about their "marital status . . . work history and current employment, criminal convictions, drug and alcohol history and usage, mental health issues, prior medical conditions" and may be required to "produce employment records, applications for jobs, personnel files, school records," transcripts, and tax returns).

199. Federal courts of appeal have jurisdiction over appeals from final decisions of district courts, 28 U.S.C. § 1291, or interlocutory decisions not applicable to discovery. 28 U.S.C. § 1292.

evoke serious and growing problems even when courts provide protection, as this Article describes next.

IV. PROTECTIVE ORDERS ARE NOT SUFFICIENT

Traditionally, protective orders under Rule 26(c) have been the mechanism by which litigants enforce privacy protections against improper discovery requests.[200] That Rule allows a court, "for good cause," to forbid, limit, seal, or otherwise protect against disclosure "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense."[201] To a lesser extent, confidentiality agreements have given litigants some comfort about the protection of sensitive information. For reasons both practical and substantive, however, these devices are insufficient to protect privacy.

A. Harm from Discovery: Loss of Autonomy and Deterrence from Litigation

As a limit that parties must seek affirmatively and for "good cause," protective orders are inadequate to safeguard against much of the harm invasive discovery requests perpetuate.[202] Instead, some harm already occurs if private information is viewed as discoverable in the first place. Violations of privacy are often difficult to articulate in concrete terms. Professors Daniel Solove and Danielle Citron have constructed a helpful typology of privacy harms, including harms to autonomy: "restricting, undermining, inhibiting, or unduly influencing people's choices."[203] Two of the autonomy harms they describe apply directly to lack of privacy in discovery: lack of control, or "the inability to make meaningful choices about one's data or prevent the potential future misuse of it;" and "chilling effects," or the act of "inhibiting people from engaging in lawful activities."[204]

The reason for the Supreme Court's jurisdiction to review the discovery ordered in *Hickman v. Taylor* was that the lawyer had been ordered jailed for contempt of court. 329 U.S. 495, 501 (1947).

200. *See* Hon. James C. Francis IV, *Good Intentions Gone Awry: Privacy as Proportionality Under Rule 26(b)(1)*, 59 SAN DIEGO L. REV. 397, 401–09 (2022); Rosenthal & Gensler, *supra* note 194, at 78–79.

201. FED. R. CIV. P. 26(c).

202. *See* Christopher Schon, *Protecting Your Client by Way of a Protective Order*, TYSON & MENDES (Oct. 5, 2020), https://www.tysonmendes.com/protecting-your-client-by-way-of-a-protective-order/ [perma.cc/TZ2J-W6CN].

203. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 BOSTON U. L. REV. 793, 845 (2022).

204. Citron & Solove, *supra* note 203, at 846.

Discovery takes away individuals' control over their data. Many communications that would be considered confidential are thus rendered fully discoverable. It has become commonplace for internal corporate emails or texts to become the key to prevailing in litigation.[205] While not a subject for much sympathy, the discovery of embarrassing internal communications is still a reason to question the system. As Professor Shepherd puts it:

> Something important is lost when private individuals may not communicate in private without the constant threat that government agents – and that is what the courts are—will listen in. If everyone were not so accustomed to discovery's intrusiveness, everyone would see more clearly that the discovery process brings the United States frighteningly close to the world in Orwell's 1984. Only here, Big Brother is a court enforcing an order compelling discovery.[206]

The concern for free communication was at the heart of the Supreme Court's decision in *Jaffee v. Redmond*, where it found that conversations between a party and her therapist, including the notes from their counseling sessions, were protected from compelled disclosure.[207] Free communication was also important to the Court in *Hickman*, when it noted that "it is essential that a lawyer work with a certain degree of privacy," and that if a lawyer were required to produce his work product "to opposing counsel on mere demand, much of what is now put down in writing would remain unwritten."[208]

The reversal of the constitutional right to privacy recognized in *Roe* makes reproductive health information particularly vulnerable to abuse.[209] Social media, internet search history, smartphone apps, and wearable devices are only part of the vast repository of biometric information that can be used to subject a person to civil and criminal sanction.[210] Individual autonomy over that information is more

---

205. *E.g.*, Zubulake v. U.B.S. Warburg, LLC., 229 F.R.D. 422 (S.D.N.Y. 2004) (discussing sanctions for deletion of internal emails relevant to plaintiff's claims of gender discrimination); U.S. Dominion, Inc. v. Fox News Network, LLC., Case No. N21C-03-257 EMD *1022, 1027 (2023) (in defamation case, text messages revealed that news anchors did not believe the allegations of election fraud reported on the network).

206. *Failed Experiment*, *supra* note 26, at 490.

207. Jaffee v. Redmond, 518 U.S. 1, 18 (1996).

208. Hickman v. Taylor, 329 U.S. 495, 511 (1947).

209. *See* Linda C. McClain, *The Poverty of Privacy?*, 3 COLUM. J. GENDER & L. 119, 154 (1992).

210. *See* Aziz Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-*Roe *Era*, N.Y.U. L. REV. Vol. 97 (forthcoming 2023) (discussing data traces of search information regarding reproductive choice).

important than ever given *Dobbs* and the passage of abortion bans in over a dozen states.[211]

Additionally, potential privacy violations have chilling effects in that they may act as a deterrent to litigants.[212] In *Seattle Times v. Rhinehart*, the Supreme Court recognized the potential for "abuse that can attend the coerced production of information," as discovery may be used for improper purposes like harassment or coercing a favorable settlement.[213] Litigation can thus be chilled, noted the Court, as, "rather than expose themselves to unwanted publicity, individuals may well forgo the pursuit of their just claims . . . resulting in frustration of a right as valuable as that of speech itself."[214]

Courts have more recently acknowledged these chilling effects in the context of broad social media requests.[215] Such requests could reveal information that is "extremely personal and embarrassing," running the "substantial risk that the fear of humiliation and embarrassment will dissuade injured plaintiffs from seeking recovery for legitimate damages or abandon legitimate claims."[216] Importantly, courts recognize that even a confidentiality agreement would not "abate the chilling effect of [private] disclosure."[217]

These risks make it crucial that discovery culture not condone reckless requests that implicate confidential information, particularly

---

211. *See* Carter Sherman & Andrew Witherspoon, *Abortion Rights Across the US: We Track Where Laws Stand in Every State*, THE GUARDIAN (Jan. 12, 2024, 2:23 PM), https://www.theguardian.com/us-news/ng-interactive/2023/nov/10/state-abortion-laws-us [perma.cc/DCS9-JBT4].

212. *See* Richard L. Marcus, *The Discovery Confidentiality Controversy*, 1991 U. ILL. L. REV. 457, 486 (1991) ("The reason Dalkon Shield claimants have proven to be more numerous than expected is that many originally chose not to sue to protect their privacy. Indeed, given the availability of intimate information about plaintiffs through discovery in personal injury cases, there may even be reason to suspect that defendants would seek to exploit this concern."); *Failed Experiment*, *supra* note 26, at 485 (noting that potential tobacco plaintiffs would not sue "because they foresaw the discovery barrage that the tobacco companies and their legions of lawyers would throw at them if they did").

213. Seattle Times v. Rhinehart, 467 U.S. 20, 34–35 (1984).

214. *Id.* at 36 n.22 (quoting Seattle Times Co. v. Rhinehart, 654 P.2d 673, 689 (Wash. 1982)).

215. *E.g.*, Gordon v. T.G.R. Logistics, Inc., 321 F.R.D. 401 (D. Wyo. 2017).

216. *Id.* at 403–04; *see also* Guillen v. B.J.C.R. LLC., 341 F.R.D. 61, 71 (D. Nev. 2022) (denying employer's request for plaintiff's immigration information in Fair Labor Standards Act case including birth certificates, medical records, and bills related to minor children) ("[R]equiring disclosure of these documents would surely have an intimidating or in terrorem effect on individuals outside this litigation, and would discourage them from raising these claims in the future.").

217. Rengifo v. Erevos Enters., 2007 U.S. Dist. LEXIS 19928 at *3 (S.D.N.Y. Mar. 20, 2007) (denying discovery of immigration status and social security number in the context of plaintiff's labor law claims) ("[The] in terrorem effect of inquiring into a party's immigration status and authorization to work in this country when irrelevant to any materials claim because it presents a danger of intimidation that would inhibit plaintiffs in pursuing their rights.").

reproductive health and sexual history. Changing the ingrained discovery mindset requires a greater alteration to the Rules and stronger protection than merely the discretion of the trial court in motions practice.

B. Limiting Dissemination Is Not Enough

If protection is only available as a check on production or further dissemination of private information, privacy violations occur regardless. As Professors Robert Keeling and Ray Mangum discuss,[218] privacy violations can occur throughout the preservation and collection processes. Even if the other party never sees the discovery, "private personal information inevitably will be preserved and later swept up during the collection process," including "not only personally identifiable information such as social security numbers and credit card information, but also more intimate and potentially embarrassing details, including everything from vacation photos to medical records."[219] At the collection stage, having multiple copies of data in multiple locations, like removable media, file shares, and staging locations, "increases the risk of improper exposure, whether purposeful or inadvertent."[220] Finally, in the review stage of large ESI cases, "dozens or even hundreds of lawyers, including contract lawyers retained solely for the purpose of review, will read and classify the collected materials," which is itself intrusive.[221]

In addition, when a protective order allows discovery but places limits on further dissemination—such as an Attorneys' Eyes Only designation, or an order for production under seal—is subject to

---

218. "Privacy considerations, therefore, are relevant from the outset – even when initially identifying the custodians, data sources, and time period likely to contain relevant information." Robert D. Keeling & Ray Magnum, *The Burden of Privacy in Discovery*, 105 DUKE U. JUDICATURE 67, 71 (2021).

219. *Id.* ("The more custodians, the broader the time period, and the more personal the data sources – especially chat systems, social media, and mobile devices – the more personal information will be potentially implicated downstream as a consequence. Moreover, such communications will very often involve numerous third parties, potentially implicating their privacy interests as well under both the Federal Rules and newer regulatory regimes such as GDPR and CCPA.").

220. *Id.* (quoting John B. v. Goetz, 531 F.3d 448, 457 (6th Cir. 2008) ("ESI productions in civil litigations can be ripe targets for corporate espionage and data breach as they may contain trade secrets and other proprietary business information; highly sensitive and private medical, health, financial, religious, sexual preference, and other personal information; or information about third parties subject to contractual confidentiality agreements.")).

221. *Id.* at 73 ("Sharing sensitive information – especially regarding intimate personal, medical, religious or financial matters – to a large group of people is a substantial burden, even if that information goes no further.").

inadvertent disclosure.[222] Once a document is produced in the case, "the producing party's control over that information is dramatically limited and the risk of disclosure heightened."[223] In the high-profile Alex Jones defamation case, his lawyers inadvertently produced to his opponents text messages they had requested but also medical, psychological, and other files, even including a nude photograph of his wife.[224] In another case of mistaken disclosure, a criminal warrant issued to Apple that should have been filed on Pacer under seal was instead fully viewable.[225] A similar error occurred when the confidential Privilege Review Team Report prepared by the Department of Justice in its case against Donald Trump was filed under seal but was not kept from public view.[226] Two separate bankruptcy cases involving the Roman Catholic Diocese have failed to protect the identity of anonymous victim claimants despite confidentiality orders.[227] Human error must factor into any consideration of the protections imposed on discovery. Moreover, courts have recognized that even de-identified data can reveal personal information.[228] Those problems can be "particularly acute when the information produced has value outside of the

---

222. *See* Adjoa Linzy, *The Attorney-Client Privilege and Discovery of Electronically-Stored Information*, 10 DUKE L. & TECH. REV. 1, 23 (Feb. 24, 2011).

223. Keeling & Magnum, *supra* note 218, at 73 (citing John B. v. Goetz, 531 F.3d 448, 458 (6th Cir. 2008)).

224. Ramon Antonio Vargas, *Alex Jones Sent Nude Photo of Wife to Roger Stone, Sandy Hook Lawyer Reveals*, THE GUARDIAN (Aug. 9, 2022, 10:16 AM), https://www.theguardian.com/us-news/2022/aug/09/alex-jones-nude-photo-wife-roger-stone [perma.cc/27D8-KJA3]; Debra Cassens Weiss, *'Probably the Worst Day of My Legal Career,' Says Lawyer for Infowars Founder in Testimony on Mistaken Revelations*, ABA J. (Aug. 29, 2022, 11:30 AM), https://www.abajournal.com/news/article/probably-the-worst-day-of-my-legal-career-lawyer-for-infowars-founder-testifies-on-mistaken-revelations/ [perma.cc/5ZNP-3MDX].

225. Ralph Losey, *Examining a Leaked Criminal Warrant for Apple iCloud Data in a High Profile Case – Part One*, EDRM BLOG (June 14, 2022), https://edrm.net/2022/06/examining-a-leaked-criminal-warrant-for-apple-icloud-data-in-a-high-profile-case-part-one/ [perma.cc/H2VZ-KT2Q].

226. Ralph Losey, *DOJ's Confidential Report Leaked in* Trump v. U.S., E-DISCOVERY TEAM (Oct. 5, 2022), https://e-discoveryteam.com/2022/10/05/dojs-confidential-report-leaked-in-trump-v-u-s/ [perma.cc/X3QX-KXF4].

227. Conor Wright, *Information of 101 Survivors Possibly Exposed in Syracuse Diocese Bankruptcy Case*, CNY CENT. NEWS (Oct. 5, 2023, 2:52 PM), https://cnycentral.com/news/local/information-of-101-survivors-possibly-exposed-in-syracuse-diocese-bankruptcy-case [perma.cc/N6SW-5LBK]; Greg Smith, *Church Abuse Victims File $42 Million Suit Against Bankruptcy Firm for Publishing Their Names*, THE DAY (Feb. 9, 2023), https://www.yahoo.com/news/church-abuse-victims-file-42-013300616.html [perma.cc/EL6M-88A3].

228. *See* Cnty. of Los Angeles v. Superior Court, 6 Cal. App. 5th 621, 648–52 (Ct. App. 2021) (discussing privacy rights of patients in de-identified data, including the possibility of reidentification); Pac. Radiation Oncology, LLC. v. Queen's Med. Ctr., 138 Haw. 14 (2016) (state constitution protects individuals from production of their medical information even when de-identified).

litigation."[229] One court has recognized the danger that information produced pursuant to a protective order may nonetheless be disclosed, choosing to deny disclosure rather than risk inadvertent exposure of nonparties' financial data.[230]

C. Protective Orders May Be Modified

Finally, a protective order can be challenged not only by parties but also by nonparties seeking to intervene, or by anyone after the litigation has concluded.[231] Even the press has been successful in intervening to obtain sensitive discovery material, like trade secrets.[232] The possibility of subsequent modification is "the most significant vulnerability in current protective order practice."[233] One district court went as far as to reject a stipulated protective order because of the "false sense of protection that [producing parties] might innocently, but wrongly, rely upon when releasing information."[234] Like the initial decision to grant a protective order, the decision whether to modify a protective order, even long after trial or settlement, is ultimately subject to the trial court's discretion.[235] Courts may exercise that discretion differently across jurisdictions.[236]

For instance, in *Simon v. Northwestern University*, a case arising out of allegations that the defendants' unethical journalism practices led to the plaintiff's wrongful conviction for a double murder, the court had entered a protective order providing for the confidentiality of pretrial disclosures.[237] The agreement gave the parties confidence that

---

229. Keeling & Magnum, *supra* note 218, at 73 (citing Zyprexa litigation incident in which millions of documents that were sealed under a protective order were obtained and disclosed to the public); William G. Childs, *When the Bell Can't Be Unrung: Document Leaks and Protective Orders in Mass Tort Litigation*, 27 REV. LITIG. 565, 578–97 (2008).

230. *See* Marcus, *supra* note 212, at 506 (citing Litton Indus. v. Chesapeake & Ohio Ry. Co., 129 F.R.D. 528, 531 (E.D. Wis. 1990) ("There is a constant danger in disclosure of confidential information pursuant to a protective order. Therefore, the party requesting disclosure must make a strong showing of need, especially when confidential information from a nonparty is sought.")).

231. Howard M. Erichson, *Court-Ordered Confidentiality in Discovery*, 81 CHI.-KENT L. REV. 357, 370 (2006).

232. *Id.*

233. *Id.*

234. *Id.*

235. *See* Marcus, *supra* note 212, at 506 n.156 (citing Wyeth Labs. v. United States District Court, 851 F.2d 321 (10th Cir. 1988)). The Court of Appeals upheld a decision to vacate a protective order after a jury trial, noting that "the materials were no longer confidential given the disclosures that had happened at the trial." *Wyeth Labs.*, 851 F.2d at 322–23.

236. *See* Cooper, *supra* note 44, at 783; discussion accompanying notes 35–37, 40–41.

237. Simon v. Northwestern Univ. (*Simon II*), Case No. 1:15-cv-01433 (N.D. Ill. Nov. 15, 2018); *see* Simon v. Nw. Univ. (*Simon I*), 175 F. Supp. 3d 973, 976 (N.D. Ill. 2016).

materials produced by parties and nonparties alike would not be disclosed other than for purposes of the litigation.[238] The parties were able to settle the matter without the court ruling on any motions requiring the publication of discovery.[239] Three years later, a party to the litigation sought to lift the protective order and unseal certain filings.[240] In a thoughtful ruling, the court denied the motion.[241] It noted the protective order had helped facilitate discovery and the settlement; undoing the protection would conflict with the parties' reliance on confidentiality, and "would disturb the finality of the matter and the parties' reasonable expectations of privacy."[242] This did not prevent the parties from being forced to litigate the issue years after the case had been settled, but the court here prevented any further erosion of the protective order's benefit.[243] This may not always happen; in fact, the court noted that its view of the privacy in pretrial proceedings is not one universally shared across jurisdictions.[244]

While protective orders give courts broad discretion to curtail unduly invasive discovery requests, they are not sufficient. As a measure that litigants must seek affirmatively, the availability of protective orders fail adequately to deter abusive discovery. When potential litigants must face the possibility that by bringing a claim they lose autonomy over personal information, they may choose not bring that claim at all. Moreover, protective orders are problematic precisely because of the discretion they grant judges, leaving litigants at the mercy of courts that may show less sympathy towards a privacy argument than in *Simon*. Finally, when courts order discovery but use protective orders to limit the dissemination of that discovery, a real risk persists that the safeguards will fail. A better solution confronts the problem at the front end by limiting the scope of discovery from the outset of a proceeding.

238. *Simon II*, at *2.
239. *Id.* at *4.
240. *Id.*
241. *Id.* at *2, *6.
242. *Id.* at *6.
243. *Id.* at *1.
244. *Id.* at n.3.

V. LIMITING SCOPE

A. Proportionality

As privacy in discovery has become a prominent issue, a number of judges and academics[245] have advocated viewing privacy as an aspect of proportionality under the revised Rule 26(b).[246] As discussed above, the 2015 revisions returned the proportionality factors to Rule 26(b)'s definition of the overall scope of discovery, urging parties to take into consideration, among other things, "whether the burden or expense of the proposed discovery outweighs its likely benefit."[247] Construing privacy as one such "burden" would allow the Rule to serve as a check on the scope of discovery rather than a subject of affirmative protection. Proponents of the privacy-as-proportionality theory argue that it is properly seen as one factor to be weighed along with the other factors in Rule 26(b)(1).[248] Opponents of that approach note that there is no indication that the drafters intended for courts to consider privacy in the proportionality test.[249] As such, opponents hold that allowing parties to make their own determination regarding whether materials should be subject to discovery based on privacy would invite abuse.[250]

An alternative to privacy as an implicit proportionality factor is explicit limitation on the scope of discovery. This could take the form of an additional proportionality factor, as set forth in the underlined portion here:

---

245. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Production*, 19 SEDONA CONF. J. 1, 128–29 (2018); The Sedona Conference, *Sedona Conference Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 27 (2019); Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 235 (2015); Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 CORNELL L. REV. 1101, 1103 (2018); Henson v. Turn, No. 15-CV-01497-JSW (LB), 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22, 2018); In re: Anthem, Inc. Data Breach Litig., No. 15-md-02617 LHK (NC), 2016 WL 11505231, at *1 (N.D. Cal. Apr. 8, 2016).

246. *See* McPeak, *supra* note 245, at 236, 287. "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and 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." FED. R. CIV. P. 26(b)(1).

247. FED. R. CIV. P. 26(b).

248. *See Sedona Conference Primer on Social Media, Second Edition*, *supra* note 245, at 27–28.

249. *See* Francis, *supra* note 200, at 430.

250. *See id.* ("[I]f privacy is considered an element in the very definition of discoverable evidence, a party anticipating litigation would be empowered to make a unilateral decision that private information is not discoverable and therefore may be destroyed even if it is potentially relevant to that litigation.").

> 26 (b) Discovery Scope and Limits.
>
> (1) Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and 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, privacy interests of the parties or of third parties, 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. Information within this scope of discovery need not be admissible in evidence to be discoverable.[251]

Some courts have already analyzed privacy as a proportionality factor.[252] In a decision from the Northern District of California, *Henson v. Turn, Inc.*, plaintiff subscribers to Verizon's cellular and data services brought a data privacy class action suit.[253] Plaintiffs alleged that Turn, a targeted advertisement business, illegally placed "zombie cookies" on users' devices to track their web browsing and use of applications to tailor advertisements to them.[254] Turn sought, among other things, all mobile devices plaintiffs had used during the class period to access the internet (or complete forensic images of the devices).[255] In denying the request for production of the phones, the court found the request called for information that was both irrelevant and disproportionate to the needs of the case.[256] As to relevance, the request threatened to reveal irrelevant information such as private communications, contact lists, and photographs.[257] As to proportionality, the court noted the growing number of cases and commentators that recognize privacy interests can be an important consideration in construing the proper scope of discovery, "particularly in the context of a request to inspect personal electronic devices."[258]

Another court considered a broad request by defendants in a motor vehicle accident for social media from the plaintiff, who sought damages based on physical injuries, traumatic brain injury, post-traumatic stress disorder, anxiety, and depression.[259] Tying its analysis to the proportionality requirement in Rule 26, the court denied

---

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

252. Henson v. Turn, Case No. 15-cv-01497-JSW (LG), 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22).

253. *Id.* at *1.

254. *Id.*

255. *Id.* at *3.

256. *Id.* at *5.

257. *Id.*

258. *Id.* (citing Tingle v. Herbert, No.15-626-JWD-EWD, 2018 WL 1726667, at *7–8 (M.D. La. Apr. 10, 2018)).

259. Gordon v. T.G.R. Logistics, Inc., 321 F.R.D. 401, 402 (D. Wyo. 2017).

discovery of the plaintiff's entire Facebook history, but ordered production of "relevant history which addresses Plaintiff's *significant* emotional turmoil, any mental disability or ability, or relate[s] *significant* events which could reasonably be expected to result in emotion distress."[260]

Aside from some cases properly limiting the scope of discovery where privacy is at risk, many courts have given thoughtful analysis to privacy interests in the context of protective orders.[261] These decisions too can serve instead as precedent for limiting the underlying scope of discovery.[262] In general, the greater the connection between the discovery and the "heart of the claim," the more likely the discovery is to be granted despite potential privacy concerns.[263] In contrast, when discovery is less connected to the claim, such as for purposes of credibility, the balance tips in favor of privacy and against disclosure.[264] Finally, as part of its balancing, a court should be careful to protect against discovery that implicates privacy of third parties.

B. Express Privacy Limitation

This Article proposes an alternative approach to protection that treats privacy, like work product, as a basis for withholding material from discovery unless a party can show substantial need.[265] This revised Rule would require a party to note the material withheld from discovery on a privilege log, divulging enough information to enable the opponent to challenge the protection. This would switch privacy from a protection that must be sought affirmatively to one that must be challenged affirmatively by the party seeking disclosure. This alternative solves

---

260. *Id.* at 406 (emphasis in original).

261. *See* Williams v. Superior Ct., 3 Cal. 5th 531, 539, 552 (2017); Tien v. Superior Ct., 139 Cal. App. 4th 528, 541 (2006).

262. *Modern Discovery*, *supra* note 9, at 710–12.

263. *See* Hedenburg v. Aramark Am. Food Servs., No. C06-5267, 2007 WL 162716, at *2 (W.D. Wash. Jan. 17) (denying production of plaintiff's home computer where defendant was "hoping blindly to find something useful in its impeachment of the plaintiff," as opposed to other cases "where the contents of the computer go to the heart of the case").

264. Antico v. Sindt Trucking, Inc., 148 So. 3d 163, 166–67 (Fla. Dist. Ct. App. 2014) (allowing narrowly tailored discovery of cell phone based on highly relevant issue of whether the decedent was texting at the time of the accident).

265. *See* Cooper v. Hallgarten & Co., 34 F.R.D. 482, 483–84 (S.D.N.Y. 1964) ("[T]he production of tax returns should not be ordered unless it clearly appears that they are relevant to the subject matter of the action or to the issued raised thereunder, and, further, that there is a compelling need therefore because the information contained therein is not otherwise readily obtainable."); New York Stock Exch., Inc. v. Sloan, 1976 WL 169086, at *3–4 (S.D.N.Y. Oct. 21, 1976) ("Where there is a strong policy behind non-disclosure, it is said that there must be 'a showing of exceptional necessity.").

Judge Francis' concern that litigants may secretly withhold private, relevant information under the guise of proportionality, since they must describe the withheld material.[266] This Article's proposed changes are underlined below:

> 26(b) Discovery Scope and Limits.
>
> (1) Scope in General. . . .
>
> (2) *Limitations on Frequency and Extent*. . . .
>
> (3) *Trial Preparation: Materials*. . . .
>
> (4) *Privacy Limitations*
>
> (A) Ordinarily, a party may not discover documents and ESI that is within a person's reasonable expectation of privacy. But, subject to Rule 26(b)(4), those materials may be discovered if:
>
> (i) they are otherwise discoverable under Rule 26(b)(1); and
>
> (ii) the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.
>
> (5) *Claiming Privilege or Protecting Trial-Preparation or Private Materials.*
>
> (A) *Information Withheld.* When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation or private material, the party must:
>
> (i) expressly make the claim; and
>
> (ii) describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.
>
> (B) *Information Produced.* If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation or private material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.[267]

Courts are accustomed to judging reasonable expectations of privacy in both the Fourth Amendment and torts contexts,[268] and some

266. *See* Francis, *supra* note 200, at 430.

267. *See* FED. R. CIV. P. 26(b)(3)–(5).

268. *See* Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 450 (D. Conn. 2009) (finding reasonable expectation of privacy in employee's email); United States v. Long, 64 M.J. 57, 64–65 (C.A.A.F. 2006) (same); United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007) (finding reasonable expectation of privacy in computer files).

have referred to such expectations in the discovery context.[269] These precedents can provide protection from overbroad, intrusive discovery requests, particularly where they impinge on reproduction and health information. As with requests for protective orders, private information will be more susceptible to disclosure the more closely connected it is to the parties' claims or defenses, as opposed to general relevance to credibility.[270]

C. Reasonable Expectations of Privacy in California Discovery

California courts in particular have used their state constitutional right to privacy to protect against intrusive discovery requests that implicate reasonable expectations of privacy.[271] That provision's "central concern" is to protect "informational privacy."[272] California courts construe their constitution to protect against disclosure of, among other things, sexual information;[273] marital information;[274] financial records;[275] tenure files and related discussions;[276] and nonparty contact information.[277] When the California constitutional right of privacy is involved, "the party seeking discovery must demonstrate a compelling need for discovery, and that compelling need must be so strong as to outweigh the privacy right when these two competing interests are carefully balanced."[278]

In one example, a California appellate court reversed an order compelling production of prescription data and patient records related to substance abuse treatment.[279] The court explained the importance of

---

269. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 970 (C.D. Cal. 2010).

270. *See supra* notes 261–64.

271. *See* Tien v. Superior Ct., 139 Cal. App. 4th 528, 539, 43 Cal. Rptr. 3d 121, 128 (2006). California's constitution provides that one of its people's "inalienable" rights is "pursuing and obtaining . . . privacy." CAL. CONST. art. I, § 1.

272. Bd. of Registered Nursing v. Superior Ct., 59 Cal. App. 5th 1011, 1039, 273 Cal. Rptr. 3d 889, 908 (2021).

273. *See Tien*, 139 Cal. App. 4th at 539.

274. Tylo v. Superior Ct., 55 Cal. App. 4th 1379, 1379, 64 Cal. Rptr. 2d 731, 731 (1997).

275. SCC Acquisitions, Inc. v. Superior Court, 243 Cal. App. 4th 741, 754 (2015).

276. *See* Kahn v. Superior Ct., 188 Cal. App. 3d 752, 752–771, 233 Cal. Rptr. 662, 662–74 (1987).

277. *See* Williams v. Superior Ct., 398 P.3d 69, 84 (Cal. 2017).

278. *Id.* at 86; *see also* Planned Parenthood Golden Gate v. Superior Court, 83 Cal. App. 4th 347, 359, 99 Cal. Rptr. 2d. 627, 637 (2000); Williams v. Superior Ct., 236 Cal. App. 4th 1151, 1151, 187 Cal. Rptr. 3d 321, 321 (Ct. App. 2015), *review granted and opinion superseded sub nom.* Williams v. S.C., 354 P.3d 301 (Cal. 2015), *and rev'd*, 3 Cal. 5th 531 (2017) ("A discovery proponent may demonstrate compelling need by establishing the discovery sought is directly relevant and essential to the fair resolution of the underlying lawsuit.").

279. 65 Cal. App. 5th 621, 626, 280 Cal. Rptr. 3d 85, 91 (2021).

privacy in medical records, which "may include descriptions of symptoms, family history, diagnoses, test results, and other intimate details concerning treatment."[280] Unauthorized disclosure of such files, particularly of nonparties, "can provoke more than just simple humiliation in a fragile personality" since the privacy right "encompasses not only the state of his mind, but also his viscera, detailed complaints of physical ills, and their emotional overtones."[281]

An earlier California case involved an actress's suit for wrongful termination after becoming pregnant.[282] The appellate court reversed the trial court's order that she answer questions concerning emotional distress related to her marital relationship.[283] Likening plaintiff's right to privacy in her marital relations to the psychiatric privilege, the court found that a compelling interest in disclosure "is demonstrated only where the material sought is *directly relevant* to the litigation."[284] Careful balancing is required when the right to discovery conflicts with constitutionally protected information, which the court likened to privileged information and its heightened protection.[285]

In a more modern version of a dispute like that in *Tylo*, an employer would likely seek not only answers to deposition questions probing the plaintiff's marital relationship and pregnancy, but all manner of communications with friends and family as well as biometric and other data from devices.[286] If the case were brought in a state with no constitutional right to privacy, the plaintiff would struggle to show any post-*Dobbs* constitutional protection for the information. The proposed rule would place the burden on the employer to show that its substantial need for the material outweighs plaintiff's legitimate interest in privacy. This higher level of protection would help ensure that discovery centers on documents the parties would use at trial rather than information designed to embarrass, oppress, or deter litigation. Such an outcome would be consistent with the goal of the rules "to secure the just, speedy, and inexpensive determination of every action and proceeding."[287]

---

280. *Id.* at 103.

281. *Id.*

282. Tylo v. Superior Ct., 55 Cal. App. 4th 1379, 1379, 64 Cal. Rptr. 2d 731, 731 (1997).

283. *Id.* The court found the plaintiff may have put her psychological condition in issue by seeking damages for emotional distress, but that waiver of privacy only extended to discovery as to injuries directly from the termination. *Id.*

284. *Id.* at 1387 (emphasis in original).

285. *Id.*

286. *See id.* at 1379, 1387; *Modern Discovery*, *supra* note 9, at 710–12.

287. FED. R. CIV. P. 1.

VI. CONCLUSION

The revolution of the 1938 Rules was intended to eliminate gamesmanship before trial by making available to all parties the relevant facts underlying the claim. Subsequent amendments sought to reduce the time and expense incurred in broad discovery, particularly considering the information explosion and emergence of pervasive surveillance culture. Along the way, technology has fundamentally altered discovery, exponentially increasing the facts in existence as texts and tweets replace face to face interactions, and devices continually gather and store data. It is impossible for the parties to have all facts that arguably fit the Rules' broad definition of relevance. In addition, the nature of the information that is created now is unprecedented. Data is created every second through constant communications as well as automatically by omnipresent devices. Fourth Amendment doctrine has evolved concurrently with this technology, recognizing that search and seizure need not entail physical trespass, and that protection should not be vitiated because of necessary third-party access to data.

The law has never treated civil discovery as bound by the Fourth Amendment, and the scope of the Rules has not narrowed to account for the privacy invasions inherent in requests. Lower courts have attempted to guard against privacy violations via protective orders, basing their rulings on persuasive privacy law, including constitutional law. Now, a majority of the Supreme Court does not believe in a constitutional right to privacy under the US Due Process Clause. This implicates discovery requests that could reveal all manner of issues including health, reproduction, contraception, sexuality, and gender identity. Rather than continuing with an extremely broad discovery system that requires affirmative efforts to avoid production of private information tangential to a case's merits, the Rules should carve out private information from the scope of what parties may seek. This is necessary to change the culture of discovery to one that presumptively protects against invasions of privacy.