RULES SUGGESTION
to the
ADVISORY COMMITTEE ON CIVIL RULES

FRCP AMENDMENTS ARE NEEDED TO GUIDE COURTS AND LITIGANTS IN PROACTIVELY MANAGING THEIR SHARED OBLIGATIONS TO PROTECT PRIVACY RIGHTS AND AVOID ATTENDANT CYBER SECURITY RISKS

September 19, 2023

Lawyers for Civil Justice ("LCJ")[1] respectfully submits this Rules Suggestion to the Advisory Committee on Civil Rules ("Advisory Committee").

BACKGROUND

As a result of the massive expansion in the amount and ubiquity of personal information[2] stored across smart phones, cloud services, corporate databases, social media, and the internet-enabled devices, courts, litigants, and non-parties face a recurring quagmire in balancing their obligation to protect the privacy rights enshrined in the Constitution[3] and defined by many statutes and

[1] Lawyers for Civil Justice ("LCJ") is a national coalition of corporations, law firms, and defense trial lawyer organizations that promotes excellence and fairness in the civil justice system to secure the just, speedy, and inexpensive determination of civil cases. For over 35 years, LCJ has been closely engaged in reforming federal procedural rules to: (1) promote balance and fairness in the civil justice system; (2) reduce costs and burdens associated with litigation; and (3) advance predictability and efficiency in litigation.

[2] As used herein, the term "personal information," includes any information considered "personally identifiable information," "personal data," or "protected health information," as well as any other information over which a person may have a reasonable expectation of privacy. The term "confidential information" describes any confidential or proprietary information such as trade secrets, sensitive commercial information, or other information subject to a confidentiality agreement whether or not it contains personal information.

[3] *See* Allyson Haynes Stuart, *A Right to Privacy for Modern Discovery*, 29 GEO. MASON L. REV. 675, 718-19 (2022) ("Stuart") ("[P]rivacy rights in discovery are protected by the Constitution when requests touch on personal, intimate matters, or implicate rights to association like donor or membership lists, and are protected by public policy when they implicate state or federal statutory confidentiality provisions."); *see also*, *Whalen v. Roe*, 429 U.S. 589, 599 (1977) (a privacy interest exists in "avoiding disclosure of personal matters"); *Seattle Times Co. v. Rhinehart*,

regulations[4] with the needs of particular cases.[5] As one commentary explains: "The pressures to balance our commitment to broad discovery with escalating privacy risks are already intense and continue to build."[6]

Unfortunately, the Federal Rules of Civil Procedure ("FRCP") fail to provide the needed structure and guidance[7] for proactively considering, avoiding, and managing the complications that arise in most civil law suits related to privacy rights and reasonable expectations, including as to the unique and pervasive personal information that is generated and stored in today's

---

467 U.S. 20, 34-35 (1984) ("It is clear from experience that pretrial discovery by depositions and interrogatories has a significant potential for abuse. This abuse is not limited to matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties." (footnote omitted)); *Nat'l Ass'n for Advancement of Colored People v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 462 (1958) (Discovery order compelling "disclosure of membership in an organization engaged in advocacy of particular beliefs" violates Due Process); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457 (1977) (acknowledging privacy interest in "'avoiding disclosure of personal matters'"); and *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965) ("the First Amendment has a penumbra where privacy is protected from governmental intrusion.").

[4] For applicable state privacy laws, *see* Int'l Ass'n of Priv. Pros., *U.S. State Privacy Legislation Tracker*, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf (last updated July 28, 2023). For state blocking statutes, *see Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa*, 482 U.S. 522, 544 n.28 (1987) *and* David Yerich et al., *Data Privacy Laws and Blocking Statutes: Five Practical Strategies for Counsel*, JD SUPRA (Jan. 30, 2023), https://www.jdsupra.com/legalnews/data-privacy-laws-and-blocking-statutes-7485715/. For state biometric information laws, *see* Bryan Cave Leighton Paisner, *U.S. Biometric Laws & Pending Legislation Tracker*, BCLP: INSIGHTS (June 2, 2023), https://www.bclplaw.com/en-US/events-insights-news/us-biometric-laws-and-pending-legislation-tracker.html#:~:text=Biometric%20privacy%20laws%20and%20regulations,biometric%20information%20or%20biometric%20identifiers. For the General Data Protection Regulation (GDPR), *see* Eur. Union, *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Sept. 11, 2023). For SEC regulations requiring reporting of cybersecurity risks effective as of September 5, 2023, *see* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51,896 (Aug. 4, 2023) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240 and 249).

[5] *See, e.g.*, *Riley v. California*, 573 U.S. 373, 385-86, 393-97 & 403 (2014), for an extensive discussion and analysis by Chief Justice Roberts writing for the Court regarding the profound nature of changes in just the past few years affecting the amount of sensitive, private information that is now routinely stored and carried around by the average member of the public and the importance of considering the reality of these changes in daily life when courts adjudicate legal controversies. *See also*, *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (chastising the government's legal position for failing to account for "the seismic shifts in digital technology" storing personal information that has occurred over the past few years.).

[6] Steven S. Gensler & Lee H. Rosenthal, *The Privacy-Protection Hook in the Federal Rules*, 105 JUDICATURE 77, 78 (2021) ("Gensler & Rosenthal").

[7] Stuart, *supra* note 3, at 677 ("The Rules do not provide for explicit protection against discovery based on privacy, with the exception of redaction of personal information under Rule 5.2." (footnote omitted)).

technology such as in cell phones[8] (including BYOD devices),[9] social media,[10] GPS,[11] personal fitness trackers,[12] AirTags,[13] and the internet of things.[14] The word "privacy" appears only once in the FRCP—in the heading of Rule 5.2, which was written before the iPhone was introduced, and is a narrow provision limited to a discrete and outdated list of items such as social security numbers and bank account information to be redacted in paper records filed with the court.[15]

By default rather than design, the lone FRCP provision for handling privacy issues in civil litigation is Rule 26(c), which authorizes courts to issue protective orders but does not mention

---

[8] The Supreme Court in *Riley*, 573 U.S. at 394-95 explained:

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

[9] *See* Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 285 (2015) ("McPeak"):

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

[10] *See Id.* at 273 ("Needless to say, social media's popularity, functionality, and ubiquity has grown in unprecedented ways since 2006, and it is safe to assume that the ESI discovery amendments did not specifically consider social media and its unique ability to compile detailed personal information."); Stuart, *supra* note 3, at 707 ("Broad requests for social media content implicate privacy concerns because people often share 'the most intimate of personal details on a host of matters, many of which may be entirely unrelated to issues in specific litigation.'").

[11] *See United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about … familial, political, professional, religious, and sexual associations") *and* Stuart, *supra* note 3, at 725 ("Clearly, Supreme Court case law provides strong support for privacy rights in cell phones, GPS data, and cell site location information[.]").

[12] Stuart, *supra* note 3, at 710 ("Information from [personal activity] devices is now a regular part of form interrogatories and document requests.").

[13] *See* Kaitlin Balasaygun, *The Biggest Risks of Using Bluetooth Trackers Like Apple AirTag, Tile*, CNBC.com (Jan. 14, 2023), https://www.cnbc.com/2023/01/14/the-biggest-security-pros-and-cons-of-using-bluetooth-gps-trackers.html#:~:text=Apple%27s%20work%20with%20law%20enforcement,may%20have%20limited%20value%2C%20though.

[14] Stuart, *supra* note 3, at 713 ("It is only a matter of time before the explosion in IoT devices leads to regular civil discovery into smart speakers, smart home alarm systems, and smart home health monitors. Civil defense lawyers already tout the importance of discovery into virtual assistants like Alexa and Siri[.]").

[15] FED. R. CIV. P. 5.2 (rule limited to social security numbers, tax ID numbers, birth dates, financial account numbers, and identifying information of minors).

privacy or provide any tools for early, proactive management of privacy issues.[16] Although "[p]rotective orders are an important mechanism for protecting privacy,"[17] and the Supreme Court has acknowledged Rule 26(c)'s role in protecting privacy,[18] the rule is now ill-equipped to meet this critical need because protective orders are by nature reactive;[19] they do not furnish a structure for considering, avoiding, minimizing, or navigating around the complications of privacy interests and attendant cyber security risks.[20] Also, protective orders are resource-intensive for both courts and parties—they require a showing of "good cause" that can be inappropriate for information that is protected by law[21] (although some courts require discovery of private information be "clearly" relevant or that it go to the "heart of the case"[22]). Protective orders also are limited in effectiveness (particularly as to cyber security risks[23]) and rarely address the standards that should govern how information is stored, accessed, and protected by receiving entities. Further, protective orders are not reasonably accessible to non-parties who are often unaware of the potential risk of prejudice to their privacy rights and, therefore, not in a position to seek the court's protection.[24]

Civil litigation, and discovery in particular, *always* involves privacy considerations and accompanying data security risks.[25] The information that litigants reveal in pleadings, request in discovery, rely on for motions, and relate in court includes not only data that a party may regard as proprietary, but may also include information that is protected by law or that parties and non-

---

[16] The 1970 Committee Note to Rule 26(c) uses the word privacy only in relation to "trade secrets and other confidential commercial information."

[17] McPeak, *supra* note 9, at 272 n.268 (citing *Seattle Times Co.*, 467 U.S. at 31).

[18] *Seattle Times Co.*, 467 U.S. at 35 n.21 ("Although the Rule [26(c)] contains no specific reference to privacy or to other rights or interests that may be implicated, such matters are implicit in the broad purpose and language of the Rule.").

[19] Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 CORNELL L. REV. 1101, 1128 (2018)

("Boliek") ("Although courts have always had the authority, in practice, courts rarely limit discovery on privacy grounds on their own motion.").

[20] *Id.* at 1132 ("These orders are not foolproof, however, and cannot replace the initial gatekeeper role of the judge in granting discovery in the first instance.").

[21] *See* McPeak, *supra* note 9, at 256 ("The good cause standard requires particular facts demonstrating potential harm, and not on conclusory allegations. The party seeking the protective order must show a particular need for protection, rather than broad allegations of harm. Further, the harm must be significant." (footnotes omitted); Robert D. Keeling & Ray Mangum, *The Burden of Privacy in Discovery*, 105 JUDICATURE 67, 68 (2021), https://judicature.duke.edu/articles/the-burden-of-privacy-in-discovery/ ("Keeling & Mangum") ("Showing good cause was (and is) often difficult in contested matters.").

[22] *See* Stuart, *supra* note 3, at 699 nn. 171, 172.

[23] Boliek, *supra* note 19, at 1132, 1145 ("protective orders are effective only when the signatories comply with their parameters, and even then information can be misplaced or disclosed inadvertently" and "hackers are hitting well-known law firms—a reminder that a protective order does not protect data from outside threats" (footnote omitted)).

[24] *Id.* at 1137-38 ("third-party interests are difficult to defend in a court of law because of the cost of intervening in a court case").

[25] *Id.* at 1104 ("the undervaluation of the privacy interest (unnecessarily) increases cybersecurity risks").

parties consider private or confidential.[26] While most people understand that their bank, insurance company, health care provider, employer, favorite search engine, email provider, mobile App, or fitness tracker has information about them, few comprehend that a court or litigant could be required to provide their information to numerous entities or people involved in a lawsuit without the data subject's knowledge or consent. Nor do many people know that the content of their emails, text messages, financial information, or search queries can be requested and ordered to be shared with unknown entities involved in a civil lawsuit of which they are not aware—even if their information is putatively protected by privacy laws. In fact, it is now routine for parties to seek and produce significant amounts of data about non-party individuals—including customers, employees, suppliers, contractors, and members of the general public—without any notice to those individuals that their personal information or other material they consider private is being disclosed and used.[27]

Non-party information raises particularly difficult questions because the holders of such data likely have different interests than the people who are the subject of that data.[28] Moreover, privacy interests cannot be honored when cyber security risks are left unaddressed. Notwithstanding substantial investments by universities, corporations, and individuals of resources in state-of-the-art security to safeguard information technology systems (often required by federal and state regulations[29]), discovery frequently requires those entities to create copies of vast amounts (gigabytes and terabytes, even in small cases) of sensitive information and deliver that information into higher-risk environments that are non-compliant with even rudimentary cybersecurity practices, making it vulnerable to both negligent and purposeful exposure.[30] Increasingly sophisticated hackers, including foreign state actors, purposely target participants in

---

[26] *See* Gensler & Rosenthal, *supra* note 6, at 79 ("Parties often seek discovery of information that is intermingled with private information, including private information of or about nonparties to a lawsuit."); Stuart, *supra* note 3, at 705-06 ("[M]odern discovery goes far beyond what we consider typical documents and communications. Litigants increasingly focus on sources of discovery that have the capacity to reveal a great deal of information, much of it highly personal.").

[27] "Courts should apply higher limits still when private information is sought from or implicates the rights of third parties." Stuart, *supra* note 3, at 719.

[28] Boliek, *supra* note 19, at 1107:

> There are certainly times when sensitive information is *not* essential to a case, and a defendant … may simply agree to release information because it is easier or cheaper to hand over the data than to litigate the issue or redact the data. This is particularly true when the information at issue is about a third party, not about the information recipient (holder) itself. In economic terms, this is an example of misaligned interests. In other words, the defendant (the recipient of the information) may bear little cost by disclosing information to the plaintiff—costs of disclosure will be largely borne by the third party (the information provider). But, in contrast, the defendant may bear high costs if he or she fights against such disclosure. Unless the defendant internalizes the consequences the disclosure has on the information provider (e.g. public embarrassment, identity theft, loss of employment due to the exposure of the personal information, etc.) a private discovery agreement between the plaintiff and that defendant will never protect the third-party privacy interests.
>
> Add to this scenario the risk of cybersecurity breaches in the transfer, storage, and disposal of sensitive data, and the risks associated with an ill-conceived judicial order explode.

[29] *See, e.g.*, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51,896 (Aug. 4, 2023) (to be codified at 17 C.F.R. pts. 229, 232, 239, 240 and 249).

[30] Boliek, *supra* note 19, at 1133-34.

the U.S. civil justice system because litigation forces the assemblage and concentration of confidential information onto less secure platforms, which explains why frequent cyber-attacks are aimed at law firms,[31] ediscovery vendors, expert witnesses and U.S. courts. Indeed, some information is at risk only because of court decisions requiring discovery.[32]

As the Sedona Principles reflect, parties have a responsibility to "take reasonable steps" to protect personal and confidential information confidential.[33] Conforming the FRCP to this accepted standard means moving beyond protective orders as the sole implement and incorporating tools throughout the FRCP, as Professor Babette Boliek observes:

> To shore up the protective order for modern day realities, courts must first acknowledge that they cannot rely solely on the protective order of old to limit the inadvertent disclosure of sensitive information. A means to assure protection is to consider and weigh the affected parties' privacy interest at every step of the discovery process.[34]

The suggestions below and attached in the appendix propose a comprehensive examination of the FRCP to identify provisions that should be amended to establish a much-needed framework for courts and parties to navigate and protect privacy rights and prevent cyber security problems in civil litigation. Such issues arise throughout the litigation process, from case filing through to trial and beyond; the FRCP's prompts and instructions should be integrated throughout the rules.[35]

PROPOSALS

These proposals reflect that, while discovery is appropriately focused on truth-seeking, the current rules are no longer adequate for helping ensure that courts and parties balance their dual responsibilities to the case and to protecting parties and non-parties from the intrinsic risk that

---

[31] *See* Graham Cluley, *Oreo Maker Mondelez Staff Hit by Data Breach at Third-Party Law Firm*, BITDEFENDER (June 21, 2023), https://www.bitdefender.com/blog/hotforsecurity/oreo-maker-mondelez-staff-hit-by-data-breach-at-third-party-law-firm/?clickid=wIY3Us2AjxyPWqWXyWTPvxroUkFU5LSPUXUYTU0&irgwc=1&MPid=4328530&cid=aff%7Cc%7CIR%2F%2F; The hacking of two of New York's most prestigious law firms in 2016 shocked the profession and highlighted the vulnerability of data entrusted to other parties during discovery, even when "protected" by confidentiality orders and possessed by the nation's most admired law firms. Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504?reflink=desktopwebshare_permalink; Jeff John Roberts, *China Stole Data From Major U.S. Law Firms,* FORTUNE (Dec. 7, 2016), https://fortune.com/2016/12/07/china-law-firms/.

[32] Boliek, *supra* note 19, at 1138 ("in some circumstances, third-party information is at risk only because of the unique prerogative of the judiciary to compel discovery").

[33] THE SEDONA PRINCIPLES, THIRD EDITION: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, 19 SEDONA CONF. J. 1, 147, princ. 10 (2018) ("Parties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions.").

[34] Boliek, *supra* note 19, at 1134.

[35] Stuart, *supra* note 3.

access, use, and disclosure of personal and confidential information can cause significant and irreversible harm.

- Rule 1: Because all stakeholders share the obligation, the starting point should be an acknowledgment in Rule 1 that courts and parties have a responsibility to protect reasonable expectations of privacy, particularly with respect to information about non-parties who have no notice of the proceedings.
- Rules 26(f) and 16(b)(3)(B): The rules should prompt early consideration of privacy and cyber security issues.
- Rule 26(a)(1) and 26(e): The rules about initial disclosures and supplementation should clarify that parties need not include information protected by federal, state, or foreign privacy laws.
- Rule 26(c): Because protective orders are frequently used to protect privacy rights, Rule 26(c) should expressly acknowledge that such orders can bar unnecessary disclosure of personal and confidential information and require reasonable steps to ensure that no personal or confidential information is placed at risk of unauthorized disclosure.
- Rule 5.2: Clear guidance is needed about the sealing of documents. Rule 5.2 is woefully outdated.
- Rule 34: As the focal point of requests for documents and ESI, Rule 34 should empower courts and parties to ensure reasonable steps are taken to protect against unauthorized access of personal or confidential information.
- Rule 26(b)(1): To ensure that courts and parties consider whether discovery requests are proportional to the needs of the case, Rule 26(b)(1) should specifically reference the legal complexities, burdens on time, risks of exposure, potential infringement on privacy rights, and financial costs of producing and/or redacting personal information when determining whether the "burden or expense of the proposed discovery outweighs its likely benefit."[36]
- Rule 26(g): Lawyers who request or respond to discovery should be reminded by Rule 26(g) certifications that reasonable steps are required to avoid unnecessary use of personal information.
- Rule 37: The FRCP should provide remedies for the failure to "take reasonable steps"[37] to protect personal and confidential information.
- Rule 26(b)(4)(A): Because experts often rely on personal and confidential information when informing and explaining their opinions, Rule 26(b)(4)(A) should provide guidance for protecting against disclosure of such information in expert reports and depositions.
- Rule 44.1: Lawyers should not seek, and courts should not order, disclosure of information the production of which puts the holder in a Catch-22 situation because disclosure is barred by federal, state, or foreign law or infringes on the privacy rights of the data subjects.

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

[37] *See* THE SEDONA PRINCIPLES, *supra* note 35, at 147, princ. 10 ("Parties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions.").

- Rule 23: Due to the duties that judges have in class action proceedings, Rule 23 should include express protections for the privacy interests of absent class members.
- Rule 45: Finally, it is very important that Rule 45 be amended to protect non-parties[38] by ensuring that subpoenas do not result in unnecessary use or disclosure of personal or confidential information, including information that is subject to federal, state, or foreign data protection laws; that the issuer must take reasonable steps to protect personal and confidential information from unauthorized disclosure; and that these duties are enforceable with appropriate sanctions.

Together, these proposals will ensure that privacy and cyber security considerations are interwoven into the fabric of the FRCP so courts and parties have coherent guidance on how to anticipate, mitigate, and manage their shared responsibilities for these issues.

I. RULE 1 SHOULD AFFIRM THAT THE FRCP SHOULD BE CONSTRUED, ADMINISTERED, AND EMPLOYED TO PROTECT THE PRIVACY RIGHTS OF PARTIES AND NON-PARTIES

The responsibility for ensuring protection of parties' and non-parties' personal and confidential information during the litigation process is shared by courts[39] and parties[40] alike. Stating this in Rule 1 would not be an invention; it would be an affirmation of the present reality. "Privacy is a core concept that underlies the civil discovery rules…."[41] and "[m]any courts refer to 'expectations of privacy' in the context of civil discovery."[42] In fact, "for decades courts have routinely limited discovery based on the private nature of the information sought" and "[c]ourts have long utilized [the "good cause"] balancing test to protect privacy rights in the context of civil discovery."[43] Just as Rule 1 proclaims that courts and parties should construe, administer, and employ the FRCP to "secure the just, speedy, and inexpensive determination of every action and proceeding,"[44] so should Rule 1 acknowledge that courts and parties have responsibilities to

[38] Boliek, *supra* note 19, at 1139 ("[T]he need to protect the privacy interest is particularly acute when third parties cannot self-protect (opt out of the transaction) and cannot pursue tort remedies in the event of disclosure. As a threshold analysis, therefore, a judge should intervene to protect privacy interests in discovery when certain elements exist because they indicate circumstances when such rights are least likely to be otherwise protected.").

[39] Federal courts are obligated to protect private information by the E Government Act of 2002, 44 U.S.C. § 3601 *et seq*.; *See also* Boliek, *supra* note 19, at 1105 ("Only the judiciary plays the solemn role of gatekeeper to discovery requests and is therefore the ultimate guardian of this country's corporate, governmental, and individual private information.").

[40] THE SEDONA PRINCIPLES, *supra* note 35, at 147, princ. 10 ("Parties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions.").

[41] McPeak, *supra* note 9, at 235.

[42] Stuart, *supra* note 3, at 714.

[43] Hon. James C. Francis IV (Ret.), *Good Intentions Gone Awry: Privacy as Proportionality Under Rule 26(b)(1)*, 59 SAN DIEGO L. REV. 397, 401, 404 (2022) ("Francis"); *See also* Richard L. Marcus, *Myth and Reality in Protective Order Litigation*, 69 CORNELL L. REV. 1, 2 (1983) ("courts have regularly entered protective orders not only to protect trade secrets, but also to avoid other undesirable consequences such as the invasion of litigants' privacy" (footnotes omitted)).

[44] Fed. R. Civ. P. 1.

protect privacy rights and should use the FRCP to help manage those duties. It is particularly important for Rule 1 to acknowledge non-party privacy interests because today's practice of seeking and producing vast quantities of data about non-party individuals without notice to such individuals or a realistic opportunity to intervene reflects a sea change in discovery that is insufficiently contemplated by the FRCP. Because Rule 1 sets the aspirations for practice under the rules, it should be amended to reflect the responsibility of courts and parties to protect reasonable expectations of privacy and confidentiality as follows:

Rule 1 – Scope and Purpose

These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding, and to protect the reasonable expectations of privacy and confidentiality of parties and non-parties.

II. PRIVACY AND CYBER SECURITY CONSIDERATIONS SHOULD BE DISCUSSED IN RULE 26(f) PRETRIAL CONFERENCES AND INCORPORATED IN SCHEDULING ORDERS ISSUED UNDER RULE 16(b)

Amending Rules 16(b)(3)(B) and 26(f) to encourage parties to discuss privacy and cybersecurity issues early in the case is as important today as it was, in the 2015 rules amendments, to encourage parties to consider preservation and FRE 502 issues.[45] The Advisory Committee recognizes that early discussions are key to managing and solving discovery issues, particularly those that involve an information gap between the parties. The Committee Note to the 2015 amendment to Rule 26(b)(1) states:

> A party requesting discovery, for example, may have little information about the burden or expense of responding. A party requested to provide discovery may have little information about the importance of the discovery in resolving the issues as understood by the requesting party. Many of these uncertainties should be addressed and reduced in the parties' Rule 26(f) conference and in scheduling and pretrial conferences with the court.[46]

Privacy and cyber security considerations should be part of this process. In fact, it would be equally accurate if the note also stated:

> A party requesting discovery also may have little information about the burden or expense of identifying personal or confidential information, whether it is protected by federal, state, or foreign data privacy laws, the feasibility of redacting such information and the associated burden, and what reasonable steps might be necessary to ensure that

[45] *See* FED. R. CIV. P. 16(b)(3)(B) advisory committee's note to 2015 amendment.

[46] FED. R. CIV. P. 26(b)(1) advisory committee's note to 2015 amendment.

> such information is handled in a manner that does not place it at increased risk of unauthorized access, use, or disclosure.

Today, some of the most complex problems in litigation require balancing privacy interests of both parties and non-parties with the needs of the case. Such problems can arise very early in the case – for example, during preservation decisions – and can grow more thorny as the case progresses if not anticipated. Privacy considerations are not often top of mind early in a case when lawyers are focused on their clients' issues and interests, which do not always include protecting the privacy interests of non-parties.[47] But as the Sedona Principles observe, "the widespread adoption of state and federal privacy laws (as well as the application of foreign data protection laws) demands protective orders and procedures that provide adequate personal privacy safeguards and meet applicable statutory and common law legal standards."[48] Too often, these matters are left out of the early planning conferences, only to show up later in the form of a motion for protective order – or, even worse, only after someone's sensitive information has already been exposed. "[C]ourts should recognize that a valid privacy concern exists when a party seeks access to a digital data compilation."[49] Rather than ignore the problem until an exigency erupts, Rule 26(f) should require parties to share proposals on how to incorporate into their discovery plans how they will minimize the use of personal and confidential information, protect such information from unauthorized access or disclosure, and comply with the privacy rights of parties and non-parties as defined by applicable laws. A Sedona comment explains:

> Redactions or other actions necessary to protect private, personal information to meet required safeguards can be costly and time-consuming. The parties should address and attempt to resolve such issues at the Rule 26(f) conference. For example, parties may agree to exclude from production categories of private, personal information that are only marginally relevant to the claims and defenses or are cumulative of other produced information.[50]

Similarly, Rule 16 should prompt judges to discuss handling these issues proactively and to include provisions in their scheduling orders that provide protection for personal and confidential information, establish appropriate cybersecurity measures for information produced during the proceeding, and direct an appropriate process for returning or destroying sensitive information after the conclusion of the case.

---

[47] While the term non-parties is used throughout this proposal, we wish to emphasize that we are not primarily focused on non-parties who receive a Rule 45 subpoena. Instead, we primarily use this term – except where otherwise noted – to describe non-party individuals whose information may be used in conjunction with a proceeding even though they have no meaningful notice of the proceeding and no way to respond. For example, the employees, customers, or suppliers of a party whose information is collected, copied, and transferred as part of the discovery process, or the friends and family members of a custodian whose chat messages and photos are collected when that custodian's personal devices are forensically imaged. No rule currently addresses the concerns or rights of such true non-parties, even though their information constitutes much of the information exchanged in discovery.

[48] THE SEDONA PRINCIPLES, *supra* note 35, at 152, cmt. 10.e.

[49] McPeak, *supra* note 9, at 288.

[50] THE SEDONA PRINCIPLES, *supra* note 35, at 163, cmt. 10.j.

A Rule 26(f) amendment could look like this:

Rule 26 – Duty to Disclose; General Provisions Governing Discovery

***

(f) CONFERENCE OF THE PARTIES; PLANNING FOR DISCOVERY.

***

(3) *Discovery Plan.* A discovery plan must state the parties' views and proposals on:

***

(F) how the use of personal and confidential information will be minimized, including through the use of data anonymization, pseudonymization, encryption and redactions;
(G) how data disclosed or used in the proceeding will be protected from unauthorized access, use, or disclosure, and how the privacy rights of parties and non-parties covered by federal, state, and foreign data privacy laws will be protected; and
(HF) any other orders that the court should issue under Rule 5.2, Rule 26(c) or under Rule 16(b) and (c).

***

A Rule 16 amendment could address the problem as follows:

Rule 16 – Pretrial Conferences; Scheduling; Management

***

(b) SCHEDULING.

***

(3) *Contents of the Order.*

***

(B) *Permitted Contents.* The scheduling order may:

***

(vii) provide measures for protecting personal and confidential information related to both parties and non-parties, including any personal information

subject to federal, state, or foreign data privacy laws, from unnecessary use, disclosure or unauthorized access during the proceeding;
(viii) provide for reasonable and appropriate cybersecurity measures to prevent unauthorized access, use or disclosure of any information produced or disclosed by a party or a non-party during the proceeding;
(ix) direct that, at the conclusion of the proceeding, information disclosed during the proceeding be returned or securely destroyed; and
(x~~vii~~) include other appropriate matters.

***

(c) ATTENDANCE AND MATTERS FOR CONSIDERATION AT A PRETRIAL CONFERENCE.

***

(2) *Matters for Consideration.* At any pretrial conference, the court may consider and take appropriate action on the following matters:

***

(P) determining reasonable procedures for protecting personal and confidential information from unnecessary use, disclosure, or unauthorized access, including any personal information subject to federal, state, or foreign data protection laws; and
(Q) facilitating in other ways the just, speedy, and inexpensive disposition of the action.

***

III. PRIVACY PROTECTIONS AND CYBER SECURITY CONSIDERATIONS SHOULD BE EXPRESSLY ACKNOWLEDGED AS LIMITS TO INITIAL AND SUPPLEMENTAL DISCLOSURES

The requirements of Rule 26(a)(1) and Rule 26(e) should reflect that parties are not obligated to make initial disclosures of information that is protected by law, and are not required to turn over personal and confidential information unless the recipients have taken reasonable steps to protect such information from unauthorized access, use, or disclosure. An amendment to Rule 26(a)(1) could look like this:

Rule 26 – Duty to Disclose; General Provisions Governing Discovery
(a) REQUIRED DISCLOSURES.
(1) *Initial Disclosure*.

***

(F) *Limits on Initial Disclosure for Privacy and Information Security*. A party's initial disclosures need not include information protected by federal, state, or foreign privacy laws, including confidential information or personal information if the recipient has not taken reasonable and appropriate steps to ensure that such information is not subject to unauthorized access, use or disclosure. A party relying on this provision must expressly so state in their initial disclosures. These limits also apply to Rule 26(e) supplementation of initial disclosures.

***

(3) *Pretrial Disclosures*.

(A) *In General*. In addition to the disclosures required by Rule 26(a)(1) and (2), a party must provide to the other parties and promptly file the following information about the evidence that it may present at trial other than solely for impeachment:

(i) the name and, if not previously provided, the address and telephone number of each witness—separately identifying those the party expects to present and those it may call if the need arises, subject to the considerations outlined in Rule 5.2(i);

***

IV. RULE 26(c) SHOULD ACKNOWLEDGE AND ENCOURAGE PROTECTIVE ORDERS ADDRESSING PRIVACY AND CYBER SECURITY ISSUES

Rule 26(c) protective orders are frequently used to address privacy interests and cyber security risks in discovery, and the Rule should be amended to reflect this important role and to emphasize that reasonable and appropriate steps are needed to prevent the negligent or purposeful unauthorized access, use, or disclosure of information. An appropriate amendment would not only conform the rule to common practice, but also could prompt orders that protect the interests of non-parties, including employees, customers, patients, and contractors who might not even be aware that their personal information is being sought and disclosed. An amendment could add a provision as follows:

Rule 26 – Duty to Disclose; General Provisions Governing Discovery

***

(c) PROTECTIVE ORDERS.

(1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

***

(I) requiring that personal and confidential information not be revealed or be revealed only in a specified manner and that reasonable and appropriate steps be taken to avoid placing it at risk of unauthorized access, use or disclosure.

***

V. RULE 5.2 SHOULD BE UPDATED TO PROVIDE CLEAR GUIDANCE FOR BALANCING LITIGATION NEEDS WITH THE NECESSITY OF PROTECTING PERSONAL AND CONFIDENTIAL INFORMATION

The sealing of information filed with the court or used in court proceedings is critical to courts' and parties' ability to balance the needs of litigation with the courts' and parties' obligation to protect personal and confidential information. As the Advisory Committee is now considering whether and how to fashion a uniform federal rule governing sealing procedures,[51] the Advisory Committee's attention should focus on helping courts and parties navigate the legal requirements and complexities of privacy interests held by parties and non-parties. The Advisory Committee recognized that a court's decision whether to allow sealing is consequential because the default practice is to make court records open to the public. The Committee Notes to Rule 5.2 warn:

> Parties must remember that any personal information not otherwise protected by sealing or redaction will be made available over the internet.[52]

Although this is an appropriate caution, it is wholly insufficient as rules guidance. Acknowledging that information belonging to parties (and non-parties, although not mentioned in Rule 5.2), even if protected by law, will be publicly available unless sealed or redacted does not provide a framework for navigating the knotty questions. Trial courts recognize that sealing of documents and portions of court proceedings is necessary to protect the privacy and proprietary interests of parties and non-parties.[53] But Rule 5.2 is outdated; it does not expressly

[51] Advisory Committee on Civil Rules, *Agenda Book* 133-34 (Mar. 28, 2023), https://www.uscourts.gov/sites/default/files/2023-03_civil_rules_committee_agenda_book_final_0.pdf.

[52] FED. R. CIV. P. 5.2 advisory committee's note.

[53] *See, e.g.*, Gina Kim, *Masimo Execs Testify Behind Closed Doors In $3B Apple Trial*, LAW360 (Apr. 6, 2023), https://www.law360.com/articles/1594526/masimo-execs-testify-behind-closed-doors-in-3b-apple-trial, ("U.S.

allow redactions of information that is now protected by privacy laws, or personal information that does not fall within the four narrow categories listed in the rule (social security number, birthdate, a minor's name, and financial account numbers).[54] Nor does the rule prompt consideration of the most basic necessary factors including the privacy and confidentiality rights of parties and non-parties, the burdens of identifying and redacting sensitive information, and whether the court and parties have taken reasonable steps to protect against negligent disclosure of, or unauthorized access to, other people's information. Alarmingly, Rule 5.2 expressly allows a person making a redacted filing to file an additional unredacted copy under seal, which could completely vitiate any protection the rule might otherwise offer. That provision shows an important defect in the rule: sealing cannot be considered a cure all. As the recent SolarWinds data breach of federal court information systems demonstrates, a sealing order is not a guarantee against disclosure, and courts' considerations should include whether their own systems are appropriately secure and whether certain information is so sensitive that it should not be filed under seal.

To address these important shortcomings, the Advisory Committee should amend Rule 5.2 to provide express guidance for considering sealing requests. The rule should make clear that a decision to seal court records is a balancing between the needs of the litigation, transparency, and the duty to protect the privacy and property interests. The rule should also recognize the responsibility of the court and parties to address the rights and interests of non-parties who might not be aware that their personal information could be disclosed through a court filing or testimony.

It is important to note that the Advisory Committee is being urged to draft an all-new rule 5.3 to curtail a perceived excess in sealing orders.[55] But an entirely new rule is not needed given that Rule 5.2 is intended to encompass the details of sealing and that the caselaw shows courts already give ample consideration to avoiding unnecessary restrictions on public access to judicial *proceedings*. To the contrary, the real problems occur when courts adopt an overly prescriptive approach to sealing *documents* containing personal or confidential information, resulting in either excessive and burdensome redactions of information that did not really need to be protected or, alternatively, grossly inadequate protections for information that should have been sealed, particularly personal information related to non-parties whose names and other personal information appear in exhibits and evidence. Our proposed amendment to Rule 5.2 solves these problems by setting explicit criteria for consideration in sealing decisions paired with sufficient flexibility to enable courts and parties to craft case-specific approaches that balance the interests of privacy and transparency.

District Judge James V. Selna ordered the courtroom sealed for portions of testimony on both direct and cross-examination from Kiani regarding the plaintiffs' purported trade secrets.").

[54] FED. R. CIV. P. 5.2(a).

[55] Letter from Eugene Volokh, Gary T. Schwartz Professor of Law, UCLA School of Law, to Members of the Advisory Committee (Aug. 7, 2020), https://www.uscourts.gov/sites/default/files/20-cv-t_suggestion_from_eugene_volokh_reporters_committee_for_freedom_of_the_press_and_the_electronic_frontier_foundation_-_rule_5_0.pdf.

An appropriate amendment could look like this:

Rule 5.2. – Privacy Protection For Filings Made with the Court

(a) Redacted Filings. Unless the court orders otherwise, in an electronic or paper filing with the court, a party:

(1) may redact personal information protected by federal, state, or foreign privacy laws; and

(2) shall redact sensitive personal information consisting of an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number; a party or nonparty making such filing may include only:

(~~1~~a) the last four digits of the social-security number and taxpayer-identification number;
(~~2~~b) the year of the individual's birth;
(~~3~~c) the minor's initials; and
(~~4~~d) the last four digits of the financial-account number.

***

(e) Protective Orders. For good cause, the court may by order in a case:

(1) require redaction of additional information; or

(2) limit or prohibit a nonparty's ~~remote electronic~~ access to a document filed with the court.

(f) Option for Additional Unredacted Filing Under Seal. For good cause, the court may by order in a case allow a~~A~~ person making a redacted filing ~~may also~~to file an unredacted copy under seal. The court must retain the unredacted copy as part of the record.

***

(i) Considerations. When the court is considering the sealing or unsealing of documents filed with the court, or whether to order discovery or disclosure under Rule 26, including the issuance of a protective order, the court shall consider: (a) whether the court or requesting party can provide reasonable and appropriate protection against unauthorized access or disclosure; (b) the rights and interests of parties and non-parties in maintaining the privacy and confidentiality of information pertaining to them; (c) the burdens on parties and non-parties, including whether those burdens are proportional to the needs of the case; (d) whether the information to be redacted is protected by federal, state, or foreign privacy laws; and (e) whether the information to be redacted is subject to a contractual confidentiality obligation or non-disclosure agreement.

VI. RULE 34 SHOULD EMPOWER COURTS AND PARTIES TO ENSURE REASONABLE STEPS ARE TAKEN TO PROTECT AGAINST UNAUTHORIZED ACCESS OF PERSONAL OR CONFIDENTIAL INFORMATION

Rule 34 defines the procedure for requesting—and objecting to requests for—documents, ESI, and tangible things, but it does not provide parties with adequate assurance of appropriate handling of such information to deal with privacy and cybersecurity concerns. The Advisory Committee has acknowledged the problem, albeit in a very limited way; the 2006 Committee Note observes that testing and sampling of ESI or information systems "may raise issues of confidentiality or privacy" and suggests that "[c]ourts should guard against undue intrusiveness" resulting from inspecting or testing information systems.[56] The rule's restraint belies the seriousness of the problems that regularly occur under the rule. As the Sedona Conference describes, Rule 34 inspections trigger significant privacy and cyber security risks:

> Direct access to an opposing party's computer systems under a Rule 34 inspection also presents possible concerns such as:
>
> a) revealing trade secrets;
> b) revealing other highly confidential or personal information, such as personnel evaluations and payroll information, properly private to individual employees;
> c) revealing confidential attorney-client or work-product communications;
> d) unreasonably disrupting the ongoing business;
> e) endangering the stability of operating systems, software applications, and electronic files if certain procedures or software are used inappropriately; and
> f) placing a responding party's computing systems at risk of a data security breach.[57]

The information explosion is posing severe challenges to courts and parties making, responding to, and ruling on discovery requests and objections. Rule 34 is the epicenter; it is the means by which parties request data from employees' BYOD devices and people's cell phones, fitness trackers, smart watches, computers, and GPS units—locations where information is almost always intermingled with sensitive, personal, and private data related to both parties and non-parties alike. Even if discoverable, such information must be protected from unnecessary disclosure or use. Rule 34 generates this type of situation frequently enough that rule guidance would be much more efficient than *ad hoc* protective orders, and the best way for Rule 34 to help is to set forth the common-sense responsibility of requesting parties to provide assurances that reasonable measures are in place to protect such information from unauthorized access, use, or disclosure. An appropriate amendment could look like this:

Rule 34 – Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes

[56] FED. R. CIV. P. 34(a)(1) advisory committee's note to 2006 amendment.

[57] THE SEDONA PRINCIPLES, *supra* note 35, at 128-29.

***

(b) Procedure.

***

(2) *Responses and Objections*.

***

(E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

***

(iv) A party may produce personal or confidential ESI by providing the requesting party with access to a secure data escrow service or other secure digital environment in which the ESI can be securely reviewed, provided such service permits the export of exhibits for use during depositions and in court filings;

(v) A party may object based on plausible concerns about the adequacy of the methods anticipated to be used by the requesting party or other recipients to prevent unauthorized access to, or use of, personal information or other confidential and proprietary information; and

(vi) A party need not produce documents or electronically stored information without having received adequate assurances that any personal information or other confidential and property information will be reasonably and adequately protected from unauthorized access or disclosure upon such transfer.

***

VII. THE SCOPE OF DISCOVERY AS DEFINED IN RULE 26(b) SHOULD REFLECT THE COMPLEXITIES AND BURDENS IMPOSED BY PRIVACY ISSUES AND CYBER SECURITY RISKS

Rule 26(b)(1) proportionality factors are highly germane to courts' and parties' consideration of discovery requests that include personal or confidential information. Those factors include whether "the burden or expense of the proposed discovery outweighs its likely benefit" and weighing "the importance of the discovery in resolving the issues."[58] The proportionality

[58] *See* THE SEDONA CONFERENCE PRIMER ON SOCIAL MEDIA, SECOND EDITION, 20 SEDONA CONF. J. 1, 27-28 (2019) ("The proportionality limitation on the scope of discovery includes two factors that implicate privacy concerns, *i.e.,* 'the importance of the discovery in resolving the issues, and whether the burden … of the proposed discovery outweighs its likely benefit'") (citing *Henson v. Turn, Inc*., No. 15-cv-01497-JSW (LB), 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018)).

analysis is especially important when, as often happens today, the discovery sought includes materials that are intertwined with personal, protected information of parties and non-parties such as data generated and stored by cell phones and other BYOD devices,[59] social media, activity trackers, and the internet of things.

"[C]ourts should take privacy burdens into account when determining the proportionality of discovery,"[60] and should consider the impact of privacy concerns on proportionality at all stages of the discovery process.[61] "Achieving proportional privacy means that the privacy invasion in some cases may outweigh the likely benefits of the discovery."[62] For example, before financial information regarding millions of people is extracted from a bank app and duplicated across multiple parties, non-parties, their consultants, experts and the courts, the court and parties should think through whether sharing so much sensitive information about other people and putting it at a higher risk for unauthorized use is proportional to the needs of the case and whether doing so on the scale proposed is fair to the non-party individuals whose information will be duplicated and disseminated.

Often, when managed early and thoughtfully, alternative approaches can provide the key information with much less risk to individuals and lower burdens on parties. Proportionality is flexible; it can be used to determine the smallest amount of data access that is proportional to the needs of the case. For example, "[h]igh costs for redaction may lead a court to order that less data be released, no data be released, or another privacy protection option be employed."[63] In contrast, ignoring proportionality analysis can lead to inefficient, inappropriate, and unfair decisions that impose complicated, time-consuming, and expensive legal work, often encumbering a single stakeholder – typically, the producing party – with sorting out the disparate legal standards and undertaking all of the redactions and other remedies required by various laws and regulations without first asking whether those burdens are proportional to the value of the information in adjudicating the claims and defenses.

"[A]n emerging consensus of courts and commentators has concluded that privacy interests may—and indeed, should—be considered as part of the proportionality analysis required under Rule 26(b)(1)."[64] Unfortunately, however, neither Rule 26(b)(1), Rule 26(b)(2)(C), nor the accompanying Committee Notes mention privacy and cyber security considerations expressly. "[I]t is difficult to shoehorn privacy interests into any of the factors identified in Rule 26(b)(1)"[65] in part because, "[d]espite the courts' preexisting authority to limit discovery based on privacy

---

[59] "[D]iscovery of content on these devices may encompass irrelevant, highly personal information of both litigants and employees who are not parties to the litigation." McPeak, *supra* note 9, at 283.

[60] *Id.* at 289.

[61] *See* Keeling & Mangum, *supra* note 21, at 71 (noting that proportionality applies to "all aspects of the discovery and production of ESI" and that privacy concerns are, therefore, "relevant from the outset" of the case) (quoting THE SEDONA PRINCIPLES, *supra* note 35, at 67) (internal quotations omitted).

[62] McPeak, *supra* note 9, at 291.

[63] Boliek, *supra* note 19, at 1143.

[64] Keeling & Mangum, *supra* note 21, at 67.

[65] Francis, *supra* note 45, at 421.

concerns, the word 'privacy' was curiously absent from this new list of factors."[66] Not only is this oversight depriving courts and parties of a useful framework for managing and avoiding complicated and important issues, but it has also led to considerable uncertainty about the meaning of the rule itself – namely, whether proportionality and mandatory protective order standards apply to discovery involving privacy issues and cyber security considerations. Some courts and lawyers are using the Rule 26(b)(1) proportionality requirement in navigating privacy issues,[67] but others say the text and history of the rule provide no basis for applying proportionality analysis to such questions.[68] Although scholars and commentators disagree about the extent to which the Rule 26(b)(1) "proportionality" requirement already provides a tool to help courts and parties balance privacy interests with the needs of discovery, even the critics of proportionality as a means of balancing privacy interests concede that proportionality is relevant. Judge Francis observes:

> Certainly, to the extent that a party is obligated to expend resources to safeguard the privacy interests of itself or of a non-party whose information it holds, those expenditures are properly considered in a traditional proportionality calculation. Thus, the costs of disaggregating data to isolate that which is private, of redacting personal information, or of anonymizing data in order to shield the identity of non-parties are all burdens appropriately included in the proportionality analysis.[69]

Any fear that amending the proportionality factors to include privacy interests would give judges too much discretion at the expense of clarity and consistency[70] would be prevented by amending other FRCP provisions as suggested herein rather than relying on Rule 26(b)(1) to do the heavy lifting.

As Judge Rosenthal and Professor Gensler urge, the correct path is "to take the subject head on" as "[i]t may well be time to rethink some of the rule choices we made in the past."[71] The Advisory Committee should end the uncertainty about whether the scope of discovery is

---

[66] Boliek, *supra* note 19, at 1129.

[67] *See* Keeling & Mangum, *supra* note 21, at 69 ("[T]he fact that specific, nonpecuniary burdens, such as privacy, were not explicitly discussed at length in the pre-2015 history of the amendments does not foreclose it as a proper factor in conducting a proportionality analysis. To the contrary, the Rule's text is plain, and it clearly evinces the drafters' intent that both monetary costs and additional nonpecuniary 'burdens' must be weighed") *and* McPeak, *supra* note 9, at 286 ("Courts already have the discretion to limit the scope of discovery based on the needs of the case and should utilize the proportionality test in Rule 26 to balance the privacy burden of overly invasive discovery against the needs of the case").

[68] Francis, *supra* note 45, at 420 ("To the extent that courts intend to treat privacy as a true proportionality factor, they are hard-pressed to find a theoretical basis for doing so").

[69] *Id*. at 435.

[70] *Id.* at 425-26, 429 ("Treating privacy as a proportionality factor also expands judicial discretion while, at the same time, reducing the clarity and consistency of court decisions" and "treating privacy as a proportionality factor can tempt judicial decision makers to cut analytic corners" and "including privacy within the proportionality analysis provides overburdened jurists a further excuse for dismissing a discovery request out of hand without doing the hard work of disaggregation first").

[71] Gensler & Rosenthal, *supra* note 6, at 81.

impacted by privacy rights—it is, has been for decades, and should be.[72] Just as the 2015 amendment to Rule 26(b)(1) reaffirms that proportionality is *always* a consideration in discovery, so should the rule reflect that privacy and cyber security concerns, which are *always* present, raise—often, even more dramatically—the very question of whether the value of requested information outweighs the complexities, burdens, and risks inherent in identifying, redacting, sharing, and protecting it.

Requiring courts and parties to consider privacy rights and cyber security risks as part of the proportionality analysis would be helpful to courts and parties who share the responsibility to protect personal information, reduce the risks created by discovery, and enhance public trust in the judicial process. Accordingly, Rule 26(b)(1) and Rule 26(b)(2)(C) should be amended to require that privacy interests and cyber security risks be considered when determining if the discovery sought is proportional to the needs of the case. Here's how such amendments might look:

Rule 26 – Duty to Disclose; General Provisions Governing Discovery

***

(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, the parties' resources, the importance of the discovery in resolving the issues, the privacy rights held by parties and non-parties, the risk of unauthorized access to, or use of, personal or confidential information, the harm such unauthorized access or use would cause, 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.

(2) *Limitations on Frequency and Extent.*

***

(C) *When Required*. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

[72] Boliek, *supra* note 19, at 1127 ("It is time … for the courts to fully employ the discretion afforded them in Rule 26 and to adopt greater protections for the privacy interest than the traditional protective order.").

(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; ~~or~~

(iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1);

(iv) the discovery sought would require the disclosure of personal information related to parties or non-parties beyond what is strictly necessary to facilitate the action, would violate any federal, state or foreign data privacy law, or otherwise infringes on reasonable privacy expectations held by parties or non-parties; or,

(v) the discovery sought poses an unreasonable risk of unauthorized access, use or disclosure of personal or other confidential information.

***

VIII. THE FRCP SHOULD REQUIRE CERTIFICATION THAT REASONABLE STEPS ARE TAKEN REGARDING PRIVACY RIGHTS AND CYBER SECURITY RISKS

As the Advisory Committee knows, compliance with the FRCP's principles and purposes does not flow automatically from rule amendments. The rules, for that reason, provide incentives for observance of particularly important provisions including via the certifications stated in Rule 26(g). Rule 26(g) makes lawyers responsible for the process by which their clients gather the information and documents that form the basis for their discovery responses as well as the mandatory initial disclosures.[73] Encouraging parties and their lawyers to make responsible decisions to balance discovery needs with privacy interests and cyber security risks is worthy of this treatment. Rule 26(g) should say that the signature on discovery requests, responses, and objections certifies that the lawyer has made reasonable efforts to avoid unnecessary requests for or use of personal or confidential information, and that any discovery request or response will not result in unnecessary risks of unauthorized access to, or disclosure of, such information. It should also function as a certification that the lawyer is taking reasonable steps to provide cybersecurity protections, including having a data breach response plan.

An appropriate amendment to Rule 26(g) might read as follows:

Rule 26 – Duty to Disclose; General Provisions Governing Discovery

***

(g) Signing Disclosures and Discovery Requests, Responses, and Objections.

[73] Steven S. Gensler, *Some Thoughts on the Lawyer's E-volving Duties in Discovery*, 36 N. KY. L. REV. 521, 558-559 (2009) (discussing the lawyer's duty to certify).

(1) Signature Required; Effect of Signature. Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must state the signer's address, email address, and telephone number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

(A) with respect to a disclosure, it is complete and correct as of the time it is made~~;~~ and that reasonable efforts have been made to avoid unnecessary use of personal or confidential information, including any personal information subject to federal, state, or foreign data privacy laws; and

(B) with respect to a discovery request, response, or objection~~, it is~~:

(i) is consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;

(ii) will not be interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; ~~and~~

(iii) will not result in unnecessary access to, use, or disclosure of, personal or other confidential information, including any personal information subject to federal, state, or foreign data privacy laws;

(~~iii~~iv) is neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action; and,

(v) will not require the production of personal or other confidential information until the requesting party and its attorneys have each implemented reasonable and appropriate cybersecurity protections for such information, including having in place a written data breach response plan.

***

IX. THE FRCP SHOULD PROVIDE MEASURES FOR THE FAILURE TO TAKE REASONABLE STEPS TO COMPLY WITH PRIVACY AND CYBER SECURITY REQUIREMENTS

Existing statutes, regulations and tort remedies often require, or at a minimum strongly incentivize, producing parties to take reasonable and appropriate steps to protect personal and confidential information that is within their possession, custody or control prior to its production in civil litigation. However, while the existing FRCP often require parties to produce large quantities of sensitive information, the current rules fail to correspondingly ensure that parties *receiving* such information take adequate steps to protect it. Accordingly, Rule 37 should be amended to incentivize appropriate handling of privacy and attendant cyber security risks by providing a remedy for losses of information due to a receiving party's or lawyer's failure to take reasonable steps to avoid such losses. This provision will act as a deterrent to the negligent or

purposeful failure to protect the privacy rights of parties and non-parties, and will compensate those who suffer from privacy-related harm. An appropriate amendment would be to add a Rule 37(g) with the elements incorporated here:

> Rule 37 – Failure to Make Disclosures or to Cooperate in Discovery; Sanctions
>
> ***
>
> (g) Failure to Provide Adequate Protection for Personal and Confidential Information. If unauthorized access to, or disclosure of, personal or confidential information during litigation is caused by the receiving party's failure to take reasonable and appropriate steps to comply with the obligations imposed by these rules, the court may require that party, the attorney advising that party, or both, to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.

X. BECAUSE EXPERTS OFTEN BASE OPINIONS ON PERSONAL AND CONFIDENTIAL INFORMATION, THE FRCP SHOULD PROVIDE EXPRESS GUIDANCE FOR PROTECTING THAT INFORMATION FROM DISCLOSURE IN EXPERT REPORTS AND DEPOSITIONS

The FRCP contemplate unabridged disclosure of information upon which an expert relies for the basis of an opinion—and rightly so in most cases. The Advisory Committee explains:

> [T]he intention is that "facts or data" be interpreted broadly to require disclosure of any material considered by the expert, from whatever source, that contains factual ingredients. The disclosure obligation extends to any facts or data "considered" by the expert in forming the opinions to be expressed, not only those relied upon by the expert.[74]

The FRCP do not, however, require or provide guidance about protecting against disclosure of the personal and confidential information the expert considers. Although it is commonplace for courts to enter stipulated protective orders that bind experts to confidentiality and non-disclosure of confidential discovery, such protective orders rarely address the critical need for parties and their counsel to ensure that experts take reasonable steps to secure that information, including measures to make information systems appropriately secure and not vulnerable to unauthorized access. Accordingly, Rule 26(b)(4)(A) should clarify the obligation with respect to experts. An amendment might look like this:

> Rule 26 – Duty to Disclose; General Provisions Governing Discovery
>
> ***

[74] FED. R. CIV. P. 26(a)(2)(B) advisory committee's note to 2010 amendment.

(b) Discovery Scope and Limits.

***

(4) Trial Preparation: Experts.

(A) Deposition of an Expert Who May Testify. A party may depose any person who has been identified as an expert whose opinions may be presented at trial. If Rule 26(a)(2)(B) requires a report from the expert, the deposition may be conducted only after the report is provided. A party deposing an expert should take reasonable and appropriate measures to protect against disclosure of personal or confidential information relating to parties or non-parties.

***

XI. RULE 23 SHOULD UPHOLD THE COURT'S ROLE IN PROTECTING ABSENT CLASS MEMBERS BY PROVIDING GUIDANCE FOR AVOIDING UNNECESSARY USE AND MISUSE OF PERSONAL INFORMATION

Rule 23 establishes a unique role for courts in protecting the interests of absent class members. Today, safeguarding personal information against unnecessary disclosure and misuse during class action litigation is just as important as – and a necessary element of – ensuring adequacy of counsel and fairness of settlements. Accordingly, Rule 23 should clarify that: (1) as a prerequisite, a class action should not unreasonably infringe on the privacy rights of putative class members; (2) certification decisions take account of the need to protect the privacy interests of putative class members, defendants, and non-parties alike; (3) notice avoids disclosing information related to individual class members; (4) in conducting the action, courts will establish appropriate procedures to protect personal and confidential information; (5) settlement agreements will provide for the return or secure destruction of all confidential information; and (6) class counsel has the ability to protect class members' and other litigants' personal and confidential information from negligent or purposeful disclosure.

Amendments to Rule 23 could include the following:

Rule 23 – Class Actions

(a) Prerequisites. One or more members of a class may sue or be sued as representative parties on behalf of all members only if:
(1) the class is so numerous that joinder of all members is impracticable;
(2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class;
(4) the representative parties will fairly and adequately protect the interests of the class, and (5) the action can be brought in a manner that does not unreasonably infringe the privacy rights of putative class members, unnamed class members and non-parties to the action,

including the right of each class member or putative class member to prevent the disclosure of any personal identifying information to class counsel without explicit written consent in advance to such disclosure.

***

(c) Certification Order; Notice to Class Members; Judgment; Issues Classes; Subclasses.
(1) *Certification Order*.

(A) *Time to Issue*. At an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action.

(B) *Defining the Class*; Appointing Class Counsel. An order that certifies a class action must define the class and the class claims, issues, or defenses, and must appoint class counsel under Rule 23(g).

(C) *Confirming Protection of Privacy and Information Security*. An order that certifies a class action must detail the specific measures that will be taken by the parties to:

(i) ensure personal information related to parties and non-parties, including unnamed class members, is accessed, used and disclosed no more than is strictly necessary to facilitate the just resolution of claims and defenses in the action;

(ii) ensure any personal information protected by federal, state, or foreign data protection laws is used or disclosed only in a manner consistent with such laws; and,

(ii) ensure reasonable and appropriate protection from unauthorized access, use or disclosure of personal or otherwise confidential information during the action and upon its conclusion.

(~~C~~D) *Altering or Amending the Order*. An order that grants or denies class certification may be altered or amended before final judgment.

(2) *Notice*.

(A) For (b)(1) or (b)(2) Classes. For any class certified under Rule 23(b)(1) or (b)(2), the court may direct appropriate notice to the class.

(B) For (b)(3) Classes. For any class certified under Rule 23(b)(3)—or upon ordering notice under Rule 23(e)(1) to a class proposed to be certified for purposes of settlement under Rule 23(b)(3)—the court must direct to class members the best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort. The notice may be by one or more of the following: United States mail, electronic means, or other appropriate means. The notice must clearly and concisely state in plain, easily understood language:

(i) the nature of the action;

(ii) the definition of the class certified;

(iii) the class claims, issues, or defenses;

(iv) the types of information related to individual class members that will be used or disclosed in the action, including during discovery, and to whom such information will be disclosed;
(~~i~~v) that a class member may enter an appearance through an attorney if the member so desires;
(vi) that the court will exclude from the class any member who requests exclusion;
(vii) the time and manner for requesting exclusion; and
(viii) the binding effect of a class judgment on members under Rule 23(c)(3).

***

(d) Conducting the Action.

***

(3) *Privacy and Information Security*. The court shall at all times safeguard the privacy rights of parties and non-parties, including the rights of unnamed class members. At a minimum, this will require the court to establish reasonable and appropriate procedures for protecting personal or other confidential information from unnecessary use, disclosure, and unauthorized access or disclosure, including any personal information subject to federal, state, or foreign data privacy laws. In making determinations related to this provision, the court must never presume that unnamed class members or non-parties would want information about them used or disclosed to facilitate the action or during its pendency.

(e) Settlement, Voluntary Dismissal, or Compromise. The claims, issues, or defenses of a certified class—or a class proposed to be certified for purposes of settlement—may be settled, voluntarily dismissed, or compromised only with the court's approval.

The following procedures apply to a proposed settlement, voluntary dismissal, or compromise:

(1) *Notice to the Class*.

***

(2) *Approval of the Proposal*. If the proposal would bind class members, the court may approve it only after a hearing and only on finding that it is fair, reasonable, and adequate after considering whether:

(A) the class representatives and class counsel have adequately represented the class;
(B) the proposal was negotiated at arm's length;

(C) the relief provided for the class is adequate, taking into account:
(i) the costs, risks, and delay of trial and appeal;
(ii) the effectiveness of any proposed method of distributing relief to the class, including the method of processing class-member claims;
(iii) the terms of any proposed award of attorney's fees, including timing of payment; and
(iv) any agreement required to be identified under Rule 23(e)(3);
(D) the proposal treats class members equitably relative to each other; and
(E) the proposal contains sufficient provisions for the return or secure destruction of all personal and confidential information, including personal information relating to unnamed class members and confidential information belonging to the parties, exchanged during the litigation.

***

(g) Class Counsel.

(1) Appointing Class Counsel. Unless a statute provides otherwise, a court that certifies a class must appoint class counsel. In appointing class counsel, the court:

(A) must consider:

(i) the work counsel has done in identifying or investigating potential claims in the action;
(ii) counsel's experience in handling class actions,
other complex litigation, and the types of claims asserted in the action;
(iii) counsel's knowledge of the applicable law;
(iv) the resources that counsel will commit to representing the class;
(v) counsel's ability to protect the privacy interests of putative and unnamed class members, including personal information and all parties' confidential information; and,
(vi) counsel's ability to provide reasonable and appropriate cyber security protections for all systems used in the litigation for accessing, viewing, sharing, communicating, or storing such information.

(B) may consider any other matter pertinent to counsel's ability to fairly and adequately represent the interests of the class;
(C) may order potential class counsel to provide information on any subject pertinent to the appointment and to propose terms for attorney's fees and nontaxable costs;
(D) may include in the appointing order provisions about the award of attorney's fees or nontaxable costs under Rule 23(h); and
(E) may make further orders in connection with the appointment.

(2) *Standard for Appointing Class Counsel*. When one applicant seeks appointment as class counsel, the court may appoint that applicant only if the applicant is adequate under Rule 23(g)(1) and (4). If more than one adequate applicant seeks appointment, the court must appoint the applicant best able to represent the interests of the class.
(3) Interim Counsel. The court may designate interim counsel to act on behalf of a putative class before determining whether to certify the action as a class action.
(4) Duty of Class Counsel. Class counsel must fairly and adequately represent the interests of the class, including protecting personal information related to each class member.

***

XII. RULE 44.1 SHOULD HELP COURTS AND PARTIES RESOLVE CONFLICTS BETWEEN DISCOVERY OBLIGATIONS AND FOREIGN LAWS DEFINING PRIVACY RIGHTS

The main purpose of Rule 44.1 is "[t]o avoid unfair surprise" when a party intends to raise an issue of foreign law.[75] Today, it is commonplace for parties to grapple with foreign privacy laws as they relate to discovery obligations, especially the General Data Protection Regulation (GDPR).[76] The "unfair surprise" is not that such foreign laws are raised, but rather that producing parties are often asked and even ordered to take actions that, absent disproportional effort, would violate laws that bar disclosure of information related to employees, consumers, patients, counterparties, and members of the public. Discovery now frequently forces producing parties to make an impossible choice between obeying a court order or complying with governing privacy laws that do not allow compliance with that order. The recurring problem is that foreign legal standards are not compatible with U.S. caselaw interpreting the FRCP-imposed discovery obligations.[77] Indeed, the original rubric established for addressing such conflicts in

[75] FED. R. CIV. P. 44.1 advisory committee's note to 1966 rule.

[76] Eur. Union, *The History of the General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Sept. 11, 2023).

[77] *See, e.g.*, *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522, 544 n.29 (1987) (noting that "[i]t is well settled that [foreign blocking] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."); *Royal Park Invs. SA/NV v. HSBC Bank USA, N.A.*, No. 14 CIV. 8175 (LGS), 2018 WL 745994, at *2 (S.D.N.Y. Feb. 6, 2018) (overruling Royal Park's objections to producing unredacted documents based on the Belgian Data Privacy Act, finding "that the comity analysis weighs in favor" of compelling production); *Knight Cap. Partners Corp. v. Henkel Ag & Co., KGaA*, 290 F. Supp. 3d 681, 687 (E.D. Mich. 2017) ("the German Federal Data Protection Act does not bar the defendant from disclosing email communications and other business records included in the plaintiff's discovery requests, principally because the Act contains an express exception to the broad prohibitions on personal data disclosure."); *Gucci Am., Inc. v. Curveal Fashion*, No. 09 CIV. 8458 RJS/THK, 2010 WL 808639, at *2 (S.D.N.Y. Mar. 8, 2010) ("courts in the Second Circuit may also consider the hardship of compliance on the party or witness from whom discovery is sought [and] the good faith of the party resisting discovery") (internal citations omitted); *Laydon v. Mizuho Bank, Ltd.*, 183 F. Supp. 3d 409, 413 (S.D.N.Y. 2016) (same); *AccessData Corp. v. ALSTE Techs. GmbH*, No. 2:08CV569, 2010 WL 318477, at *2 (D. Utah Jan. 21, 2010) (the court found that the party resisting discovery failed to demonstrate how the legal claims or consent exceptions did not apply, and ordered the production of documents).

discovery was created nearly 40 years ago in a case that did not consider the issue of privacy at all, *Société Nationale,*[78] and at a vastly different time when the internet, smart phones, and social media did not exist and few companies were truly global. Today, the world is more interconnected than ever and it is now common for even seemly small cases or small business to involve discovery of personal information stored abroad or pertaining to employees, customers, and other individuals residing aboard. Struggling to make sense of the challenges, the Sedona Conference has produced more than 10 different guides addressing the complexities created by the intersection of privacy and cross-border discovery in the past six years.[79] These issues will continue to grow even more labyrinthian as more jurisdictions create laws, more people become interconnected, and more cases involve data related to consumers, employees, and others who are located abroad.

The solution is not to put the onus of Catch-22 obligations exclusively on the shoulders of a producing party or non-party, but rather to clarify the shared responsibility that courts and parties have to navigate applicable laws. It is also critically important to the credibility and fairness of the U.S. judicial system to recognize that these foreign privacy laws often exist to protect important rights held by individual non-parties living and working in their home countries, who have demanded through the democratic process of those countries that their rights be protected. It does not reflect well on the U.S. judiciary when individual rights that are highly valued and often hard fought are cast aside by U.S. courts and parties who give them short shrift. The once-little-used provisions of Rule 44.1 are now front and center, and the rule can and should be amended to help resolve these constant conflicts. An amendment along these lines is needed:

Rule 44.1 – Determining Foreign Law

(a) A party who intends to raise an issue about a foreign country's law must give notice by a pleading or other writing. In determining foreign law, the court may consider any relevant material or source, including testimony, whether or not submitted by a party or admissible under the Federal Rules of Evidence. The court's determination must be treated as a ruling on a question of law.

(b) When evidence is sought from a foreign country and the laws of that country create a right to privacy held by individuals residing therein that conflicts with US law, or the law of that country places restrictions on the transfer of data outside the country, the court must

[78] *Société Nationale*, 482 U.S. 522.

[79] *See, e.g.*, THE SEDONA CONFERENCE PRACTICAL IN-HOUSE APPROACHES FOR CROSS-BORDER DISCOVERY AND DATA PROTECTION, 17 SEDONA CONF. J. 397 (2016); THE SEDONA CONFERENCE INTERNATIONAL LITIGATION PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION IN CIVIL LITIGATION (TRANSITIONAL EDITION) (The Sedona Conference Working Group Series, 2017); THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES FOR ADDRESSING DATA PROTECTION IN CROSS-BORDER GOVERNMENT & INTERNAL INVESTIGATIONS: PRINCIPLES, COMMENTARY & BEST PRACTICES, 19 SEDONA CONF. J. 557 (2018); THE SEDONA CONFERENCE COMMENTARY AND PRINCIPLES ON JURISDICTIONAL CONFLICTS OVER TRANSFERS OF PERSONAL DATA ACROSS BORDERS, 21 SEDONA CONF. J. 393 (2020); THE SEDONA CONFERENCE COMMENTARY ON THE ENFORCEABILITY IN U.S. COURTS OF ORDERS AND JUDGMENTS ENTERED UNDER GDPR, 22 SEDONA CONF. J. 277 (2021); THE SEDONA CONFERENCE COMMENTARY ON MANAGING INTERNATIONAL LEGAL HOLDS, 24 SEDONA CONF. J. 429 (2023).

ensure such privacy rights are respected and accorded substantial deference, particularly if the evidence sought relates to non-party individuals residing abroad.

XIII. RULE 45 SHOULD PROVIDE EXPLICIT REQUIREMENTS FOR PROTECTING PERSONAL AND CONFIDENTIAL INFORMATION FROM DISCLOSURE AND SET OBJECTIVE STANDARDS FOR QUASHING SUBPOENAS THAT FAIL TO MEET THOSE STANDARDS

Although Rule 45 acknowledges an important need to protect "a person subject to the subpoena,"[80] it makes no mention of privacy rights, which today are considerations that are at least if not even more pressing than the considerations enumerated in the rule. "[C]ourts should be careful to protect against discovery that implicates privacy of third parties."[81] It is insufficient in today's digitized world to put the burden on subpoena recipients, particularly those who are innocent bystanders to the litigation, to bring affirmative motions to quash whenever a subpoena requests information that is personal, confidential, and/or subject to legal protections. It is also important to note that "private litigants may have little incentive to incur security costs to protect third-party information."[82] Additionally, it is unthinkable to require the production of such information, even when necessary for the case, to a party that fails to take reasonable steps to protect that information from unauthorized access, use, or disclosure. The issuers of subpoenas, not solely the recipients, have responsibilities to exercise due care in the scope of information requests and in the handling of personal and confidential data produced due to their requests. Accordingly, Rule 45 should be amended to clarify that protecting "a person subject to the subpoena" begins with the issuer's duties to minimize and protect personal information and includes enumerating specific privacy factors for quashing an overreaching subpoena. An amendment should include the following elements:

Rule 45 – Subpoena

***

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions.

(A) A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. At a minimum, this requires the issuing party or attorney to:

[80] FED. R. CIV. P. 45(d).

[81] Stuart, *supra* note 3, at 724.

[82] Boliek, *supra* note 19, at 1108.

(i) ensure the subpoena will not result in the unnecessary use or disclosure of personal or other confidential information, including any personal information that is subject to federal, state, or foreign data protection laws; and,

(ii) undertake reasonable and appropriate steps to protect personal and confidential information, including personal information relating to parties and non-parties, from unauthorized access, use or disclosure after production of such information to the requesting party or attorney.

(B) The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings, ~~and~~ reasonable attorney's fees, costs, and reimbursement of reasonable expenses incurred by the responding party or any individual person harmed as a result of noncompliance—on a party or attorney who fails to comply.

***

CONCLUSION

Any notion that the FRCP do not protect privacy[83] is untenable in the digital age – and in fact, has never been true.[84] The FRCP have a critical role in guiding courts, parties, and non-parties to fulfill their obligations to protect privacy rights while balancing those duties with the needs of particular cases. Unfortunately, the FRCP are failing to provide sufficient guidance to courts and parties on the privacy and cyber security issues that are now intrinsic and recurring in litigation. The two FRCP rules that have any relevance to the problems – rules 5.2 and 26(c) – are not only outdated but also inherently lack the dimension necessary to give courts and parties adequate structure for proactively considering, minimizing, and handling the complexities of personal and confidential information in litigation.

The suggested amendments discussed above and attached in the appendix are needed because they address critical and frequent privacy issues. At the same time, they are modest because they reflect best practices that have already developed among forward-thinking judges and practitioners. While discovery is appropriately focused on obtaining and disclosing information relevant to the claims and defenses in the case, FRCP guidance is needed to ensure that courts and parties balance that purpose with the legal, commercial, personal, and reputational peril that

[83] *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 30 (1984) ("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").

[84] *Id*. at 35 n.21 ("[a]lthough the Rule [26(c)] contains no specific reference to privacy or to other rights or interests that may be implicated, such matters are implicit in the broad purpose and language of the Rule"). *See also*, Boliek, *supra* note 19, at 1127 ("Indeed, for more than eighty years, courts have recognized the burden imposed on private parties when their personal, private information is disclosed as part of a discovery request" (footnote omitted) *and* Francis, *supra* note 45, at 401 ("for decades courts have routinely limited discovery based on the private nature of the information sought, sometimes even characterizing the right of privacy as 'constitutionally-based.' Courts have traditionally relied upon Rule 26(c) to protect privacy." (footnotes omitted)).

inherently exists when an increasingly large amount of information is requested, produced, duplicated, stored, shared, and used in litigation.

Appendix

Rule 1. Scope and Purpose

These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding, and to protect the reasonable expectations of privacy and confidentiality of parties and non-parties.

Rule 5.2. Privacy Protection For Filings Made with the Court

(a) Redacted Filings. Unless the court orders otherwise, in an electronic or paper filing with the court, a party:

(1) may redact personal information protected by federal, state, or foreign privacy laws; and

(2) shall redact sensitive personal information consisting of an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number; a party or nonparty making such filing may include only:

(~~1~~a) the last four digits of the social-security number and taxpayer-identification number;
(~~2~~b) the year of the individual's birth;
(~~3~~c) the minor's initials; and
(~~4~~d) the last four digits of the financial-account number.

***

(e) Protective Orders. For good cause, the court may by order in a case:

(1) require redaction of additional information; or

(2) limit or prohibit a nonparty's ~~remote electronic~~ access to a document filed with the court.

(f) Option for Additional Unredacted Filing Under Seal. For good cause, the court may by order in a case allow a~~A~~ person making a redacted filing ~~may also~~ to file an unredacted copy under seal. The court must retain the unredacted copy as part of the record.

***

(i) Considerations. When the court is considering the sealing or unsealing of documents filed with the court, or whether to order discovery or disclosure under Rule 26, including the issuance of a protective order, the court shall consider: (a) whether the court or requesting party can provide reasonable and appropriate protection against unauthorized access or disclosure; (b) the

rights and interests of parties and non-parties in maintaining the privacy and confidentiality of information pertaining to them; (c) the burdens on parties and non-parties, including whether those burdens are proportional to the needs of the case; (d) whether the information to be redacted is protected by federal, state, or foreign privacy laws; and (e) whether the information to be redacted is subject to a contractual confidentiality obligation or non-disclosure agreement.

Rule 16. Pretrial Conferences; Scheduling; Management

***

(b) Scheduling.

***

(3) *Contents of the Order.*

(A) *Required Contents.* The scheduling order must limit the time to join other parties, amend the pleadings, complete discovery, and file motions.

(B) *Permitted Contents.* The scheduling order may:

(i) modify the timing of disclosures under Rules 26(a) and 26(e)(1);
(ii) modify the extent of discovery;
(iii) provide for disclosure, discovery, or preservation of electronically stored information;
(iv) include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced, including agreements reached under Federal Rule of Evidence 502;
(v) direct that before moving for an order relating to discovery, the movant must request a conference with the court;
(vi) set dates for pretrial conferences and for trial; ~~and~~
(vii) provide measures for protecting personal and confidential information related to both parties and non-parties, including any personal information subject to federal, state, or foreign data privacy laws, from unnecessary use, disclosure or unauthorized access during the proceeding;
(viii) provide for reasonable and appropriate cybersecurity measures to prevent unauthorized access, use or disclosure of any information produced or disclosed by a party or a non-party during the proceeding;
(ix) direct that, at the conclusion of the proceeding, information disclosed during the proceeding be returned or securely destroyed; and
(~~vii~~x) include other appropriate matters.

***

(c) Attendance and Matters for Consideration at a Pretrial Conference.

***

(2) *Matters for Consideration.* At any pretrial conference, the court may consider and take appropriate action on the following matters:

(A) formulating and simplifying the issues, and eliminating frivolous claims or defenses;
(B) amending the pleadings if necessary or desirable;
(C) obtaining admissions and stipulations about facts and documents to avoid unnecessary proof, and ruling in advance on the admissibility of evidence;
(D) avoiding unnecessary proof and cumulative evidence, and limiting the use of testimony under Federal Rule of Evidence 702;
(E) determining the appropriateness and timing of summary adjudication under Rule 56;
(F) controlling and scheduling discovery, including orders affecting disclosures and discovery under Rule 26 and Rules 29 through 37;
(G) identifying witnesses and documents, scheduling the filing and exchange of any pretrial briefs, and setting dates for further conferences and for trial;
(H) referring matters to a magistrate judge or a master;
(I) settling the case and using special procedures to assist in resolving the dispute when authorized by statute or local rule;
(J) determining the form and content of the pretrial order;
(K) disposing of pending motions;
(L) adopting special procedures for managing potentially difficult or protracted actions that may involve complex issues, multiple parties, difficult legal questions, or unusual proof problems;
(M) ordering a separate trial under Rule 42(b) of a claim, counterclaim, crossclaim, third-party claim, or particular issue;
(N) ordering the presentation of evidence early in the trial on a manageable issue that might, on the evidence, be the basis for a judgment as a matter of law under Rule 50(a) or a judgment on partial findings under Rule 52(c);
(O) establishing a reasonable limit on the time allowed to present evidence; ~~and~~
(P) determining reasonable procedures for protecting personal and confidential information from unnecessary use, disclosure, or unauthorized access, including any personal information subject to federal, state, or foreign data protection laws; and
(~~P~~Q) facilitating in other ways the just, speedy, and inexpensive disposition of the action.

***

Rule 23. Class Actions

(a) Prerequisites. One or more members of a class may sue or be sued as representative parties on behalf of all members only if:
(1) the class is so numerous that joinder of all members is impracticable;
(2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class;

(4) the representative parties will fairly and adequately protect the interests of the class, and
(5) the action can be brought in a manner that does not unreasonably infringe the privacy rights of putative class members, unnamed class members and non-parties to the action, including the right of each class member or putative class member to prevent the disclosure of any personal identifying information to class counsel without explicit written consent in advance to such disclosure.

***

(c) Certification Order; Notice to Class Members; Judgment; Issues Classes; Subclasses.
(1) *Certification Order*.
(A) *Time to Issue*. At an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action.
(B) *Defining the Class*; Appointing Class Counsel. An order that certifies a class action must define the class and the class claims, issues, or defenses, and must appoint class counsel under Rule 23(g).
(C) *Confirming Protection of Privacy and Information Security*. An order that certifies a class action must detail the specific measures that will be taken by the parties to:
(i) ensure personal information related to parties and non-parties, including unnamed class members, is accessed, used and disclosed no more than is strictly necessary to facilitate the just resolution of claims and defenses in the action;
(ii) ensure any personal information protected by federal, state, or foreign data protection laws is used or disclosed only in a manner consistent with such laws; and,
(ii) ensure reasonable and appropriate protection from unauthorized access, use or disclosure of personal or otherwise confidential information during the action and upon its conclusion.
(~~C~~D) *Altering or Amending the Order*. An order that grants or denies class certification may be altered or amended before final judgment.
(2) *Notice*.
(A) For (b)(1) or (b)(2) Classes. For any class certified under Rule 23(b)(1) or (b)(2), the court may direct appropriate notice to the class.
(B) For (b)(3) Classes. For any class certified under Rule 23(b)(3)—or upon ordering notice under Rule 23(e)(1) to a class proposed to be certified for purposes of settlement under Rule 23(b)(3)—the court must direct to class members the best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort. The notice may be by one or more of the following: United States mail, electronic means, or other appropriate means. The notice must clearly and concisely state in plain, easily understood language:
(i) the nature of the action;
(ii) the definition of the class certified;
(iii) the class claims, issues, or defenses;
(iv) the types of information related to individual class members that will be used or disclosed in the action, including during discovery, and to whom such information will be disclosed;

(~~i~~v) that a class member may enter an appearance through an attorney if the member so desires;
(vi) that the court will exclude from the class any member who requests exclusion;
(vii) the time and manner for requesting exclusion; and
(viii) the binding effect of a class judgment on members under Rule 23(c)(3).

***

(d) Conducting the Action.

***

(3) *Privacy and Information Security*. The court shall at all times safeguard the privacy rights of parties and non-parties, including the rights of unnamed class members. At a minimum, this will require the court to establish reasonable and appropriate procedures for protecting personal or other confidential information from unnecessary use, disclosure, and unauthorized access or disclosure, including any personal information subject to federal, state, or foreign data privacy laws. In making determinations related to this provision, the court must never presume that unnamed class members or non-parties would want information about them used or disclosed to facilitate the action or during its pendency.

(e) Settlement, Voluntary Dismissal, or Compromise. The claims, issues, or defenses of a certified class—or a class proposed to be certified for purposes of settlement—may be settled, voluntarily dismissed, or compromised only with the court's approval.

The following procedures apply to a proposed settlement, voluntary dismissal, or compromise:

(1) *Notice to the Class*.

***

(2) *Approval of the Proposal*. If the proposal would bind class members, the court may approve it only after a hearing and only on finding that it is fair, reasonable, and adequate after considering whether:
(A) the class representatives and class counsel have adequately represented the class;
(B) the proposal was negotiated at arm's length;
(C) the relief provided for the class is adequate, taking into account:
(i) the costs, risks, and delay of trial and appeal;
(ii) the effectiveness of any proposed method of distributing relief to the class, including the method of processing class-member claims;
(iii) the terms of any proposed award of attorney's fees, including timing of payment; and
(iv) any agreement required to be identified under Rule 23(e)(3);

(D) the proposal treats class members equitably relative to each other; and
(E) the proposal contains sufficient provisions for the return or secure destruction of all personal and confidential information, including personal information relating to unnamed class members and confidential information belonging to the parties, exchanged during the litigation.

***

(g) Class Counsel.

(1) Appointing Class Counsel. Unless a statute provides otherwise, a court that certifies a class must appoint class counsel. In appointing class counsel, the court:

(A) must consider:

(i) the work counsel has done in identifying or investigating potential claims in the action;
(ii) counsel's experience in handling class actions,
other complex litigation, and the types of claims asserted in the action;
(iii) counsel's knowledge of the applicable law;
(iv) the resources that counsel will commit to representing the class;
(v) counsel's ability to protect the privacy interests of putative and unnamed class members, including personal information and all parties' confidential information; and,
(vi) counsel's ability to provide reasonable and appropriate cyber security protections for all systems used in the litigation for accessing, viewing, sharing, communicating, or storing such information.

(B) may consider any other matter pertinent to counsel's ability to fairly and adequately represent the interests of the class;
(C) may order potential class counsel to provide information on any subject pertinent to the appointment and to propose terms for attorney's fees and nontaxable costs;
(D) may include in the appointing order provisions about the award of attorney's fees or nontaxable costs under Rule 23(h); and
(E) may make further orders in connection with the appointment.

(2) *Standard for Appointing Class Counsel*. When one applicant seeks appointment as class counsel, the court may appoint that applicant only if the applicant is adequate under Rule 23(g)(1) and (4). If more than one adequate applicant seeks appointment, the court must appoint the applicant best able to represent the interests of the class.
(3) Interim Counsel. The court may designate interim counsel to act on behalf of a putative class before determining whether to certify the action as a class action.
(4) Duty of Class Counsel. Class counsel must fairly and adequately represent the interests of the class, including protecting personal information related to each class member.

***

Rule 26. Duty to Disclose; General Provisions Governing Discovery

(a) Required Disclosures.

(1) Initial Disclosure.

***

(F) *Limits on Initial Disclosure for Privacy and Information Security*. A party's initial disclosures need not include information protected by federal, state, or foreign privacy laws, including confidential information or personal information if the recipient has not taken reasonable and appropriate steps to ensure that such information is not subject to unauthorized access, use or disclosure. A party relying on this provision must expressly so state in their initial disclosures. These limits also apply to Rule 26(e) supplementation of initial disclosures.

***

(3) Pretrial Disclosures.

(A) In General. In addition to the disclosures required by Rule 26(a)(1) and (2), a party must provide to the other parties and promptly file the following information about the evidence that it may present at trial other than solely for impeachment:

(i) the name and, if not previously provided, the address and telephone number of each witness—separately identifying those the party expects to present and those it may call if the need arises, subject to the considerations outlined in Rule 5.2(i);

(ii) the designation of those witnesses whose testimony the party expects to present by deposition and, if not taken stenographically, a transcript of the pertinent parts of the deposition; and

(iii) an identification of each document or other exhibit, including summaries of other evidence—separately identifying those items the party expects to offer and those it may offer if the need arises.

***

(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, the parties' resources, the importance of the discovery in resolving the issues, the privacy rights held by parties and non-parties, the risk of unauthorized access to, or use of, personal or confidential information, the harm such unauthorized access or use would cause, 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.

(2) *Limitations on Frequency and Extent.*

***

(C) *When Required*. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; ~~or~~

(iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1);

(iv) the discovery sought would require the disclosure of personal information related to parties or non-parties beyond what is strictly necessary to facilitate the action, would violate any federal, state or foreign data privacy law, or otherwise infringes on reasonable privacy expectations held by parties or non-parties; or,

(v) the discovery sought poses an unreasonable risk of unauthorized access, use or disclosure of personal or other confidential information.

***

(4) Trial Preparation: Experts.

(A) Deposition of an Expert Who May Testify. A party may depose any person who has been identified as an expert whose opinions may be presented at trial. If Rule 26(a)(2)(B) requires a report from the expert, the deposition may be conducted only after the report is provided. A party deposing an expert should take reasonable and appropriate measures to protect against disclosure of personal or confidential information relating to parties or non-parties.

***

(c) Protective Orders.

(1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

(A) forbidding the disclosure or discovery;

(B) specifying terms, including time and place or the allocation of expenses, for the disclosure or discovery;

(C) prescribing a discovery method other than the one selected by the party seeking discovery;

(D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters;

(E) designating the persons who may be present while the discovery is conducted;

(F) requiring that a deposition be sealed and opened only on court order;

(G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way; ~~and~~

(H) requiring that the parties simultaneously file specified documents or information in sealed envelopes, to be opened as the court directs; and

(I) requiring that personal and confidential information not be revealed or be revealed only in a specified manner and that reasonable and appropriate steps be taken to avoid placing it at risk of unauthorized access, use or disclosure.

***

(f) Conference of the Parties; Planning for Discovery.

***

(3) *Discovery Plan.* A discovery plan must state the parties' views and proposals on:

(A) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement of when initial disclosures were made or will be made;
(B) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;
(C) any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;
(D) any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502;
(E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; ~~and~~

(F) how the use of personal and confidential information will be minimized, including through the use of data anonymization, pseudonymization, encryption and redactions;
(G) how data disclosed or used in the proceeding will be protected from unauthorized access, use, or disclosure, and how the privacy rights of parties and non-parties covered by federal, state, and foreign data privacy laws will be protected; and
(HF) any other orders that the court should issue under Rule 5.2, Rule 26(c) or under Rule 16(b) and (c).

* * *

(g) Signing Disclosures and Discovery Requests, Responses, and Objections.

(1) Signature Required; Effect of Signature. Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must state the signer's address, email address, and telephone number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

(A) with respect to a disclosure, it is complete and correct as of the time it is made; and that reasonable efforts have been made to avoid unnecessary use of personal or confidential information, including any personal information subject to federal, state, or foreign data privacy laws; and
(B) with respect to a discovery request, response, or objection, it is:
(i) is consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;
(ii) will not be interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
(iii) will not result in unnecessary access to, use, or disclosure of, personal or other confidential information, including any personal information subject to federal, state, or foreign data privacy laws;
(iiiiv) is neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action; and,
(v) will not require the production of personal or other confidential information until the requesting party and its attorneys have each implemented reasonable and appropriate cybersecurity protections for such information, including having in place a written data breach response plan.

***

Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes

***

(b) Procedure.

***

(2) *Responses and Objections*.

***

(E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

(i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; ~~and~~

(iii) A party need not produce the same electronically stored information in more than one form~~.~~; and

(iv) A party may produce personal or confidential ESI by providing the requesting party with access to a secure data escrow service or other secure digital environment in which the ESI can be securely reviewed, provided such service permits the export of exhibits for use during depositions and in court filings;

(v) A party may object based on plausible concerns about the adequacy of the methods anticipated to be used by the requesting party or other recipients to prevent unauthorized access to, or use of, personal information or other confidential and proprietary information; and

(vi) A party need not produce documents or electronically stored information without having received adequate assurances that any personal information or other confidential and property information will be reasonably and adequately protected from unauthorized access or disclosure upon such transfer.

***

Rule 37. Failure to Make Disclosures or to Cooperate in Discovery; Sanctions

***

(g) Failure to Provide Adequate Protection for Personal and Confidential Information. If unauthorized access to, or disclosure of, personal or confidential information during litigation is caused by the receiving party's failure to take reasonable and appropriate steps to comply with the obligations imposed by these rules, the court may require that party, the attorney advising that party, or both, to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.

Rule 44.1 Determining Foreign Law

(a) A party who intends to raise an issue about a foreign country's law must give notice by a pleading or other writing. In determining foreign law, the court may consider any relevant material or source, including testimony, whether or not submitted by a party or admissible under the Federal Rules of Evidence. The court's determination must be treated as a ruling on a question of law.

(b) When evidence is sought from a foreign country and the laws of that country create a right to privacy held by individuals residing therein that conflicts with US law, or the law of that country places restrictions on the transfer of data outside the country, the court must ensure such privacy rights are respected and accorded substantial deference, particularly if the evidence sought relates to non-party individuals residing abroad.

Rule 45. Subpoena

***

(d) Protecting A Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions.

(A) A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. At a minimum, this requires the issuing party or attorney to:

(i) ensure the subpoena will not result in the unnecessary use or disclosure of personal or other confidential information, including any personal information that is subject to federal, state, or foreign data protection laws; and,

(ii) undertake reasonable and appropriate steps to protect personal and confidential information, including personal information relating to parties and

non-parties, from unauthorized access, use or disclosure after production of such information to the requesting party or attorney.

(B) The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings, ~~and~~ reasonable attorney's fees, costs, and reimbursement of reasonable expenses incurred by the responding party or any individual person harmed as a result of noncompliance—on a party or attorney who fails to comply.

***