Consilio / ADVANCED LEARNING INSTITUTE

Consilio Symposium 2023

# YOU MAY APPROACH THE BENCH: JUDICIAL PERSPECTIVES ON CURRENT ISSUES

## CLE HANDOUTS

# CONTENTS

**Off-Channel Communication Discussion – PCC and Reasonable Steps**

- Matthew Verga, "When the Needles Aren't in the Haystack: Off-Channel Communications," Consilio Advanced Learning Institute (May 8, 2023).
- *In re Pork Antitrust Litigation*, 2022 WL 972401 (D. Minn. Mar. 31, 2022).
- *La Belle v. Barclays Capital Inc.*, 340 F.R.D. 74 (S.D.N.Y. Jan. 13, 2022).
- U.S. Department of Justice, "Evaluation of Corporate Compliance Programs (Updated March 2023)" 17-18 (Mar. 3, 2023).
- Deputy Attorney General Lisa Monaco, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group," U.S. Department of Justice (Sept. 15, 2022).

**Production Issues Discussions – New Sources Raising New Questions**

- Staci Kaliner, Monica McCarroll, and Ben Barnes, "Let's Start by Calling Them What They Are for Discovery: 'Pointers' Not 'Modern Attachments,'" Legaltech News (Aug. 11, 2022).
- *Famulare v. Gannett Co.*, 2022 WL 815818 (D.N.J. Mar. 17, 2022).
- Matthew Verga, "Emoji in eDiscovery: Technical and Interpretive Challenges," Consilio Advanced Learning Institute (July 2021).
- Matthew Verga, "How Should Productions of Mobile Device Messages Be Formatted?," Consilio Advanced Learning Institute (July 2021).

**Proportionality Discussion – An Underutilized Tool?**

- Kevin Brzozowski, Stuart Claire, and Jason Froehlich, "Takeaways from Georgetown Law's AEDI Keynote," JD Supra (Dec. 13, 2022).
- Allyson Haynes Stuart, "A Right to Privacy for Modern Discovery," 29 GEO. MASON L. REV. (Issue 3, 2022).
- *In re Pork Antitrust Litigation*, 2022 WL 972401 (D. Minn. Mar. 31, 2022).
- *Benebone v. Pet Qwerks, et al.*, 2021 WL 831025 (C.D. Cal. Feb. 18, 2021).

**Rule 502(d) Discussion – An Overlooked Safety Net**

- Fed. R. Evid. 502.
- Hon. Andrew J. Peck (ret.), Draft 502(d) Order Governing ESI.
- Isha Marathe, "The E-Discovery 502(d)ilemma: Attorneys Continue to Neglect an 'Amazing Level of Protection,'" Legaltech News (Feb. 24, 2023).

Consilio / ADVANCED LEARNING INSTITUTE

# WHEN THE NEEDLES AREN'T IN THE HAYSTACK: OFF-CHANNEL COMMUNICATIONS

*by Matthew Verga, Director of Education*

Never have there been so many communication devices, apps, and services available for use by employees – more than any company can evaluate and implement. When a company's employees choose to help themselves to these options and use communication channels beyond those approved for their use, those communications are known as off-channel communications, and they can present significant identification, preservation, and collection challenges.

## Off-Channel Communications

Off-channel communications occur in three main ways:

- First, employees may utilize unapproved apps or services on company-owned devices.
  - For example, an employee might download Slack or sign up for Signal using their company-issued laptop or smartphone, despite them being prohibited.
- Second, employees may utilize approved personal devices in unapproved ways.
  - For example, using a personal smartphone approved under a BYOD program to engage in business communications via text message, which is not permitted by company policy.
- Third, employees may utilize unapproved personal devices.
  - For example, an employee with a work-issued smartphone might choose to engage in business communications using their personal smartphone instead.

## Growing Importance

Whenever a reasonable anticipation of litigation arises, parties have a common law duty to preserve[1] any unique, potentially-relevant documents in their possession, custody, or control.[2] The existence of unknown unknowns like off-channel communications can make it difficult for companies to fulfill this duty – as well as to fulfill the compliance obligations applicable to regulated companies, such as those in the financial services industry.[3]

Failure to address off-channel communications in discovery projects and compliance plans risks significant costs and complications. In civil litigation, the risks range from expensive motion practice and supplementary discovery to actual spoliation sanctions. In regulatory compliance, the risks have grown dramatically as federal agencies have made this a recent focus.

Over the past year, federal agencies have begun making examples of regulated companies that did not adequately address their employees' use of off-channel communications, with total fines exceeding $1.2 billion.[4] Since then, the Department of Justice has also revised its guidance on "Evaluation of Corporate Compliance Programs" to emphasize the importance of addressing off-channel communications.[5] In announcing the new policy, the Assistant Attorney General for the Criminal Division said that, "[d]uring the investigation if a company has not produced communications from those third-party messaging applications, our prosecutors will not accept that representation purely at face value."[6]

[1]See Margaret M Koesel & Tracey L Turnbull, *SPOLIATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION* 1-6 (3rd Ed. 2013), available at https://www.americanbar.org/content/dam/aba-cms-dotorg/products/inv/book/214612/Chapter%201.pdf.
[2]See Fed R. Civ. P. 26, Fed. R. Evid. 401, and Fed. R. Civ. P. 34.
[3]See, e.g., Securities Exchange Act Rule 17a-4(b)(4), Investment Advisers Act Rule 204-2(a)(7), Financial Industry Regulatory Authority Rule 4511.
[4]Neil T. Smith, Hayley Trahan-Liptak, Christopher F. Warner, Peter W. Shanley, "Message Received: SEC Zeros in on Off-Channel Communication," K&L Gates HUB (Feb. 14, 2023), available at https://www.klgates.com/Message-Received-SEC-Zeros-In-On-Off-Channel-Communication-2-14-2023.
[5]U.S. Department of Justice, "Evaluation of Corporate Compliance Programs (Updated March 2023)" 17-18 (Mar. 3, 2023), available at https://www.justice.gov/criminal-fraud/page/file/937501/download.
[6]Ben Penn, "DOJ Getting Tougher with Companies on Messaging App Evidence," Bloomberg Law (Mar. 3, 2023), available at https://news.bloomberglaw.com/us-law-week/doj-gets-tougher-with-corporations-on-messaging-app-evidence.

## Logistical and Technical Challenges

As noted above, off-channel communications can present significant identification, preservation, and collection challenges:

- Identification
  - First and foremost is the challenge of identifying such communications. Since they are unknown unknowns, occurring in channels not approved and preserved by the company, investigative steps must be taken to check for them. Employee surveys and custodian interviews are commonly used to gather this sort of information and eliminate blind spots.
- Preservation
  - Since these communications are on apps, services, or devices the company doesn't administer, its preservation options may be limited. For example, it cannot control retention settings on a personal account on a third-party service, and it cannot simply swap out an employee's personal smartphone to lock away the current one. Preservation through collection is often the only safe option.
- Collection
  - Collection itself may also be complicated for the same reasons. Employees may be uncomfortable with granting the company access to their communication accounts or allowing the company to collect the data on their phone. Even when employees are cooperative, companies will still face the technical challenges always associated with collections from smartphones and communication apps, including access and export limitations, encryption, ephemerality, and more.

## Legal Complications

One legal complication created by the growth of off-channel communications, is uncertainty around how hard and how proactively companies must look for such communications. FRCP 37(e) requires that, before the application of curative measures or spoliation sanctions, there must be a showing that "a party failed to take reasonable steps to preserve" evidence it should have preserved. Once a party is on notice such materials exist, the reasonable steps are clear, but what about reasonable steps to look for off-channel communications in the first place?

In regulated industries, the regulations and enforcement guidance provide clarity around the high level of proactivity and efficacy that is expected and around the risks of noncompliance.[7] Things are less clear in civil litigation, however, where courts are still wrestling with when companies can safely assume their policies are being followed and when they must be more proactively investigatory in their approach.[8] Ignorance of the law is famously no defense, but ignorance of extant off-channel communications might be, in some situations.

Another legal complication that has arisen relates to possession, custody, or control. FRCP 34(a)(1) specifies that the scope of discovery and preservation extends not just to materials a company physically or electronically possesses, but also to any that it legally controls. But to what extent do employers "control" the messages and other data in their employees' personal accounts or on their personal smartphones and laptops?

Courts are still wrestling with this question as well. In 2022, one widely-discussed case[9] applied a multi-factor analysis that looked at the language of the applicable company policies, the technical realities of the company's BYOD program, and the general practices in the work relationship between employees and the company. That court found that the factors did not establish the defendant had "control over text messages on the personally-owned phones of its employees." That court also argued that a company should not be compelled to extort its employees, through the threat of termination, into surrendering personal devices for collection.

Please note that the resolution of possession, custody, or control questions may also depend on the jurisdiction, as there are multiple standards for how far it extends.[10]

[7] See, e.g., U.S. Department of Justice, "Evaluation of Corporate Compliance Programs (Updated March 2023)" 17-18 (Mar. 3, 2023), available at https://www.justice.gov/criminal-fraud/page/file/937501/download.
[8] See, e.g., *La Belle v. Barclays Capital Inc.*, 340 F.R.D. 74, 84 (S.D.N.Y. Jan. 13, 2022).
[9] *In re Pork Antitrust Litigation*, 2022 WL 972401 (D. Minn. Mar. 31, 2022), available at https://casetext.com/case/in-re-pork-antitrust-litig-5.
[10] See The Sedona Conference, *The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 468, 482 (2016), available at https://thesedonaconference.org/publication/Commentary_on_Rule_34_and_Rule_45_Possession_Custody_or_Control.

Consilio / ADVANCED LEARNING INSTITUTE

# KEY TAKEAWAYS

Never have there been so many communication devices, apps, and services available for use by employees, and employees helping themselves to these options can create significant identification, preservation, and collection challenges. Failure to meet those challenges can result in expensive motion practice and supplementary discovery, in actual spoliation sanctions, and in enforcement actions and fines from regulatory agencies. To minimize these risks, companies should carefully consider their policies and practices surrounding communication channels and become more proactive in checking for employee compliance with them.

## ABOUT THE AUTHOR

Matthew Verga is an attorney, consultant, and eDiscovery expert proficient at leveraging his legal experience, technical knowledge, and communication skills to make complex eDiscovery topics accessible to diverse audiences. A sixteen-year industry veteran, Matthew has mastered every phase of the EDRM and worked at every level, from the project trenches to enterprise program design. As Director of Education for Consilio, he leverages this background to produce engaging educational content to empower practitioners at all levels with knowledge they can use to improve their projects, their careers, and their organizations.

**Matthew Verga, Esq.**
Director of Education
**m** +1.704.582.2192
**e** matthew.verga@consilio.com
**consilio.com**

***Disclaimers***

*The information provided in this publication does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this publication are provided for general informational purposes only. While efforts to provide the most recently available information were made, information in this publication may not constitute the most up-to-date legal or other information.This publication contains links to third-party websites. Such links are only for the convenience of the reader; Consilio does not recommend or endorse the contents of the third-party sites.*

*Readers of this publication should contact their attorney to obtain advice with respect to any particular legal matter. No reader of this publication should act or refrain from acting on the basis of information in this book without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.*

*Use of this publication, or any of the links or resources contained within, does not create an attorney-client relationship between the reader and the author or Consilio. All liability with respect to actions taken or not taken based on the contents of this publication is expressly disclaimed. The content of this publication is provided "as is." No representations are made that the content is error-free.*

2022 WL 972401
Only the Westlaw citation is currently available.
United States District Court, D. Minnesota.

IN RE PORK ANTITRUST LITIGATION
This Document Relates To: All Class Actions

Case No. 18-cv-1776 (JRT/HB)
|
Signed 03/31/2022

**ORDER ON MOTION TO COMPEL HORMEL AND HORMEL CUSTODIANS TO PRODUCE RESPONSIVE TEXT MESSAGE CONTENT**

HILDY BOWBEER, United States Magistrate Judge

***1** This matter is before the court on Class Plaintiffs' Motion to Compel Hormel to Produce Responsive Text Message Content and to Enforce Subpoenas to Hormel Custodians. [ECF No. 883.] Plaintiffs seek an order: (1) compelling defendant Hormel Foods Corporation to produce the text message content of its currently employed custodians, including backup content stored on cloud services; (2) declaring Hormel had at the outset of the litigation an obligation to image text message content from all of its custodians' mobile devices and cloud backups, and an accompanying order for Hormel to do so now; and to the extent necessary (3) enforcing the subpoenas to the Hormel custodians for the same material. For the reasons set forth below, the Court grants in part and denies in part the motion.

**I. Background**

Plaintiffs in this coordinated multidistrict litigation, which includes several putative plaintiff classes and a number of "direct action plaintiffs," allege that Defendants, among America's largest pork producers and integrators, conspired to limit the supply of pork and thereby fix prices in violation of federal and state antitrust law. (See Oct. 20, 2020 Am. Mem. Op. & Ord. at 2 [ECF No. 520].) They allege Defendants were able to carry out the conspiracy in two ways: 1) by exchanging detailed, competitively sensitive, and closely guarded non-public information about prices, capacity, sales, volume, and demand through Agri Stats—a private service that gathers data from Defendants and produces market reports for paying subscribers; and 2) by signaling the need to cut production through public statements aimed at one another. (*Id.* at 6.) Plaintiffs allege that through these mechanisms, Defendants stabilized or increased the price of pork products from 2009 to the present.

In 2018, Class Plaintiffs requested that Hormel preserve data from personal cell phones of five company executives, James Snee, Jim Sheehan, Thomas Day, Steven Binder, and Cory Bollum, through forensic imaging. (Hormel Ex. 2 [ECF No. 929-1].) After objecting on several grounds, Hormel agreed to forensically image the phones. (Hormel Ex. 3 [ECF No. 929-2]; Hormel Ex. 4 [ECF No. 929-3].)

In 2019, Hormel and the Plaintiffs agreed to an ESI Protocol [ECF No. 292] and a Protocol for Preservation of Phone Records (Hormel Ex. 5 [ECF No. 929-4]). The Preservation Protocol applied to Hormel and its document custodians. Hormel initially identified seven document custodians. (Hormel Ex. 6 at 4 [ECF No. 929-5].) As a result of negotiations concluding in November 2020, the custodians now number thirty. (*See* Hormel Ex. 9 [ECF No. 929-8].) Seventeen are current employees; thirteen are former employees. (Custodians' Mem. at 2 [ECF No. 925].)

In November 2018, Plaintiffs served their first requests for production, in part seeking communications and meetings between the Defendants or related to the lawsuit's subject matter, and information regarding supply, demand, and price of pork products. (Bourne Decl. Ex. 5 at Requests 3–8, 14–19 [ECF Nos. 888-2].) It defined "document" to include text messages and cloud backups or archived text message data. (Bourne Decl. Ex. 5 at Definitions ¶¶ 8, 10.) Hormel objected that it did not have possession, custody, or control of the custodians' personal cell phone data. (Bourne Decl. Ex. 13 at 20 [ECF No. 888-2].) Hormel responded to the same effect to Plaintiffs' November 2020 interrogatories, which sought further information about the make, model, and use of the custodians' cell phones, though Hormel did provide the cell phone numbers of the custodians. (Bourne Decl. Ex. 4 at 20–23 [ECF 887-1].) On April 19, 2021, Plaintiffs asked whether Hormel had produced the text messages of two custodians' cell phones, to which Hormel responded that it did not have possession, custody, or control over those phones, so it would not produce those messages. (Bourne Decl. Ex. 6 [ECF No. 888-2].) Plaintiffs complained that Hormel had not alerted them earlier that it disclaimed control over those cell phones and insisted that Hormel produce the texts. (Bourne Decl. Exs.

7, 9 [ECF No. 888-2].) Hormel replied that it had complied with its duties under the phone record preservation protocol and general preservation obligation related to the personal cell phones outside its control. (Bourne Decl. Exs. 8, 10 [ECF No. 888-2].)

***2** While disagreeing with Hormel, Plaintiffs also subpoenaed the custodians directly for the information. (Bourne Decl. Ex. 17 [ECF No. 888-2].) The custodians' counsel interviewed each custodian to determine whether they might have potentially responsive communications on their cell phones. (Stephens Decl. ¶ 5 [ECF No. 926].) All of the custodians responded that they were currently using different phones from the phones they had used during the relevant time-period (January 1, 2008 – August 17, 2018). (Bourne Decl. Ex. 2.)[1] As summarized by the custodians' counsel,

> Of the thirty Subpoena Recipients, only a small group reported using their personal cell phones for work-related text communications external to Hormel during the relevant time period. More than half of those reported having their devices previously imaged. None of the Subpoena Recipients reported having any text communications with anyone outside of Hormel regarding supply and demand conditions in the pork industry. The vast majority of the Subpoena Recipients either did not use text messaging for work related communications or only used text messaging for communications with other Hormel employees.

(Stephens Decl. ¶ 8.) Somewhat more detail is provided in the information that was attached to the declaration of Plaintiffs' counsel. For purposes of this motion, the custodians' responses to the question of whether and to what extent they used their personal cell phones for work purposes and/or texted for work purposes, generally fell into five categories:

- Rarely communicated by text message for work-related matters: Cory Bollum, Donald Temperley, Eric Steinbach, Glenn Leitch, Holly LaVallie, James Fiala, and Jose Rojas.
- Did not communicate by text outside Hormel: Paul Bogle, Nathan Annis, Jerry Aldwell, Mark Coffey, Neal Hull, Steven Binder, Steven Venenga, and William Snyder, and Al Lieberum.
- Did not use text for communications of the nature sought by the subpoena: Jim Sheehan, Thomas Day, Jeff Ettinger, Jody Feragen, and James Snee.
- Never texted about work-related matters: Paul Peil, Lance Hoefflin, Alan Meiergerd, Jana Haynes, Jennifer Johnson, Michael Gyarmaty, Bryan Farnsworth, and Jesse Hyland.
- Never used their personal cell phone at all for work-related communications: Jessica Chenoweth.

(Bourne Decl. Ex. 1.) All custodians objected to the subpoenas. (Bourne Decl. Ex. 2.)

In further negotiations, Plaintiffs and the custodians discussed imaging the phones and allowing a forensic search with mutually agreed upon search terms. (Stephens Decl. ¶ 10.) Plaintiffs proposed that all phones be searched for all text messages sent to or received from 781 phone numbers associated with individuals affiliated with Hormel or any other Defendant or any of the other identified pork integrators, plus remaining texts containing any of 330 keywords, following which the custodians' counsel would review the results and produce relevant messages. (*Id.*, Ex. B [ECF No. 926-2]; Bourne Decl. ¶ 12 [ECF No. 887], Ex. 16 [ECF No. 888-2].) Plaintiffs demanded, however, that all "inter-defendant" text messages be produced without a further relevance review, on the ground that all such messages were relevant. (Stephens Decl. Ex. B.)

***3** Ultimately, the custodians maintained that Plaintiffs had not shown that all thirty custodians were likely to have texts responsive to the subpoenas, and that the proposed searches were overly broad and unduly burdensome. (Stephens Decl. ¶ 17.) The two sides also disagreed about which of them would bear the costs of the proposed searches. (Stephens Decl. ¶¶ 10, 17, Ex. B.)

Failing to reach an agreement with Hormel or the custodians, Plaintiffs filed this motion. Plaintiffs move this Court to compel Hormel to produce text message content relevant to its conspiracy claims within Hormel's possession, custody,

or control, in response to its requests for production seeking that information. They seek the same relief with regard to the custodians they subpoenaed.

Plaintiffs also seek a declaration that Hormel had from the outset of the litigation an obligation to image text message content from all of its custodians' mobile devices and cloud backups, and an accompanying order for Hormel to do so now.

**II. Whether Hormel Can Be Compelled to Produce Its Employees' Text Message Data**

Parties may obtain discovery that is

> relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

Fed. R. Civ. P. 26(b)(1). Rule 34 requires the production of any relevant and responsive documents in the responding party's possession, custody, or control, including text message content. *See, e.g.*, *Paisley Park v. Boxill*, 330 F.R.D. 226, 234 (D. Minn. 2019). Here, Hormel alleges that it does not have the requisite "possession, custody, or control" over the text messages sent by and to its employees on their personally-owned cell phones.

**A. The Meaning of "Control"**

Plaintiffs claim Hormel has failed to identify and produce relevant text message content from its document custodians over which Hormel has control. (Pls.' Mem. at 8 [ECF No. 885].) Hormel disputes control. While the Eighth Circuit has not weighed in, district courts in this Circuit have applied varying definitions of "control." Some have interpreted "control" to mean the legal right to obtain the documents. *See, e.g., Beyer v. Medico Ins. Group,* Case No. 08-CV-5058, 2009 WL 736759, at *5 (D.S.D. Mar. 17, 2009) ("The rule that has developed is that if a party 'has the legal right to obtain the document' then the document is within that party's 'control' and, thus, subject to production under Rule 34." (internal citation omitted)).

Other courts, including courts in this District, have held that "control" may also include the "practical ability" to obtain the documents. *See, e.g., Afremov v. Sulloway & Hollis, P.L.LC.*, Case No. 09-cv-03678 (PSJ/JSM), 2011 WL 13199154, at *2 (D. Minn. Dec. 2, 2011) (" 'Control' encompasses actual physical possession of the documents, but also the legal right or practical ability to demand the documents from a third party."); *In re Hallmark Cap. Corp.*, 534 F. Supp. 2d 981, 982 (D. Minn. 2008) ("documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action"); *Prokosch v. Catalina Lighting, Inc.*, 193 F.R.D. 633, 636 (D. Minn. 2000) (stating that "under Rule 34, control does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability, to obtain the documents from a non-party to the action" (quotations omitted), and directing the defendant to produce not only documents in its physical possession but also those that it was "capable of obtaining upon demand"); *New Alliance Bean & Grain Co. v. Anderson Commodities, Inc.,* Case No. 8:12-CV-197, 2013 WL 1869832, at *3 (D. Neb. May 2, 2013) ("documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action"); *Handi-Craft v. Action Trading, S.A.,* Case No. 4:02-CV-1731, 2003 WL 26098543, at *6 (E.D. Mo. Nov. 25, 2003) (holding that "the appropriate test is not of legal entitlement, but of control or practical ability to obtain the documents").

***4** Where the practical ability test is applied, the burden of demonstrating that the party from whom discovery is sought has the practical ability to obtain the documents at issue lies with the party seeking discovery. *New Alliance Bean & Grain,* 2013 WL 1869832, at *5. In assessing whether a party has the practical ability to obtain documents from a non-party, courts have focused on the "mutuality" of the responding party's relationship with the document owner, including whether the documents sought are considered records which the party is apt to request and obtain in the normal course of business, or whether the prior history of the case demonstrates cooperation by the non-party, including the production of documents and other assistance in conducting discovery, and the non-

party has a financial interest in the outcome of the litigation. *See Afremov*, 2011 WL 13199154, at *2 (D. Minn. Dec. 2, 2011) (collecting cases). The undersigned has also applied a practical ability analysis in ruling on a motion seeking to compel a U.S.-based party to produce documents in the possession of a Brazilian affiliate. Order, *M-I Drilling Fluids UK Ltd. v. Dynamic Air Inc.*, 14-cv-4857 (D. Minn. Nov. 13, 2015) [ECF No. 171].

That said, the Eighth Circuit has never decided whether the "legal right" or "practical ability" standard should govern, and other circuits are split on the issue. *See generally,* The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," 17 Sedona Conf. J. 467, 482-92 (2016) (collecting cases). Indeed, in part because of that variability, the Sedona Conference has urged adoption of a consistent, "reliable, objective approach" that defines control "as the legal right to obtain and produce the Documents and ESI on demand." *Id.* at 528. The Sedona Conference has criticized the "practical ability" standard on several grounds, including that its imprecision "has resulted in inconsistent and, at times, inequitable results in many contexts." *Id.* It describes the standard as "inherently vague," "unevenly applied," having the potential to lead to "disparate results," and potentially leading to inequitable or even "futile" results. To that last point, the commentary cites by way of example one court's observation that even if it were to order a party employer to collect and turn over personal emails of its employees, the moving party had not identified any authority under which the employer could *force* the employees to turn them over. *Id.* at 542 n. 126, citing *Matthew Enter., Inc. v. Chrysler Grp. LLC,* Case No. 13-cv-04236-BLF, 2015 WL 84982256 (N.D. Cal. Dec. 10, 2015).

Relatedly, the Ninth Circuit has recognized that "[o]rdering a party to produce documents that it does not have the legal right to obtain will oftentimes be futile, precisely because the party has no certain way of getting those documents." *In re Citric Acid Litig.*, 191 F.3d 1090, 1108 (9th Cir. 1999). And yet, a strong argument can be made that if a party's relationship with a non-party is such that the former routinely obtains certain kinds of documents from the latter in the ordinary course of business, and perhaps has already even leveraged that access to obtain documents for its own use in the litigation, fairness would require that it also be required to do so for purposes of responding to discovery. Order, *M-I Drilling*, 14-cv-4857, at 7–9.

In this case, however, the Court need not choose between the "legal right" and "practical ability" standard because, for the reasons discussed below, it finds that regardless of the standard applied, Plaintiffs have not shown that Hormel has control over text messages on the personally-owned phones of its employees.

### B. Whether Hormel's BYOD Policy Gives Hormel Control Over Text Messages on Personally-Owned Cell Phones

Plaintiffs argue that Hormel has control of the custodians' personal text messages because its "bring your own device" (BYOD) requires employees to use their cell phones to conduct business, and Hormel controls all data on those phones through the BYOD policy and the ability afforded as a result of that policy to wipe all data on personally-owned phones whenever it deems necessary. (Pls.' Mem. at 9–11.) Hormel responds that the BYOD policy does not give it the legal authority to access, view, image, or control the text messages, and therefore it lacks control over those messages. (Hormel Mem. at 12–13.)

***5** Hormel has had a BYOD policy since at least 2011.[2] (*See* Bourne Decl. Ex. 14 [ECF No. 887-1]; Hormel Ex. 1 [ECF No. 930].) The policy allows employees to use their personally-owned cell phones to interact remotely with certain Hormel corporate systems. (*See* Hormel Ex. 1 § A.) It also provides for employees who have a defined business need to be reimbursed for mobile device service for a personally-owned phone, although the employee is responsible for all costs associated with purchasing and maintaining the phone and any accessories, as well as the costs of any application downloads or purchases. (Hormel Ex. 1 at 4, 5 § B; Morrison Decl. ¶¶ 10, 15–16 [ECF No. 928].) Hormel claims ownership of all "data that is sourced from Hormel systems and synced between the mobile device and its servers." (*See* Hormel Ex. 1 at 6 § F; Morrison Decl. ¶¶ 7–8.) Such data "primarily consists of company email, calendars, and contacts (if set up through an employee's corporate email account)," but does not include "text messages or other information on a personally-owned device." (Morrison Decl. ¶¶ 8–9.) The policy does not explicitly assert ownership, control, or ability to access, inspect, copy, image, or limit personal text messages. (*See* Hormel Ex. 1 § F.)

Hormel requires an employee who accesses Hormel data using their personal phone to install the MobileIron application. (Morrison Decl. ¶¶ 11, 14, 18.) MobileIron

prevents an employee from copying or backing up Hormel-owned data residing on their phone. (Morrison Decl. ¶¶ 13–14.) It does not interfere with or limit the employee's ability to copy, delete, or back up text messages, nor does it enable Hormel to access or image text messages. (Morrison Decl. ¶¶ 18–20.) Through the BYOD policy, Hormel reserves the right to remotely remove MobileIron and the company data controlled by MobileIron, or to remotely wipe (i.e. factory reset) the phone in order to wipe all Hormel-owned data, but the policy warns that such a wipe may delete all data the phone, including personal data such as text messages. (Hormel Ex. 1 § F; Morrison Decl. ¶¶ 11–12.) However, following a wipe, the employee may freely restore any personal data he or she had previously backed up to external storage. (Morrison Decl. ¶ 17.)

Plaintiffs read the BYOD policy's provision that "[a]ll approved employees will be expected to use a personally-owned mobile device" to mean that all Hormel employees are required to own personal cell phones and to use them for business. (Pls.' Mem. at 8.) Plaintiffs misconstrue the policy by taking this statement out of its context. An employee must request Hormel's permission to use a personally-owned cell phone to access Hormel's systems, and may request that Hormel reimburse the employee for monthly carrier service charges. Hormel will approve such a request if it concludes the employee has a "defined business need" to use the phone in the ordinary course of his or her work for the company. (*See* Hormel Ex. 1 § A, App. A.) However, nothing in the policy appears to require any employee to use a personally-owned phone to conduct work, and nothing in the policy requires any employee who uses a personally-owned phone to use text messaging to conduct work.

Plaintiffs next argue Hormel's remote wipe ability gives it control over employee texts, but the Court disagrees. The MobileIron application does not give Hormel the ability to access, inspect, copy, or image text messages; it only gives Hormel the ability to wipe those messages as part of a remote factory reset of the phone if Hormel concludes the security of its own data on the phone has been put at risk and if it cannot limit the wipe to only company data. Similarly, the BYOD policy does not assert Hormel's ownership over any data other than data "sourced from Hormel systems and synced between the mobile device and its servers"—which does not include text messages (except, perhaps, if the employee copied data sourced from a Hormel system and embedded it in a text)—nor does it assert Hormel's right to demand that its employees allow it to access or inspect any other data. Hormel's right and ability to remotely wipe an entire phone is for the sole and express purpose of removing company data—such as in response to the phone being lost or stolen. The company's ability to wipe personal data from a personally-owned device by resetting the device to a factory floor state in order to purge company data does not give the company control—legal or practical—over that personal data. The Sedona Conference has taken the position that an employer does not legally control personal text messages despite a BYOD policy when the policy does not assert employer ownership over the texts and the employer cannot legally demand access to the texts. The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 Sedona Conf. J. 495, 531 (2018).

***6** The Court is not persuaded otherwise by *H.J. Heinz Co. v. Starr Surplus Lines Ins. Co*. Case No. 2:15-cv-00631-AJS, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015), *report and recommendation adopted*, 2015 WL 12792025 (W.D. Pa. July 31, 2015). (Pls.' Mem. at 9–10.) The special master in *Heinz* concluded that since Heinz's BYOD program provided that all company information and emails on both company-owned and personally-owned mobile devices were the sole property of the company, the company had custody and control of its own data on those devices. The special master did not, however, suggest that the control extended to any personal data on the phone. 2015 WL 12791338 at *4. Notably, the special master was not required to resolve the question of whether Heinz had control over text messages on personally-owned phones because the only such custodian specifically before the special master stated he did not use his personal phone to send or receive text messages related to substantive Heinz business. And while the special master recommended that the company be required to interview other custodians about the existence of any potentially relevant text messages on their phones and to produce such messages if they existed, it is not clear whether that requirement was limited to the scope of the underlying reasoning—i.e., text messages on company-owned phones and text messages on personally-owned phones that contained company data—or whether the special master assumed Heinz could require that its employees produce for inspection, review, and production text messages on personally-owned phones that did not include company-owned data (and if so, on what legal basis). Nothing in the special master's report and recommendation suggested, as Plaintiffs do here, that the company had overall control over text messages on an personally-owned cell phones.

Therefore, the Court is not persuaded by Plaintiffs' arguments that the BYOD policy gives Hormel control over the text messages on personally-owned cell phones.

**C. Whether the Relationship Between Hormel and the Custodians Gives Hormel Control Over Text Messages on Personally-Owned Cell Phones**

Plaintiffs argue that even if the BYOD policy did not give Hormel the legal right to demand access to text messages on personally-owned phones, the relationship between it and its employees gives it the practical ability to demand access to that data. Plaintiffs argue Hormel could have asked all of its custodians to give it access to text messages and all custodians likely would have agreed. They base that argument in part on the fact that Hormel had previously asked for and received permission to *image* (although not to inspect, copy, or produce the content of) the personal cell phones of five executive custodians: James Snee, Jim Sheehan, Thomas Day, Steven Binder, and Cory Bollum. (Tr. at 15–16 [ECF No. 945].) (Hormel Exs. 2–3; Bourne Ex. 1.)

The Court disagrees. It is one thing to show that a responding party may *ask* for documents in the possession of someone with whom it has a relationship, but quite another to conclude that the party has the practical ability to *demand* such documents, and therefore has "control" over them. The Court is particularly sensitive to this distinction in the context of the employment relationship. While one might argue that the employees' fear for their job security or interest in the financial well-being of the company will incentivize them to say "yes" to turning over their text messages for inspection and possible production is not, in the opinion of the undersigned, the kind of "practical ability" contemplated by that standard. Practical ability to demand access to documents has generally been found where the relationship between the party and non-party, and the types of data or documents at stake, give rise to the conclusion that the non-party would give (and often, has given) the party access to those data and documents in the ordinary course of business. *See, e.g.,* Order, *M-I Drilling*, 14-cv-4857, at 7–9; *Camden Iron & Metal, Inc. v. Marubeni Amer. Corp.,* 138 F.R.D. 438, 443 (D.N.J. 1991) ("The proper inquiry here is whether the documents sought are considered records which [the defendant subsidiary] is apt to request [from the non-party parent] and obtain in its normal course of business."); *Cooper Indus., Inc. v. British Aerospace,* 102 F.R.D. 918, 919–20 (S.D.N.Y. 1984) (holding that where the defendant was the distributor and servicer of the non-party affiliate's planes, it must produce certain documents in the possession of the affiliate, and noting that the documents sought "all relate to the planes that defendant works with every day; it is inconceivable that defendant would not have access to these documents and the ability to obtain them for its usual business.").

***7** Here, there is no evidence that in the ordinary course of business Hormel seeks, needs, or expects to gain access to the content of employees' text messages on their personally-owned phones. That five executives agreed to have their phones imaged for the purpose of preserving the data does not establish that Hormel has the practical ability to demand that it be allowed to inspect or produce the data, and it is no evidence at all that other custodians would be amenable to doing so. Plaintiffs contend that at least those custodians who are currently employed by Hormel will wish to help their employer in this case. (Tr. at 15–16.) But while those custodians may feel a sense of company loyalty and/or have an interest in the company's financial health, it goes too far to extrapolate from that a practical ability on Hormel's part to demand access to the data on their phones. *Cf. U.S. Intern. Trade Com'n v. ASAT, Inc.,* 411 F.3d 245, 255 (D.C. Cir. 2005) (rejecting the "untenable position" that simply because the parent may have a financial interest in the outcome of litigation involving its subsidiary, the subsidiary has the ability to control its parent's documents).

Similarly, the fact that Hormel employees willingly responded to questions from Hormel's counsel regarding whether and to what extent they conducted company business by use of personal text messages, (Tr. at 30–31), does not establish a practical ability to demand that the data on those telephones be turned over to Hormel for imaging, review and production. While Hormel owns, and therefore may have a legal right to demand, company data that resides on a personal cell phone—even if that data may reside in a text message—what Plaintiffs are demanding here is that Hormel leverage that putative right in order to demand access to *all* text messages so that it can review and produce those deemed responsive to discovery in this case, regardless of whether they include company data over which Hormel claims ownership per the BYOD policy. The Court shares the Sedona Conference's view that "organizations should not be compelled to terminate or threaten employees who refuse to turn over their devices for preservation or collection." 19 Sedona Conf. J. at 531.

Accordingly, the Court denies Plaintiff's motion insofar as it seeks to compel Hormel to collect, review, and produce

responsive text messages on its employees' personally-owned cell phones.

**III. Whether Plaintiffs' Subpoenas to Hormel's Employees and Former Employees Should Be Enforced**

Plaintiffs also move that the Court enforce their subpoenas directed to the custodians for text message information in their phones and cloud backups. (Pls.' Mem. at 14.) The scope of discovery for a Rule 45 subpoena is the same as the scope of discovery under Rules 34 and 26 and is subject to the same constraints on relevance and proportionality. *See* Fed. R. Civ. P. 34(c), 45; *Mille Lacs Band of Ojibwe v. Cty. of Mille Lacs*, No. 17-cv-5155 (SRN/LIB), 2020 WL 1847574, at *5 (D. Minn. Apr. 13, 2020); *Shukh v. Seagate Tech., LLC*, 295 F.R.D. 228, 236 (D. Minn. 2013). A person subject to a subpoena may object to the subpoena, as the custodians did here, in which case the requesting party may move the court to compel production. Fed. R. Civ. P. 45(d)(2)(B). (Custodians' Mem. at 7–8 [ECF No. 925].)

Under Rule 45(d)(1), even if the subpoena seeks relevant information, discovery is not permitted where it imposes an undue burden on the subpoenaed person, considering the same factors as those relied on for proportionality in Rule 26(b). *See Misc. Docket Matter No. 1 v. Misc. Docket Matter No. 2*, 197 F. 3d 922, 925 (8th Cir. 1999); *see also Deluxe Fin. Servs., LLC v. Shaw*, Case No. 16-cv-3065 (JRT/HB), 2017 WL 7369890, at *4 (D. Minn. Feb. 13, 2017) ("These considerations are echoed in the proportionality factors set forth in the amended Rule 26(b)(1)."). Concern for the burden on a non-party subject to a subpoena carries special weight when balancing competing needs. *Id.* The Court must quash or modify a subpoena that imposes an undue burden on the non-party or requests irrelevant information. Fed. R. Civ. P. 45(c)(3)(A)(iv).

***8** Neither party bears a rigid evidentiary burden in this dispute. The advisory committee notes for the 2015 amendments to Rule 26 advise that the parties and the Court bear "collective" responsibility to consider relevance and proportionality/undue burden. A party requesting production should be able to explain the ways the requested information bears on the issues of the case, while the person resisting production will ordinarily have much better or the only information about the burden and expense of production. *Id.* The Court does not place the burden of proving relevance or proportionality/undue burden on any party, but instead considers all the information brought by the parties to determine the appropriate scope of the subpoenas. *Deluxe Fin. Servs., LLC v. Shaw*, Case No. 16-cv-3065 (JRT/HB), 2017 WL 7369890, at *4 (D. Minn. Feb. 13, 2017). [3]

Plaintiffs' subpoenas made seven requests, and all custodians gave substantively the same response to each. (*See* Bourne Decl. Ex. 2.) Plaintiffs do not identify the specific requests for which they seek the motion to compel, but their arguments address the information requested by Requests 1 and 5, and they do not raise any issues with the custodians' responses to the other requests. (*Compare* Pls.' Mem. at 14-16, *with*, Bourne Decl. Ex. 17 Requests 1–7.) The Court accordingly confines its review to Requests Nos. 1 and 5. Those requests and the custodians' responses are as follows:

> **Request No. 1**: Produce a copy of each Text Message that you sent or received during the Relevant Time Period with an Employee or Representative of a Pork Integrator, or any other individual with whom you communicated about supply and demand conditions in the Pork industry.
>
> **Response:** [The custodian] objects to this request as vague and ambiguous, and overbroad and unduly burdensome to the extent it seeks information not relevant to any party's claims or defenses in this litigation, and is disproportionate to the needs of the case. [The custodian] objects to this request to the extent it imposes an undue burden on a non-party by seeking "each Text Message" exchanged with the identified individuals over a ten-year period that ended three years ago. [The custodian] further objects to this request to the extent it seeks information equally available from another source that would be less burdensome and more appropriate under the circumstances. Subject to and without waiving the foregoing objections, [the custodian] is not aware of any documents responsive to this request.
>
> ***9 Request No. 5**: Documents sufficient to show, and provide access to the forensic vendor for collection purposes, the location, date, and scope of any archived copies of your cellphone data, such as iTunes archives or iCloud archives.
>
> **Response**: [The custodian] objects to this request as vague and ambiguous, and overbroad and unduly burdensome to the extent it seeks information not relevant to any party's claims or defenses in this litigation, and is disproportionate to the needs of the case. [The custodian] objects to this request to the extent it imposes an undue burden on a non-party by seeking all archived cellphone data over an unreasonably long period of time.

(Bourne Decl. Ex. 2.) The custodians' explained their objections further in letters attached to the responses and during the motion hearing and in their memorandum opposing Plaintiffs' motion. (*Id.*; Custodians' Mem. at 10; Tr. at 45–48.) They objected that the subpoenas seek irrelevant information, are ambiguous and vague, and that information sought was equally available from their cell phone service providers; the subpoenas imposed an undue burden on them; the definition of "pork integrator" was overbroad and unduly burdensome; Plaintiffs had not shown that responsive texts were likely to exist on their phones or data backups; and there was no adequate protective order to protect private and confidential information on their phones. [4] (*See, e.g.*, Bourne Decl. Ex 2 at ECF 13–14, 18–19. *See also* Custodians' Mem. at 9–11; Tr. at 45–48.)

**A. Whether the Custodians' Have Adequately Demonstrated That They Do Not Have Responsive Texts**

Counsel for the custodians argue they have undertaken reasonable steps to investigate whether unique responsive information exists on any custodian's cell phone; both Hormel and the custodians argue that those inquiries have suggested that no such information exists, while Plaintiffs have not shown reason to conclude to the contrary. (Hormel Mem. at 25–28; Custodian's Mem. at 9–10; *see generally* Stephens Decl.)

A court may deny a motion to compel when the information sought is "almost certainly nonexistent or the object of pure speculation." *Struzyk v. Prudential Ins. Co. of Am.*, Case No. 99-1736 (JRT/FLN), 2003 WL 21302966, at *2 (D. Minn. May 16, 2003). A court will do so when evidence shows that the responding party has searched for the information but cannot find it or disclaims its existence after the search, and the movant shows no evidence to suggest the information exists. *See id.* (denying motion to compel where responding party argued that it produced all responsive documents and presented detailed affidavits of its efforts to locate any responsive documents, while the movant presented no contrary evidence); *Johnson v. Charps Welding & Fabricating, Inc.*, Case No. 14-cv-2081 (RHK/LIB), 2017 WL 9516243, at *11 (D. Minn. Mar. 3, 2017) (denying in part motion to compel where responding party agreed to produce certain responsive documents, argued that no additional related documents existed, and presented an affidavit describing the creation and storage of the documents, while the movant presented no contrary evidence); *compare Farmers Ins. Exch. v. West*, Case No. 11-cv-2297 (PAM/JJK), 2012 WL 12894845, at *5 (D. Minn. Sept. 21, 2012) (granting in part motion to compel where responding party disclaimed the existence of responsive documents, but the record failed to show that the party searched for them and the movant presented evidence suggesting that the documents existed).

***10** This standard strikes a balance between two interests in discovery. A responding party has a duty under the Federal Rules of Civil Procedure to affirmatively, reasonably search for responsive information available to it. *Farmers Ins. Exch.*, 2012 WL 12894845, at *5. But once it fulfills that responsibility, "[t]he Court must accept, at face value, a party's representation that it has fully produced all materials that are discoverable ... because the Court has no means to test the veracity of such avowals." *Bombardier Recreational Prod., Inc. v. Arctic Cat, Inc.*, Case No. 12-cv-2706 (MJD/LIB), 2014 WL 5685463, at *7 (D. Minn. Sept. 24, 2014).

Here, the custodians' counsel interviewed the custodians to ascertain whether it was likely that potentially relevant and responsive texts would be on their phones. They represent that in those interviews, all of the custodians disclaimed on one basis or another having any texts that might be responsive. (Bourne Decl. Exs. 1, 2; Stephens Decl. ¶¶ 5–8.) But with the exception of Jessica Chenowith, who stated unequivocally that she *never* used her personal cell phones for work-related communications, the Court cannot conclude from the responses that adequate steps were taken to describe to the custodians what kinds of communications might be relevant and responsive information in the context of this complex litigation, or to test the accuracy of their recall about whether, at some point over the relevant period or periods, they sent or received relevant or responsive texts.

Granted, the evidence that responsive texts *do* exist is quite weak. Plaintiffs declare under oath that they obtained records from a telephone service provider showing custodians Eric Steinbach, Holly LaVallie, James Fiala, Michael Gyarmaty, and Steven Venenga texted work-related contacts. (Pls.' Mem. at 15–16; Bourne Decl. ¶¶ 18–20.) But the provider had no information about the content of the messages, and the fact that the texts were sent to or from work-related contacts does not mean the content of the texts was work-related, let alone that the content was relevant to the claims or defenses in this case. Plaintiffs also argue that certain of the custodians —Paul Bogle, Corwyn Bollum, Jessica Chenoweth, Lance Hoefflin, Paul Peil, Jose Rojas, and Donald Temperley— worked with Agri Stats and/or managed the throughput of

pork in Hormel's operations, suggesting that they are more likely to have responsive texts. (Hormel Exs. 6, 8 at 2.) Several of them—Bogle, Bollum, Rojas, and Temperley—also implied or acknowledged in their subpoena responses that they used text messaging for business to some degree. (Bourne Decl. Ex. 1.)

Provided Chenowith submits to Plaintiffs a sworn declaration reiterating her unequivocal representation that she did not use her personal cell phone for work related communications at all, the Court concludes Chenowith has adequately shown that responsive texts on her cell phone or in her archived data are "almost certainly nonexistent or the object of pure speculation." *Struzyk*, 2003 WL 21302966, at *2. Unlike the other custodians, Chenowith alone appears to have observed a clear boundary about the use of her personal cell phone, and could say without qualification that she did not use it in any manner for work purposes. Plaintiffs have offered no evidence to the contrary. Accordingly, the Court will not enforce the subpoena directed to Chenowith with regard to Requests Nos. 1 and 5.

But as to the remaining custodians, the Court is not satisfied that the inquiries made by counsel and the resulting representations by the custodians adequately demonstrate that there was a reasonable search for responsive texts such that the Court can conclude such texts are almost certainly nonexistent. *See Farmers Ins. Exch.*, 2012 WL 12894845, at *5. All custodians but Chenowith either acknowledge they might have used their cell phones for work related communications, even if only minimally, or they made no representations at all on that subject. Nothing suggests the custodians did, or were asked to do, anything beyond consulting their memories about whether they might have sent or received responsive or relevant texts, or even that they understood the full scope of what kinds of communications that might encompass. No evidence suggests that anything was done to test their memories, which is particularly problematic given that the time periods are in some instances years in the past and text-messaging is by its very nature short, quick, often reactive, and therefore unlikely to be particularly memorable.

***11** Since for all custodians other than Chenowith, the evidence does not show a reasonable search or that responsive texts are "almost certainly nonexistent or the object of pure speculation" *Struzyk*, 2003 WL 21302966, at *2, this argument does not provide a basis for the Court to decline to enforce Requests Nos. 1 and 5 as to those custodians.

### B. Whether the Court Should Decline to Enforce the Requests Because They Are Vague or Ambiguous, or Because the Information is Available From Other Sources

The Court overrules the custodians' objections regarding vagueness and ambiguity, including with respect to the definition of "pork integrator," because they provide no arguments, explanation, or evidence to support those objections. *Mead Corp. v. Riverwood Nat. Res. Corp.*, 145 F.R.D. 512, 515 (D. Minn. 1992) ("[A]n objection to a discovery request cannot be merely conclusory, and ... intoning the 'overly broad and burdensome' litany, without more, does not express a valid objection.") Though the Court does not place an evidentiary burden on those objections, the Court cannot determine the grounds on which the custodians base these objections without some explanation to support them. Moreover, vagueness and ambiguity objections, even if otherwise well-taken, can be addressed in a meaningful meet-and-confer. These objections are therefore overruled.

The Court also overrules the objection that the information sought is equally available from the cell phone providers. Plaintiffs declare under oath that they obtained records from a telephone service carrier showing that custodians Eric Steinbach, Holly LaVallie, James Fiala, Michael Gyarmaty, and Steven Venenga sent texts to work-related contacts. (Pls.' Mem. at 15–16; Tr. at 13; Bourne Decl. ¶¶ 18–20.) The carrier did not record the content of any text messages, so the information is not available from that source. (Tr. at 14.) Plaintiffs also point out that carrier data would not reveal iMessage to iMessage content, as that content is only available on the respective iPhones. (Tr. at 51.) The custodians do not offer any concrete support for their claim that the content of any relevant and responsive text messages would be available from any other source. Thus, the record fails to substantiate this objection.

### C. Whether Imaging the Phones and Searching the Data Imposes an Undue Burden and is Disproportionate to the Needs of the Case

The custodians object that the very imposition of the requests for cell phone data imposes an undue burden on the custodians that is disproportionate to the needs of the case. (*See, e.g.*, Bourne Decl. Ex. 2 at ECF 13–14, 18–19. *See also* Custodians' Mem. at 9–11; Tr. at 45–48.). Undue burden in the subpoena context relies on similar factors to proportionality in the broader context of a motion to compel,

though courts have heightened concern for and reluctance to impose discovery burdens on a non-party compared to a party. *Deluxe Fin. Servs.*, 2017 WL 7369890, at *4. Any order compelling compliance with a subpoena "must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance." Fed. R. Civ. P. 45(d)(2)(B)(ii).

> An objection that discovery is overly broad and unduly burdensome must be supported by affidavits or offering evidence revealing the nature of the burden and why the discovery is objectionable. It is not sufficient to simply state that the discovery is overly broad and burdensome, nor is a claim that answering the discovery will require the objecting party to expend considerable time and effort analyzing 'huge volumes of documents and information' a sufficient factual basis for sustaining the objection.

***12** *Abhe & Svoboda, Inc. v. Hedley*, Case No. 15-cv-1952 (WMW/BRT), 2016 WL 11509914, at *3 n.5 (D. Minn. Mar. 15, 2016). Though the non-party resisting a subpoena is often in the best position to provide information to sustain its objection, the Court will examine all evidence in the record. *Id.* at *3.

The custodians argue burden along several lines. They allege that they have an estimate of between $65,000 and $85,000 in total to image all thirty phones [5], that imaging each phone will take between three hours and more than a day based on the amount of data on the phone, and that some number of them live out of state or in rural Minnesota and will have to mail their phones to Hormel's third-party forensic imaging provider. (Custodians' Mem. at 10; Tr. at 45–48.) They also argue the production will capture significant amounts of private and confidential information unrelated to this case. (*Id.*) The Court addresses these concerns in order.

First, as to the costs or time to image the phones, there are no affidavits or other evidence of record establishing the amount of data on any individual custodian's phone or the estimated time or cost to image it. Furthermore, it is not entirely clear to the Court that the cell phones would need to be imaged in their entirety, or whether text messages in particular can be extracted more economically. Nor is it clear to the Court that all cell phones would need to be imaged, given that currently used cell phones were not in use during the period from January 1, 2008 – August 17, 2018 and messaging data from prior phones may not have been carried over to the new phone. Furthermore, the custodians acknowledge that they have no estimate of the number of texts that might be captured and reviewed for relevance under Plaintiffs' proposed search method, nor do they seem to have explored other means of capturing and filtering the data more cost-effectively, so the Court cannot assess the time or cost for that aspect of the production process. The Court accepts in the abstract that the imaging may be costly, but it has no information on how custodians calculated their cost estimate or how much it might cost any particular custodian.

That said, the Court agrees with the custodians that of all the players in this mix, the individual custodians are least equipped to bear the financial burden of having their cell phones imaged. As discussed below in Section III.D., the Court will compel the custodians to search for and produce text messages within certain parameters, and to preserve data in the event this production, or other discovery, reveals a basis to expand the search. Consequently, the Court directs Plaintiffs' counsel, Hormel's counsel, and the custodians' counsel to meet and confer regarding which devices should be imaged, or from which devices text messaging data should be extracted by other means, taking into account the time period during which those devices were in service and whether older data was carried over.

***13** In addition, to the extent the result of those discussions results in the imaging of any cell phones, or the forensic extraction of text messaging data by other means, the Court exercises its discretion and orders that the reasonable costs associated with that imaging or data extractions must be split equally between the Class Plaintiffs, on the one hand, and Hormel, on the other. The Court further orders that the reasonable costs associated with conversion and storage of any data obtained from those phones as well as conversion and storage of any data obtained from archives or cloud storage be borne equally by the Class Plaintiffs and Hormel. The Court finds this cost-sharing arrangements appropriate as to Plaintiffs because Rule 45(d)(1) clearly places on the party serving the subpoena the obligation to avoid imposing undue burden or expense on the person subject to the subpoena. It finds this arrangement appropriate as to Hormel because its BYOD policy not only allowed but to some extent financially supported the use of personal cell phones for work purposes, and so it is appropriate that it share in the cost of harvesting and storing the data so that it can be ascertained whether there are relevant and responsive work-related texts.

The Court also recognizes that being deprived of a phone for more than a day either to mail it in and image it, or simply

image it, may be inconvenient, and perhaps burdensome. But no evidence suggests which custodians will have to mail their phones rather than drop them off in person, or that it will take more than a day rather than three hours to image any custodian's phone. Nor is it clear that the custodians have explored alternatives to "mailing in" their phones. [6] . In short, the Court cannot sustain these aspects of each custodian's burden in the absence of evidence showing how the burden actually, rather than theoretically, would fall on the custodians and that the custodians have diligently explored alternatives that would reduce that burden.

As for the privacy concerns, the Court accepts as a matter of common knowledge that modern smart phones store a tremendous amount of their owner's personal, private, or confidential information. But the custodians have not persuaded the Court that that concern cannot be managed through targeted searches. Plaintiffs allege that forensic imaging vendors can target specific phone applications or types of data, in which case a vendor could image only the messages saved in communication apps on the phone. (Tr. at 52.) The custodians have done nothing to persuade the Court that they have explored the options for more targeted data extraction and come up empty-handed. Furthermore, the Court is aware that reputable forensic imaging vendors employ strict protocols to protect data within their control, and in any event, as will be discussed below, the Court's order will provide that only relevant and responsive information will be delivered to Plaintiffs, reducing the risk that a custodian's personal confidential information will be transmitted. Finally, the information may be produced subject to the protective order in this case, further minimizing any risk of public disclosure of private information. Thus, the Court finds the custodians' privacy concerns, while understandable, are manageable and not a basis for declining to enforce Requests Nos. 1 and 5 of the subpoenas.

**D. Whether the Court Should Decline to Enforce Requests Nos. 1 and 5 on the Grounds That They Are Overly Broad and Seek Irrelevant Information**

The Court concludes that while Requests Nos. 1 and 5 seek some relevant information, they extend beyond the bounds of relevance and must therefore be narrowed to target relevant and proportional information.

The Court observes at the outset that it is unclear on the face of Request No. 1 whether it seeks the production of all texts on the custodians' phones exchanged with other Hormel employees, Defendants' employees, and employees of other pork integrators (defined as any of the Defendants and any of over sixty other named companies), regardless of content, or whether the phrase "about supply and demand conditions in the Pork industry" at the end of the request qualifies and limits not only the second clause of the request but the first as well. (Bourne Decl. Ex. 17 Definitions ¶ 14, Request 1.) Request No. 5 does not, on its face, actually seek texts, but seeks information from which a "forensic vendor" could gain access to all archived copies of the custodians' cell phone data, including relevant text messages, in locations like cloud backups, older cell phones, or non-internet archives, without regard to subject matter. (Bourne Decl. Ex. 17 Request 1.)

***14** Plaintiffs proposed a search method that sheds some light on their intended scope. Plaintiffs propose that *all* texts exchanged with any number on a list of 781 phone numbers associated with individuals affiliated with Hormel or any other Defendant or any of the other identified pork integrators, be produced without regard to content. As to all other texts, they propose a key term search, the results of which would be reviewed for relevance by the custodians' counsel. (Bourne Decl. ¶ 12 [ECF No. 887], Ex. 16 [ECF No. 888-2].) This same protocol would, presumably, be applied to both data residing on the cell phones and data gathered from other locations pursuant to Request No. 5. Plaintiffs argue that all texts exchanged with any of the 781 numbers are presumptively relevant as "work-related texts," so they do not need relevance review before production, while any other texts are less likely to be relevant, so a keyword search to narrow the universe, followed by a relevance review of all "hits" is appropriate. (Pls.' Mem. at 15.)

Unquestionably some of the information encompassed by each request is relevant. Request No. 1 seeks text messages between Defendants' employees about pork supply, demand, and pricing (the subject matter of the conspiracy) during the relevant time-period, and between Defendants and other pork integrators. Plaintiffs argue these messages are relevant to help Plaintiffs understand the tone, language, and content of Defendants' communications about that subject matter, and potentially to reveal substance of the alleged conspiracy, and neither Hormel nor the custodians argue persuasively to the contrary. Request No. 5 similarly includes within its scope some relevant information, insofar as the custodians have changed phones and prior relevant messages may be saved in the custodians' archives, cloud backups, or older phones. While Hormel and the custodians dispute whether it is likely that any relevant texts will be found on the cell phones, they

do not seriously disagree that *if* there are texts pertaining to pork supply, demand, and pricing, that were sent during the relevant time period among Hormel employees, or between Hormel employees and other pork integrators, those texts would likely be relevant and responsive to discovery in this case.

But not all texts to all individuals on the 781 phone numbers connected to Defendants and pork integrators will involve this subject matter, and Plaintiffs do not satisfactorily explain why the Court should presume otherwise. The evidence does not show that the custodians texted those numbers only (if at all) about the relevant subject matter, as opposed to other work-related topics or even non-work topics like social plans. Just because there may be some relevant texts within a data set does not make all texts within that set presumptively relevant.

For the same reasons, Request No. 5 also sweeps too broadly in effectively demanding access to all archived text messaging data from all of the custodians' phones.

Furthermore, the time-period of the requested production, January 1, 2008 – August 17, 2018, was not tailored to the job responsibilities of the individual custodians, and therefore also is overly broad. The custodians held different job duties at different times throughout this period, and some of them retired during that period. (*See, e.g.*, Hormel Ex. 10 at 5, Ex. 11 [ECF Nos. 929-9, -10].) The parties designated each custodian based on relevant job duties held during specific subsets of the period of the alleged conspiracy. (*See, e.g.*, Hormel Ex. 8 at 2, Ex. 10 at 5, Ex. 11 [ECF Nos. 929-7, - 9, -10].) Their text data within those time periods are potentially a source of relevant communications, but those distinctions were ignored by Plaintiffs' subpoena requests, which were "one-size-fits-all." While that uniform time frame makes good sense for efficient conduct of party discovery, it is not as appropriate for individual custodians whose confidential personal information is at stake, nor is it proportional in view of the narrower time periods within which these individuals were in relevant roles and therefore may have had relevant communications (if at all).

***15** Accordingly, the Court will enforce the subpoenas as to Requests Nos. 1 and 5 (for all custodians except Chenowith) and orders the custodians (other than Chenowith) to search for and produce relevant text messages within a modified scope and subject to a modified search protocol, as follows: Each subpoena will be limited to the time period or periods within which that custodian held the position that resulted in his or her being identified as a custodian. Plaintiffs' counsel, Hormel's counsel, and the custodian's counsel shall meet and confer to confirm they have a common understanding on that subject. The text messaging data, including data extracted from the custodians' current phones, older phones, or archive or backup data from those phones, must be searched first to identify all texts that were sent to or received from any number on the list of 781 phone numbers identified by Plaintiffs within the time period or periods pertaining to that custodian. The number of resulting texts for each custodian must be reported to Plaintiffs' counsel. The custodian's counsel may then choose to manually review all of the resulting texts for that custodian for relevance; however, the custodian's counsel may meet and confer with Plaintiffs' counsel about a threshold volume of messages for a custodian that would trigger the application of search terms (to be negotiated between counsel), the results of which further filtering would then be reviewed for relevance by the custodian's counsel.

The Court does not rule out the possibility that review by Plaintiffs of the resulting text message production, or other discovery in this case, may provide a more concrete basis upon which to justify an expanded search for relevant messages beyond what the Court has permitted here. Accordingly, the custodians are further ordered to preserve all text messaging data and all archived and cloud-stored text messaging data for the period January 1, 2008 – August 17, 2018, until December 31, 2022, or until such other date as may be agreed upon by the parties or ordered by the Court. Relatedly, Chenowith is also ordered to preserve all text messages, including all archived and cloud-stored messages, from the period January 1, 2008 – August 17, 2018 (or, in the alternative, to arrange at Hormel's and Plaintiffs' shared expense to have such text messages imaged and preserved).

## IV. Hormel's Preservation Duty Did Not Extend to Imaging Personally-Owned Cell Phones and Archiving Cloud Backups

Plaintiffs assert that Hormel knew or should have known that its custodians were conducting substantive work-related business over text message so that it was under an obligation to image those phones and preserve cloud backups at the start of the litigation; they request a declaration that Hormel had an obligation at the start of litigation to preserve its custodians' text message content by imaging their phones and preserving their cloud backup data, and an order compelling Hormel to do so now. (Pls.' Mem. at 11–14.) The duty to preserve evidence arises when a party knows or should have

known that the evidence in its control is relevant to current or reasonably foreseeable litigation, at which point the party must take reasonable steps to preserve it. *Paisley Park*, 330 F.R.D. at 232; Fed. R. Civ. P. 37(e). "The duty to preserve relevant evidence must be viewed from the perspective of the party with control of the evidence." *Paisley Park*, 330 F.R.D. at 232. The duty "extends to those persons likely to have relevant information – the key players in the case, and applies to unique, relevant evidence that might be useful to the adversary." *Id.* at 233.

Whether a party has taken reasonable steps to preserve information is a factual inquiry considering the context of the case, the information sought, and the steps taken. *See id.* at 233–35 (holding that the defendants unreasonably failed to preserve their personal text messages by purging their phone data even though they texted for work purposes and knew of pending litigation involving their business); *In re Petters Co., Inc.*, 606 B.R. 803, 822 (Bankr. D. Minn. 2019).

Here, however, the Court has found Hormel did not control the text messages on the personally-owned cell phones of its custodians. It did communicate litigation holds to reasonably anticipated custodians and Plaintiffs have not shown that those holds were inadequate to communicate to those custodians that they should preserve relevant information under their own control, including text messaging data. (Hormel Mem. at 21–22.) The Court therefore denies Plaintiffs' motion for a "declaration" that Hormel had a duty to do more than it did. [7] Plaintiffs' concerns for preservation going forward are addressed by the Court's order described above in Section III.D.

***16** Accordingly, based on all the files, records, and proceedings, **IT IS HEREBY ORDERED** that Class Plaintiffs' Motion to Compel Hormel To Produce Responsive Text Message Content and to Enforce Subpoenas to Hormel Custodians [ECF No. 883] is **GRANTED IN PART** and **DENIED IN PART** as described fully herein.

**All Citations**

Slip Copy, 2022 WL 972401

## Footnotes

1 Exhibit 2 to the Bourne Declaration [ECF No. 888-2 at 12–162] are the full letters and objections transmitted to Plaintiffs' counsel by the custodians through their counsel. Exhibit 1 to that declaration [ECF No. 888-2 at 1–11] is a chart created by Plaintiffs' counsel summarizing the responses. The Court notes that none of the subpoena responses included (or were required to include) sworn declarations by the custodians.

2 The conspiracy allegedly began in 2009 and none of the parties address pre-BYOD policy communications.

3 Hormel and the custodians object at the outset that Plaintiffs did not engage in good faith meet-and-confer efforts prior to filing this motion. (Hormel Mem. at 27; Custodians' Mem. at 10–11 [ECF No. 925].) "Before filing a motion ... the moving party must, if possible, meet and confer with the opposing party in a good-faith effort to resolve the issues raised by the motion," and certify the same to the Court alongside its motion. D. Minn. L.R. 7.1, 37.1; *see also* Fed. R. Civ. P. 37(a)(1). This obligation is only fulfilled when parties have engaged in a genuine and good-faith discussion about each discovery request that is in dispute. *Mgmt. Registry, Inc. v. A.W. Companies, Inc.*, Case No. 17-cv-05009 (JRT/KMM), 2019 WL 2024538, at *1 (D. Minn. May 8, 2019).

Based on the record of the parties' communications, the Court overrules this objection. Before this motion was filed, Plaintiffs and Hormel exchanged numerous emails and letters arguing their opposing positions regarding whether Hormel had control over its custodians' personal cell phones, whether it met its obligations to preserve text message data, and whether it had to produce that data. (*See* Bourne Decl. Exs. 6–10 [ECF No. 888-2].) In addition, the record reflects that after the custodians received the subpoenas, their counsel "participated in meet and confer communications with opposing counsel including four letters, several e-mails, and two telephone conferences" on June 1 and August 2. (Stephens Decl. ¶¶ 9–18.) The parties'

descriptions of their telephone meetings, and the letters and emails in the record, show an effort by both to explain their positions and concerns, and explore possible compromises, but finally conclude that they were too far apart. (*Id.*; Exs. A–G.) The exchanges show both sides engaged in a genuine discussion over these issues but refused to concede their positions after bringing factual and legal arguments to bear. This satisfies the meet-and-confer requirement.

4 Hormel raises objections to the subpoenas in its memorandum. (Hormel Mem. at 28–29.) Hormel is not subject to the subpoenas nor moving for a protective order, so it lacks standing to quash or modify the subpoenas. *Shukh v. Seagate Tech., LLC*, 295 F.R.D. 228, 236 (D. Minn. 2013). The Court will consider its arguments only to the extent they shed additional light or support for or against the custodians' objections.

5 The Court assumes that this estimate does not include the cost for imaging the five phones that were already imaged by Hormel. Obviously, if it does, this total cost estimate overstates that aspect of the burden.

6 Plaintiffs suggest, for example, that it is possible to mail imaging kits to custodians for whom mailing their phone or travelling to Hormel would be burdensome. (Tr. at 50.) To the extent the custodians are arguing that having to mail in their phones is the necessary result of working with Hormel's vendor, it undercuts their complaint regarding monetary burden, as it suggests strongly that Hormel and not the individual custodians will be paying for the imaging in any event.

7 The Court does not address Hormel's argument that Plaintiffs did not follow proper procedure to request a declaratory judgment. (Hormel Mem. at 18.)

End of Document

340 F.R.D. 74
United States District Court, S.D. New York.

Brian LA BELLE, Plaintiff,

v.

BARCLAYS CAPITAL INC., Defendant.

19 Civ. 3800 (JPO) (GWG)
|
Signed 01/13/2022

**Synopsis**

**Background:** Employee brought action against employer for unlawful retaliation under the Sarbanes-Oxley Act. Employee moved for discovery sanctions under rules of civil procedure and court's inherent authority, alleging that employer misled court in relation to existence of recordings of phone calls and violated court order relating to those recordings and that employer engaged in spoliation of evidence.

**Holdings:** The District Court, Gabriel W. Gorenstein, United States Magistrate Judge, held that:

employee was not entitled to discovery sanctions under rules of civil procedure, statute governing counsel's liability for excessive costs, or court's inherent powers for failure to produce recordings of phone calls;

employer had no duty to preserve notebooks allegedly used by employee during his employment;

employee did not show that text messages sent by his supervisors on employer-issued devices were not produced because they had been destroyed;

employer's duty to search supervisors' personal devices for text messages that were responsive to employee's requests for production of text messages regarding his retaliation claim did not arise until there was some indication that evidence relevant to claims was contained on personal devices; and

employee offered no evidence that any destruction of text messages from supervisors' personal devices took place after employer's duty to preserve text messages arose.

Motion denied.

**Attorneys and Law Firms**

***77** Steven Karl Barentzen, The Law Office of Steven Barentzen, Washington, DC, for Plaintiff.

Allen Baron Roberts, Ronald M. Green, James David MacKinson, John Francis Fullerton, III, Elizabeth Kiernan McManus, Epstein Becker & Green, P.C., New York, NY, for Defendant.

OPINION AND ORDER

GABRIEL W. GORENSTEIN, United States Magistrate Judge

Plaintiff Brian La Belle has sued defendant Barclays Capital Inc. ("Barclays") for unlawful retaliation under the Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745. See generally Amended Complaint, filed July 21, 2021 (Docket # 147) ("Comp.").[1] La Belle has moved for discovery sanctions against Barclays pursuant to Fed. R. Civ. P. 37, 28 U.S.C. § 1927, and the Court's inherent authority.[2] For the reasons explained below, La Belle's motion is denied.

I. BACKGROUND

La Belle was employed by Barclays from July 2015 until his termination in August 2018. See Comp. ¶¶ 8, 59. La Belle alleges that while at Barclays he reported violations of law and other misconduct. See Comp. ¶¶ 11-59. La Belle alleges that thereafter, he faced retaliation from his supervisors — principally, Larry Kravetz, Brian Wiele, and Eric Wu — that included his termination. See id. Barclays denies these allegations and asserts it properly terminated La Belle. See Answer, filed Aug. 4, 2021 (Docket # 153).

II. DISCUSSION

La Belle seeks sanctions against Barclays on three grounds: (1) that Barclays misled the Court and wasted plaintiff's time in relation to the existence of recordings of Wiele's phone calls and violated a Court order relating to those recordings, see Pl. Mem. at 1-8, 13-17; Pl. Reply at 3-5; (2) that Barclays engaged in spoliation by failing to preserve notebooks used by La Belle during his employment; see Pl. Mem. at 11-13,

17-19; Pl. Reply at 9-10; and (3) that Barclays engaged in spoliation by failing to preserve text messages to or from Kravetz and Wiele, see Pl. ***78** Mem. at 8-11, 17-19; Pl. Reply at 5-8. We address each ground next.

A. Recording of Wiele's Phone Calls

1. Facts

Barclays recorded the phone lines of certain employees, including Wiele. See Letter from Steven Barentzen, filed Apr. 22, 2021 (Docket # 120), at 5. On April 22, 2021, La Belle requested that this Court direct Barclays to produce or provide a log of recordings from Wiele's phone line from January 1, 2018 to August 15, 2018. See id. at 5-6. Barclays opposed the request on the ground that such an undertaking would be unduly burdensome under Fed. R. Civ. P. 26(b)(2). See Letter from Allen B. Roberts, filed Apr. 29, 2021 (Docket # 121) ("Apr. 29 Letter"), at 12-14. Barclays noted that creating a log of recordings would require "a search of devices assigned to Mr. Wiele, then a search of servers where his devices were recorded," information which would then need to be collated to create the log. Id. at 14. In other words, creating a log of recordings required Barclays to undergo a "full collection of the [recording] data." Transcript from May 7, 2021 Discovery Conference, filed May 10, 2021 (Docket # 124), at 28:21-23. La Belle then asked for, and Barclays agreed to produce, a "phone bill" or "record of[ ] every single phone call," so La Belle could identify calls he wanted produced, and Barclays would thereafter determine whether those calls were recorded and, if so, produce them to La Belle. Id. at 30:10-32:13. The Court ordered production of this "log" noting that it was not yet ruling "that anyone is ever going to have to listen to any phone call." Id. at 34:6-14.

On May 28, 2021, Barclays provided La Belle with Wiele's phone billing records from January 2018. At the time, Barclays told La Belle:

> As previously stated, the billing system is not aligned to the audio recording systems and is not Barclays' official record of audio call recordings (as explained in our briefing and during the conference with the Court).

Email from James Mackinson to Steven Barentzen, dated May 28, 2021, Exhibit B to Green Decl. (Docket # 188-2). Barclays provided La Belle with the remainder of the billing records on June 4, 2021. Email from Elizabeth McManus to Steven Barentzen, dated June 4, 2021, Exhibit C to Green Decl. (Docket # 188-3). Again, Barclays noted that "the billing system is not aligned to the audio recording systems and is not Barclays' official record of audio call recordings." Id. That same day, Barclays made an identical representation to the Court when informing the Court that the billing records had been fully produced. See Letter from Allen B. Roberts, filed June 4, 2021 (Docket # 130), at 2, 2 n.1.

On July 21, 2021, La Belle sought an order directing Barclays to produce recordings of 48 calls to or from Wiele. See Letter from Steven Barentzen, filed July 21, 2021 (Docket # 148), at 1-2. La Belle identified these calls by reviewing the billing records and comparing calls on the records against documents produced by Barclays. See id.; see also Pl. Mem. at 5; Def. Mem. at 5. Barclays opposed the request on burdensomeness grounds, stating: "Retrieving any additional available audio for the January 5, 2018 to April 30, 2018 time period would require searching numerous databases and then exporting any located files through a time-consuming and sometimes manual process." Letter from Allen Roberts, filed July 23, 2021 (Docket # 149) ("July 23 Letter"), at 1-2. Barclays noted that it had previously collected recordings of Wiele's calls from May 1, 2018 forward in connection with an SEC request, and Barclays agreed to produce 22 such calls to La Belle. See id. at 2. On August 3, 2021, the Court rejected Barclays' burdensomeness objection and ordered Barclays to "search for and produce the remaining 26 phone calls identified by" La Belle. Order of August 3, 2021 (Docket # 152) ("Aug. 3 Order"), at 1-2. On September 15, 2021, La Belle moved to compel the production of the 26 calls within two weeks. See Letter from Steven Barentzen, filed Sept. 15, 2021 (Docket # 161), at 3. Barclays opposed the motion, arguing that the two week timeframe would place an undue burden on Barclays because while Barclays was "working to identify and produce any relevant recordings that may exist of the ***79** 26 calls," "retrieving and searching for audio recording data is a time-consuming process." Letter from Ronald Green, filed Sept. 17, 2021 (Docket # 162), at 3. On September 20, 2021, the Court ordered that the 26 calls be produced by October 15, 2021. Order of September 20, 2021 (Docket # 163) ("Sept. 20 Order").

On October 8, 2021, Barclays informed La Belle that it had "completed multiple searches in an effort to retrieve any

available audio recordings of the 26 calls to/from custodian Brian Wiele ... within the period from January 5, 2018 to March 16, 2018 and confirmed that Mr. Wiele's phone was not recorded during that time." Email from Elizabeth McManus to Steven Barentzen, dated October 8, 2021, Exhibit D to Green Decl. (Docket # 188-4). Barclays additionally noted "that Mr. Wiele's phone was not subject to recording requirements at any point in 2018. Rather, his phone was only temporarily recorded between late April and August of 2018 due to an error that occurred when the Syndicate Securitization team was migrated from Cisco phone systems hardware to IPC Turret hardware." Id.

La Belle maintains that the information provided to him on October 8, 2021 "not only contradicts what Barclays previously told Plaintiff and the Court" but "is completely inconsistent with Barclay's [sic] relentless arguments over the previous two years that it should not have to produce the calls, or even information concerning the calls, because it would be too burdensome to do so." Pl. Mem. at 7. La Belle emphasizes that "Barclays at no point during the process stated that recordings of these calls don't exist or that Mr. Wiele's phone line did not need to be recorded." Id. Barclays responds that it did not know whether the recordings in fact existed until it went through the "collection and review process that Barclays repeatedly explained would be necessary ... to determine whether [the] recordings existed." Def. Mem. at 8.

Although La Belle seeks a variety of sanctions in connection with Barclays' failure to produce the 26 calls, see Pl. Mem. at 15-17, we decline to impose any sanction against Barclays or its attorneys because La Belle has not established that Barclays violated its discovery obligations or an order of this Court.

2. Governing Law

La Belle seeks sanctions under Fed. R. Civ. P. 37(a)(5), the Court's "inherent power," and 28 U.S.C. § 1927. See Pl. Mem. at 13-14.

Federal Rule of Civil Procedure 37(a)(5)(A) provides that if a motion for an order compelling disclosure or discovery is granted,

> the court must, after giving an opportunity to be heard, require the party or deponent whose conduct necessitated the motion, the party or attorney advising that conduct, or both to pay the movant's reasonable expenses incurred in making the motion, including attorney's fees. But the court must not order this payment if:
>
> (i) the movant filed the motion before attempting in good faith to obtain the disclosure or discovery without court action;
>
> (ii) the opposing party's nondisclosure, response, or objection was substantially justified; or
>
> (iii) other circumstances make an award of expenses unjust.

Notwithstanding Rule 37(a)(5)(A)'s limitation to an award of expenses, plaintiff asks for other sanctions. See Pl. Mem. at 15-17. In support, La Belle appears to rely on Rule 37(b)(2), see id. at 13, 15-17, which provides that a party who "fails to obey an order to provide or permit discovery" may be subject to sanctions including but not limited to "directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;" and "prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence." Fed. R. Civ. P. 37(b)(2)(A). In all such cases, "the court must order the disobedient 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 ***80** circumstances make an award of expenses unjust." Fed. R. Civ. P. 37(b)(2)(C).

28 U.S.C. § 1927 states:

> Any attorney or other person admitted to conduct cases in any court of the United States or any Territory thereof who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct.

Id. Finally, a court retains inherent authority to impose sanctions as necessary "to manage its own affairs." Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d

99, 107 (2d Cir. 2002); accord Chambers v. NASCO, Inc., 501 U.S. 32, 43-46, 111 S.Ct. 2123, 115 L.Ed.2d 27 (1991).

The Second Circuit has held that "the only meaningful difference between an award made under § 1927 and one made pursuant to the court's inherent power is that awards under § 1927 are made only against attorneys or other persons authorized to practice before the courts while an award made under the court's inherent power may be made against an attorney, a party, or both." Enmon v. Prospect Cap. Corp., 675 F.3d 138, 144 (2d Cir. 2012) (citation and punctuation omitted). Courts therefore commonly consider sanctions under the court's inherent powers and § 1927 as part of the same inquiry. See id. at 144-49; Schlaifer Nance & Co., Inc. v. Est. of Warhol, 194 F.3d 323, 336 (2d Cir. 1999); United States v. Prevezon Holdings, Ltd., 305 F. Supp. 3d 468, 478 (S.D.N.Y. 2018).

To impose sanctions under either § 1927 or the Court's inherent powers, there must be clear evidence that "(1) the offending party's claims were entirely without color, and (2) the claims were brought in bad faith — that is, motivated by improper purposes such as harassment or delay." Eisemann v. Greene, 204 F.3d 393, 396 (2d Cir. 2000) (per curiam) (quotation omitted); accord Prevezon Holdings, 305 F. Supp. 3d at 478-79. The Second Circuit has explained that

> [c]onduct is entirely without color when it lacks any legal or factual basis; it is colorable when it has some legal and factual support, considered in light of the reasonable beliefs of the attorney whose conduct is at issue. [Schlaifer, 194 F.3d] at 337. A finding of bad faith, and a finding that conduct is without color or for an improper purpose, must be supported by a high degree of specificity in the factual findings. Id.; Eisemann[ ], 204 F.3d [at 396.]

Wolters Kluwer Fin. Servs., Inc. v. Scivantage, 564 F.3d 110, 114 (2d Cir. 2009).

3. Application

La Belle has not shown that Barclays acted improperly with respect to the Wiele recordings. After the Court ordered Barclays to collect and produce the 26 calls, see Aug. 3 Order at 2; Sept. 20 Order, Barclays underwent the investigatory process it had repeatedly described previously and determined that the calls requested by La Belle were not recorded. See Exhibit D to Green Decl. (Docket # 188-4). La Belle believes Barclays acted improperly by not divining that its process would lead to discovering that none of the 26 calls were recorded. But La Belle has not shown that Barclays could have known that the recordings did not exist before it collected and reviewed the recording data. Additionally, Barclays' earlier refusals to examine the recordings were based on burdensomeness objections, see Apr. 29 Letter at 12-14; July 23 Letter at 1-2, which — while ultimately partially unsuccessful, see Aug. 3 Order at 1-2 — were nonetheless substantially justified and not unreasonable in light of the extensive time and effort required to collect and review the recorded calls. See Fed. R. Civ. P. 26(b)(2)(B) (a producing party "need not provide discovery of electronically stored information ["ESI"] from sources that the party identifies as not reasonably accessible because of undue burden or cost"); Klein v. Torrey Point Grp., LLC, 979 F. Supp. 2d 417, 442 (S.D.N.Y. 2013) (refusing to award attorneys' fees under Rule 37(a) when defendant initially withheld records on relevance grounds because although "[d]efendant's relevancy argument ... proved unavailing, it was not without substance"). Upon completing ***81** its review of the phone recording data and notifying La Belle that no additional responsive calls existed, Barclays fulfilled its obligations to La Belle and under the Court's Order. See generally Bank of New York v. Meridien BIAO Bank Tanzania Ltd., 171 F.R.D. 135, 152 (S.D.N.Y. 1997) ("Under ordinary circumstances, a party's good faith averment that the items sought simply do not exist ... should resolve the issue of failure of production." (quotation omitted)).

For the same reasons, La Belle cannot prevail under 28 U.S.C. § 1927 or the Court's inherent powers. Critically, La Belle has offered no clear evidence of bad faith. We also reject La Belle's alternative argument that Barclays violated the "spirit" of the Court's Orders. See Pl. Reply at 4. Thus, La Belle's motion for sanctions as to Barclays' failure to produce the Wiele recordings is denied.

B. Spoliation

La Belle seeks sanctions — specifically, adverse inference instructions — for the alleged spoliation of La Belle's

notebooks and of text messages sent by Barclays' employees. See Pl. Mem. at 8-13, 18-19.

1. Governing Law

"Spoliation is the destruction or significant alteration of evidence, or failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93, 148 (2d Cir. 2008) (internal quotation marks omitted) (quoting Allstate Ins. Co. v. Hamilton Beach/Proctor Silex, Inc., 473 F.3d 450, 457 (2d Cir. 2007)). A party seeking sanctions for spoliation has the burden of establishing the elements of a spoliation claim. See Residential Funding, 306 F.3d at 107 (citation omitted); accord John Wiley & Sons v. Book Dog Books, LLC, 2015 WL 5769943, at *6 (S.D.N.Y. Oct. 2, 2015) (citations omitted). These elements are "(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the [evidence was] destroyed with a culpable state of mind; and (3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense." Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135, 162 (2d Cir. 2012) (internal quotation marks omitted) (quoting Residential Funding, 306 F.3d at 107). With respect to ESI — for example, text messages — Rule 37(e) provides:

> If [ESI] that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Whether evidence is electronically-stored or not, "spoliation sanctions can be imposed only when the party seeking such sanctions demonstrates that relevant evidence has been lost." See Leidig v. Buzzfeed, Inc., 2017 WL 6512353, at *7 (S.D.N.Y. Dec. 19, 2017) (citations and internal quotation marks omitted).

Although Rule 37(e) does not specifically address the first element of spoliation, courts have recognized that the standard for showing that a party had an obligation to preserve evidence is the same for both ESI and non-ESI. See, e.g., Leidig, 2017 WL 6512353, at *8; accord Greene v. Bryan, 2019 WL 181528, at *4 n.5 (E.D.N.Y. Jan. 14, 2019). To meet the first element, La Belle must show that Barclays "had an obligation to preserve [the evidence] at the time it was destroyed." Chin, 685 F.3d at 162 (quotation omitted). "Identifying the boundaries of the duty to preserve [evidence] involves two related inquiries: when does the ***82** duty to preserve attach, and what evidence must be preserved?" Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (emphasis omitted). In the usual situation, "[t]he obligation to preserve evidence arises when [a] party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." Fujitsu Ltd. v. Fed. Exp. Corp., 247 F.3d 423, 436 (2d Cir. 2001) (citation omitted); accord R.F.M.A.S., Inc. v. So, 271 F.R.D. 13, 23 (S.D.N.Y. 2010); Scalera v. Electrograph Sys., Inc., 262 F.R.D. 162, 171 (E.D.N.Y. 2009); Treppel v. Biovail Corp., 249 F.R.D. 111, 118 (S.D.N.Y. 2008). Thus, the duty to preserve evidence arises "most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation." Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998) (citations omitted); accord In re 650 Fifth Ave. & Related Props., 830 F.3d 66, 105 (2d Cir. 2016). A determination of "when the duty to preserve evidence arises may, under certain circumstances, be dependent upon the nature of the evidence." Arista Records LLC v. Usenet.com, Inc., 608 F. Supp. 2d 409, 430 (S.D.N.Y. 2009).

2. Application

a. Notebooks

La Belle seeks to sanction Barclays for destroying notebooks La Belle used during his employment with Barclays.[3] La Belle claims that these notebooks would reveal he took thorough notes while at Barclays, disproving Barclays' contention that La Belle was fired in part for inadequate notetaking. See Pl. Mem. at 11-13, 19; Pl. Reply at 9-10. La Belle contends that he kept the notebooks in his desk. See Pl. Mem. at 12. Barclays disputes that the notebooks ever existed, see Def. Mem. at 31-33, but explains in a footnote that any non-personal items in La Belle's desk would have been destroyed upon La Belle's termination, pursuant to Barclays' policy. See id. at 13 n.3 ("In any event, typically, items in desks that are not personal to an employee are disposed of when an employee is separated from Barclays.").

As a threshold matter, a party seeking spoliation sanctions must necessarily show that the evidence at issue actually existed. See Dilworth v. Goldberg, 3 F. Supp. 3d 198, 202 (S.D.N.Y. 2014) (collecting cases). We accept that La Belle has shown the notebooks existed on the day he was fired considering his detailed testimony describing the notebooks and their location. See Deposition of Brian La Belle, dated May 25, 2021, Exhibit O to Pl. Mem. (Docket # 182-15), at 418-20. However, La Belle has provided no evidence of their existence thereafter.

As just discussed, the duty to preserve evidence may arise before suit is filed "when a party should have known that the evidence may be relevant to future litigation." Kronisch, 150 F.3d at 126. In such an instance, evidence must be preserved when litigation is "reasonably foreseeable." In re Terrorist Bombings, 552 F.3d at 148 (quotation omitted); accord Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 435 (S.D.N.Y. 2010) (quotation and citations omitted). Because La Belle has provided no evidence that the notebooks existed after the day he was fired, La Belle can prevail only by showing that Barclays had a duty to preserve the notebooks as of the date of his firing.

La Belle points to three exhibits in support of his assertion that Barclays should ***83** have viewed litigation as reasonably foreseeable in August 2018, when La Belle was terminated, and thus should have preserved the notebooks on that date. See Pl. Mem. at 11; Pl. Reply at 9. First, La Belle cites a May 10, 2018 email from Amanda Cohen, a Human Resources employee at Barclays. See Pl. Mem. at 11. In that email, Cohen responds to an inquiry from another Human Resources employee who asked whether La Belle's actions constituted whistleblowing. Specifically, Cohen states:

> The approach will be to tag team with Compliance & ER (similar to what we did last time) so that we are covered on all bases if he files suit. I made it clear on the call I do not want this blowing up into a bigger issue and we need to protect Larry and his reputation. He has been doing the best he can with a difficult situation.

Email from Amanda Cohen to Anne Marie Devoti, dated May 10, 2018, Exhibit L to Pl. Mem. (Docket # 182-12) ("Cohen Email"). La Belle also cites handwritten notes from February 2018 indicating that a Barclays HR employee named Elyse Gonzalez spoke to La Belle and La Belle mentioned that he "engaged external counsel." Pl. Reply at 9 (citing Handwritten Notes, dated Feb. 27, 2018, Exhibit G to La Belle Decl. (Docket # 191-7) ("Feb. 2018 Note")); see also Email from Elyse Gonzalez to Brian La Belle, dated May 8, 2018, Exhibit S to Pl. Mem. (Docket # 182-19), at *4 (identifying "Elyse" as "Elyse Gonzalez"). Finally, La Belle cites a transcript of a recorded August 1, 2018, conversation in which La Belle was notified of his termination. See Pl. Reply at 9. In particular, La Belle relies on a portion of the conversation in which he informed an HR representative that La Belle intended to have his lawyer review Barclays' non-solicitation policy. See Transcript of August 1, 2018 Conversation Between Brian La Belle, Brian Wiele, and Traci Lavelle, dated Oct. 30, 2018, Exhibit H to La Belle Decl. (Docket # 191-8), at 7.

Taken together or separately, these three exhibits are insufficient to show that litigation between La Belle and Barclays was reasonably foreseeable on the date of La Belle's termination — a showing necessary to charge Barclays with an obligation to preserve the notebooks.

As an initial matter, La Belle's August 1, 2018 remark regarding consulting his attorney on the non-solicitation policy gives no indication that he planned to file suit regarding his termination. As for the two remarks made by HR employees, Cohen's email — referring to protecting the company "if La Belle files suit" — suggests that the HR representative understood that a lawsuit was possible. Cohen Email (emphasis added). But it does not indicate that a lawsuit was in fact expected, let alone likely. See Fed. R. Civ. P. 37(e),

2015 Advisory Committee Note (in evaluating the first factor, "[c]ourts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant."). The second remark came months before La Belle was fired and merely indicates that a Barclays employee was aware that La Belle had retained an attorney. See Feb. 2018 Note. But the mere claim by an employee that he has hired an attorney does not suggest that a lawsuit is likely or should reasonably be expected, even if that employee is later terminated.

Accordingly, La Belle has not met his burden to establish spoliation as to his notebooks.

i. Text Messages

La Belle seeks sanctions in connection with Barclays' alleged failure to produce certain text messages to and from Kravetz and Wiele. See Pl. Mem. at 8-11, 18-19. Barclays states that it preserved and produced ESI on Barclays-issued devices but did not undertake those efforts as to any personal cellphones until "late 2019" in light of Barclays' policy forbidding its employees from conducting business on their personal cellphones. See Def. Mem. at 9-11. We will assume arguendo that there were some text messages on Kravetz and Wiele's cellphones during La Belle's employment that were relevant to La Belle's claims.

On July 17, 2019, La Belle's counsel requested from Barclays' counsel "All communications and documents to, from, by or between Larry Kravetz, Eric Wu, ... [and] ***84** Brian Wiele ... concerning [La Belle]." Plaintiff's First Set of Document Requests, dated July 17, 2019, Exhibit M to Pl. Mem. (Docket # 182-13), at *5, *8. By September 2019, La Belle specifically informed Barclays by letter that this request included text messages, though La Belle did not mention that he was seeking a search of personal cellphones. See Letter from Steven Barentzen to Allen Roberts, dated Sept. 20, 2019, Exhibit E to La Belle Decl. (Docket # 191-5), at *2. Barclays concedes that by "late 2019" it was aware of La Belle's "interest in Mr. Kravetz's personal cellular device." Def. Mem. at 10, 26.

As to texts on Barclays-issued devices, Barclays asserts that any texts to or from Barclays-issued devices would have been subject to Barclays' 10-year document retention protocol. See id. at 9, 22. Barclays claims that it collected "all text message data preserved from the Barclays-issued devices for Mr. Kravetz and Mr. Wiele" on November 26, 2019. Id. at 9. It points to multiple pages of texts that it did produce, Bates-stamped D015038-D015049. See id. Although La Belle insists there must be additional texts, it is his burden to show that preservation did not occur. The only evidence La Belle has provided on this score is an email from Wiele to Kravetz asserting that a text was sent on a particular date, combined with the fact that this text was not produced. See Email from Brian Wiele to Larry Kravetz, dated May 4, 2018, Exhibit G to Pl. Mem. (Docket # 182-7). However, given that there was no testimony that Kravetz actually received this text, and the fact that Kravetz gave sworn testimony that his Barclays-issued device was unreliable with texting, see Deposition of Larry Kravetz, dated Oct. 27, 2021, Exhibit H to Green Decl. (Docket # 188-8), at 197, LaBelle's evidence is simply insufficient for this Court to find that texts were not produced to plaintiff from the Barclays devices because they had been destroyed.

With respect to the texts from personal devices, our consideration of this issue must be evaluated against the backdrop of the specific Barclays policy that prohibited employees from discussing company business on such devices without company approval. See Barclays' Business Communications Global Standard, Exhibit G to Green Decl. (Docket # 188-7), at 4. While it is a close question, we are not prepared to find that Barclays acted unreasonably in assuming that its employees complied with such a policy — notwithstanding LaBelle's claim that employees frequently violated the policy, see La Belle Decl. ¶¶ 2-9. Certainly, it is a better practice for a company to make a searching inquiry of all relevant employees to determine whether they violated a company policy regarding use of devices. But in light of the enormous demands that discovery places on any party, we do not find that Barclays acted unreasonably in assuming the policy was followed and limiting its document search to company-issued devices until the issue was brought to its attention. La Belle was obviously aware of the company policy and it would have been simple enough for his attorney to have specified in his July document request or his September letter to defense counsel that personal devices should be included in Barclays' search.

Accordingly, we find that the duty to search for messages on Wiele and Kravetz's personal cellphones did not arise until there was some indication that evidence relevant to plaintiff's claims was contained on the personal devices of those employees. The record is unclear as to when this occurred, though Barclays concedes that it was made aware in

"late 2019." Def. Mem. at 10, 26. La Belle offers no evidence showing that any destruction of messages took place between that point and January 2020, when Barclays apparently undertook to search for such messages. See Declaration of Larry Kravetz, dated Oct. 27, 2021, Exhibit K to Green Decl. (Docket # 188-11) ("Kravetz Decl.") ¶¶ 4-5; Declaration of Brian Wiele, dated Oct. 27, 2021, Exhibit L to Green Decl. (Docket # 188-12) ("Wiele Decl.") ¶¶ 4-5. Indeed, Barclays has submitted evidence to the contrary. See Kravetz Decl. ¶¶6; Wiele Decl. ¶ 6. The fact that a former employee, Eric Wu, may have preserved and produced messages from his own cellphone, see Text Messages between Eric Wu and Larry Kravetz, Exhibit I to Pl. Mem. (Docket # 182-9), does not ***85** show that there was any improper destruction by Kravetz or Wiele. It is La Belle's burden to prove all elements of spoliation, including that evidence was destroyed with some degree of culpability. Given the above, we cannot find that La Belle has met his burden as to the text messages.

## III. CONCLUSION

For the foregoing reasons, La Belle's motion for sanctions (Docket # 181) is denied.

SO ORDERED.

**All Citations**

340 F.R.D. 74, 111 Fed.R.Serv.3d 1164

## Footnotes

1 The Amended Complaint renders plaintiff's name both as "La Belle" and "LaBelle." For consistency, we use "La Belle."

2 See Notice of Motion for Discovery Sanctions, filed Oct. 21, 2021 (Docket # 181); Memorandum of Law in Support, filed Oct. 21, 2021 (Docket # 182) ("Pl. Mem."); Declaration of Ronald M. Green in Opposition, filed Oct. 28, 2021 (Docket # 188) ("Green Decl."); Memorandum of Law in Opposition, filed Oct. 28, 2021 (Docket # 189) ("Def. Mem."); Reply Memorandum of Law in Support, filed Nov. 1, 2021 (Docket # 190) ("Pl. Reply"); Declaration of Brian La Belle, filed Nov. 1, 2021 (Docket # 191) ("La Belle Decl.").

3 La Belle occasionally refers to the notebooks of other Barclays employees. See Pl. Mem. at 13, 19. La Belle suggests that Barclays' failure to provide more than "a few pages from Sammy Hamididdin" indicates that these other notebooks were "lost or destroyed." Id. We find La Belle's scattered references to the notebooks of others insufficient to indicate that he is seeking spoliation sanctions as to those notebooks and, in any event, we would deny any such sanctions for the same reasons that apply to La Belle's notebooks and for the additional reason that there has been no showing of anything but the most minimal relevance of any such notebooks. See Khaldei v. Kaspiev, 961 F. Supp. 2d 564, 570 (S.D.N.Y. 2013) ("[B]ecause plaintiff's argument that there has been any actual loss of evidence relevant to the claims or defenses in this case amounts to pure speculation, it is insufficient to sustain a motion for spoliation sanctions.").

End of Document

**U.S. Department of Justice**
**Criminal Division**

# Evaluation of Corporate Compliance Programs

**(Updated March 2023)**

## Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

3. Does the corporation's compliance program work in practice?

*See* JM 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.[1] The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.[2] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

## I. Is the Corporation's Compliance Program Well Designed?

The critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or permitting employees to engage in misconduct. JM 9-28.800.

Accordingly, prosecutors should examine the comprehensiveness of the compliance program, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

### A. Risk Assessment

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

Prosecutors should consider whether the program is appropriately "designed to detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[]." JM 9-28.800.[3] For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) ("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?

- **Risk-Tailored Resource Allocation –** Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

- **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

## B. Policies and Procedures

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all

company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

### C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise.

Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

## D. Confidential Reporting Structure and Investigation Process

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual

misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has established corporate governance mechanisms that can effectively detect and prevent misconduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

## E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9-28.800.

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third-party relationship managers

about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

- **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

## F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

## II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one implemented, resourced, reviewed, and revised, as appropriate, in an effective manner. JM 9-28.800. In this regard, prosecutors should evaluate a corporation's method for assessing and addressing applicable risks and designing appropriate controls to manage these risks. In addition, prosecutors should determine whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it." JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

### A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* … shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

## B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy, as an indicator of whether compliance personnel are in fact empowered and positioned to effectively detect and prevent misconduct. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); *see also* U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive

within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

- **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

## C. Compensation Structures and Consequence Management

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear consequence management procedures (procedures to identify, investigate, discipline and remediate violations of law, regulation, or policy) in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, prosecutors may consider whether a company has publicized disciplinary actions internally, where appropriate and possible, which can have valuable deterrent effects. Prosecutors may also consider whether a company is tracking data relating to disciplinary actions to measure effectiveness of the investigation and consequence management functions. This can include monitoring the number of compliance-related allegations that are substantiated, the average (and outlier) times to complete a compliance investigation, and the effectiveness and consistency of disciplinary measures across the levels, geographies, units or departments of an organization.

The design and implementation of compensation schemes play an important role in fostering a compliance culture. Prosecutors may consider whether a company has incentivized compliance by designing compensation systems that defer or escrow certain compensation tied to conduct consistent with company values and policies. Some companies have also enforced contract provisions that permit the company to recoup previously awarded compensation if the recipient of such compensation is found to have engaged in or to be otherwise responsible for corporate wrongdoing. Finally, prosecutors may consider whether provisions for recoupment or reduction of compensation due to compliance violations or misconduct are maintained and enforced in accordance with company policy and applicable laws.

Compensation structures that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance. At the same time,

providing positive incentives, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership, can drive compliance. Prosecutors should examine whether a company has made working on compliance a means of career advancement, offered opportunities for managers and employees to serve as a compliance "champion", or made compliance a significant metric for management bonuses. In evaluating whether the compensation and consequence management schemes are indicative of a positive compliance culture, prosecutors should consider the following factors:

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? How transparent has the company been with the design and implementation of its disciplinary process? In circumstances where an executive has been exited from the company on account of a compliance violation, how transparent has the company been with employees about the terms of the separation? Are the actual reasons for discipline communicated to employees in all cases? If not, why not? Is the same process followed for each instance of misconduct, and if not, why? Has the company taken steps to restrict disclosure or access to information about the disciplinary process? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Disciplinary Measures** – What types of disciplinary actions are available to management when it seeks to enforce compliance policies? Does the company have policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee? What policies and practices does the company have in place to put employees on notice that they will not benefit from any potential fruits of misconduct? With respect to the particular misconduct at issue, has the company made good faith efforts to follow its policies and practices in this respect?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why? What metrics does the company apply to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the organization?

- **Financial Incentive System** – Has the company considered the impact of its financial rewards and other incentives on compliance? Has the company evaluated whether commercial targets are achievable if the business operates within a compliant and ethical manner? What role does the compliance function have in designing and awarding financial incentives at senior levels of the organization? How does the company incentivize compliance and ethical behavior? What percentage of executive

compensation is structured to encourage enduring ethical business objectives? Are the terms of bonus and deferred compensation subject to cancellation or recoupment, to the extent available under applicable law, in the event that non-compliant or unethical behavior is exposed before or after the award was issued? Does the company have a policy for recouping compensation that has been paid, where there has been misconduct? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied, compensation recouped or deferred compensation cancelled) as a result of compliance and ethics considerations?

- **Effectiveness** – How has the company ensured effective consequence management of compliance violations in practice? What insights can be taken from the management of a company's hotline that provide indicia of its compliance culture or its management of hotline reports? How do the substantiation rates compare for similar types of reported wrongdoing across the company (*i.e.* between two or more different states, countries, or departments) or compared to similarly situated companies, if known? Has the company undertaken a root cause analysis into areas where certain conduct is comparatively over or under reported? What is the average time for completion of investigations into hotline reports and how are investigations that are addressed inconsistently managed by the responsible department? What percentage of the compensation awarded to executives who have been found to have engaged in wrongdoing has been subject to cancellation or recoupment for ethical violations? Taking into account the relevant laws and local circumstances governing the relevant parts of a compensation scheme, how has the organization sought to enforce breaches of compliance or penalize ethical lapses? How much compensation has in fact been impacted (either positively or negatively) on account of compliance-related activities?

## III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor

should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

### A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management

and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?

- **Culture of Compliance** – How often and how does the company measure its culture of compliance? How does the company's hiring and incentive structure reinforce its commitment to ethical culture? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

## B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

- **Independence and Empowerment** – Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the company? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?

Messaging applications have become ubiquitous in many markets and offer important platforms for companies to achieve growth and facilitate communication. In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications. Policies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company. Prosecutors should consider how the policies and procedures have been communicated to employees, and whether the corporation has enforced the policies and procedures on a regular and consistent basis in practice. In conducting this evaluation, prosecutors should consider the following factors:

- **Communication Channels** – What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does that practice vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each? What is the rationale for the company's approach to determining which communication channels and settings are permitted?

- **Policy Environment** – What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced? What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the organization's ability to ensure security or monitor/access business-related communications? If the company has a "bring your own device" (BYOD) program, what are its policies governing preservation of and access to corporate data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies? How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications? Do the organization's policies permit the company to review business communications on BYOD and/or messaging applications? What exceptions or limitations to these policies have been permitted by

the organization? If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

- **Risk Management** – What are the consequences for employees who refuse the company access to company communications? Has the company ever exercised these rights? Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and exercise control over the communication channels used to conduct the organization's affairs? Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company's business needs and risk profile?

### C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue? Did the company take any actions to recoup or reduce compensation for responsible employees to the extent practicable and available under applicable law?

[1] Many of the topics also appear in the following resources:

- Justice Manual ("JM")
    - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
    - JM 9-47.120 and the Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, *available at* https://www.justice.gov/criminal-fraud/file/1562831/download.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/CHAPTER_8.pdf.
- Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download; updated Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Kenneth A. Polite, Jr., on March 1, 2023, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.
- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (the Department of Justice's ("DOJ") Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).
- A Resource Guide to the U.S. Foreign Corrupt Practices Act (2d ed.) ("FCPA Guide"), published in July 2020 by the DOJ and the Securities and Exchange Commission ("SEC"), *available at* https://www.justice.gov/criminal-fraud/file/1292051/download.
- Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions, amended by the Organization for Economic Co-operation and Development ("OECD") Council on November 25, 2021, *available at* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378.
- Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook"), published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank, *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.
- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ's Antitrust Division, *available at* https://www.justice.gov/atr/page/file/1182001/download.

- A Framework for OFAC Compliance Commitments, published in May 2019 by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), *available at https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.*

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

[3] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations, require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars. Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).

**U.S. Department of Justice**

Office of the Deputy Attorney General

The Deputy Attorney General

*Washington, D.C. 20530*

September 15, 2022

MEMORANDUM FOR ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION
ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION
ASSISTANT ATTORNEY GENERAL, ENVIRONMENT AND NATURAL RESOURCES DIVISION
DEPUTY ASSISTANT ATTORNEY GENERAL, TAX DIVISION
ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
DIRECTOR, EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS
ALL UNITED STATES ATTORNEYS

FROM: THE DEPUTY ATTORNEY GENERAL Lisa Monaco

SUBJECT: Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group

By combating corporate crime, the Department of Justice protects the public, strengthens our markets, discourages unlawful business practices, and upholds the rule of law. Strong corporate criminal enforcement also assures the public that there are not two sets of rules in this country—one for corporations and executives, and another for the rest of America. Corporate criminal enforcement will therefore always be a core priority for the Department.

In October 2021, the Department announced three steps to strengthen our corporate criminal enforcement policies and practices with respect to individual accountability, the treatment of a corporation's prior misconduct, and the use of corporate monitors. *See* Memorandum from Deputy Attorney General Lisa O. Monaco, "Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies," Oct. 28, 2021 ("October 2021 Memorandum"). Simultaneously, we established the Corporate Crime Advisory Group ("CCAG")[1] within the Department to evaluate and recommend further guidance and consider

[1] CCAG members included leaders and experienced prosecutors from all components of the Department that handle corporate criminal matters: the Criminal Division; the Antitrust Division; the Executive Office of United States

revisions and reforms to enhance our approach to corporate crime, provide additional clarity on what constitutes cooperation by a corporation, and strengthen the tools our attorneys have to prosecute responsible individuals and companies.[2] This review considered and incorporated helpful input from a broad cross-section of individuals and entities with relevant expertise and representing diverse perspectives, including public interest groups, consumer advocacy organizations, experts in corporate ethics and compliance, representatives from the academic community, audit committee members, in-house attorneys, and individuals who previously served as corporate monitors, as well as members of the business community and defense bar.

With the benefit of this input, this memorandum announces additional revisions to the Department's existing corporate criminal enforcement policies and practices. This memorandum provides guidance on how prosecutors should ensure individual and corporate accountability, including through evaluation of: a corporation's history of misconduct; self-disclosure and cooperation provided by a corporation; the strength of a corporation's existing compliance program; and the use of monitors, including their selection and the appropriate scope of a monitor's work. Finally, this memorandum emphasizes the importance of transparency in corporate criminal enforcement.

In order to promote consistency across the Department, these policy revisions apply Department-wide. Some announcements herein establish the first-ever Department-wide policies on certain areas of corporate crime, such as guidance on evaluating a corporation's compensation plans; others supplement and clarify existing guidance. The policies set forth in this Memorandum, as well as additional guidance on subjects like cooperation, will be incorporated into the Justice Manual through forthcoming revisions, including new sections on independent corporate monitors.[3]

## I. Guidance on Individual Accountability

The Department's first priority in corporate criminal matters is to hold accountable the individuals who commit and profit from corporate crime. Such accountability deters future illegal activity, incentivizes changes in individual and corporate behavior, ensures that the proper parties are held responsible for their actions, and promotes the public's confidence in our justice system. *See* Memorandum from Deputy Attorney General Sally Quillian Yates, "Individual Accountability for Corporate Wrongdoing," Sept. 9, 2015. Many existing Department policies promote the identification and investigation of the individuals responsible for corporate crimes. The following policies reinforce this priority.

---

Attorneys; multiple United States Attorneys' Offices; the Civil Division; the National Security Division; the Environment and Natural Resources Division; the Tax Division; and the Federal Bureau of Investigation.

[2] While this Memorandum refers to corporations and companies, the terms apply to all types of business organizations, including partnerships, sole proprietorships, government entities, and unincorporated associations. *See* Justice Manual ("JM") § 9-28.200.

[3] Department prosecutors will continue to employ the Principles of Federal Prosecution of Business Organizations—as amended by the October 2021 Memorandum and this memorandum—to guide investigations and prosecutions of corporate crime, including with respect to prosecutors' assessment and evaluation of just and efficient resolutions in corporate criminal cases. *See* JM §§ 9-28.000 *et seq.* ("Principles of Federal Prosecution of Business Organizations").

A. Timely Disclosures and Prioritization of Individual Investigations

To be eligible for any cooperation credit, corporations must disclose to the Department all relevant, non-privileged facts about individual misconduct. *See* October 2021 Memorandum, at 3. The mere disclosure of records, however, is not enough. If disclosures come too long after the misconduct in question, they reduce the likelihood that the government may be able to adequately investigate the matter in time to seek appropriate criminal charges against individuals. The expiration of statutes of limitations, the dissipation of corroborating evidence, and other factors can inhibit individual accountability when the disclosure of facts about individual misconduct is delayed.

In particular, it is imperative that Department prosecutors gain access to all relevant, non-privileged facts about individual misconduct swiftly and without delay. Therefore, to receive full cooperation credit, corporations must produce on a timely basis all relevant, non-privileged facts and evidence about individual misconduct such that prosecutors have the opportunity to effectively investigate and seek criminal charges against culpable individuals. Companies that identify significant facts but delay their disclosure will place in jeopardy their eligibility for cooperation credit. Companies seeking cooperation credit ultimately bear the burden of ensuring that documents are produced in a timely manner to prosecutors.

Likewise, production of evidence to the government that is most relevant for assessing individual culpability should be prioritized. Such priority evidence includes information and communications associated with relevant individuals during the period of misconduct. Department prosecutors will frequently identify the priority evidence they are seeking from a cooperating corporation, but in the absence of specific requests from prosecutors, cooperating corporations should understand that information pertaining to individual misconduct will be most significant.

Going forward, in connection with every corporate resolution, Department prosecutors must specifically assess whether the corporation provided cooperation in a timely fashion. Prosecutors will consider, for example, whether a company promptly notified prosecutors of particularly relevant information once it was discovered, or if the company instead delayed disclosure in a manner that inhibited the government's investigation. Where prosecutors identify undue or intentional delay in the production of information or documents—particularly with respect to documents that impact the government's ability to assess individual culpability—cooperation credit will be reduced or eliminated.

Finally, prosecutors must strive to complete investigations into individuals—and seek any warranted individual criminal charges—prior to or simultaneously with the entry of a resolution against the corporation. If prosecutors seek to resolve a corporate case prior to completing an investigation into responsible individuals, the prosecution or corporate resolution authorization memorandum must be accompanied by a memorandum that includes a discussion of all potentially culpable individuals, a description of the current status of the investigation regarding their conduct and the investigative work that remains to be done, and an investigative plan to bring the matter to resolution prior to the end of any statute of limitations period. *See* JM § 9-28.210. In such cases,

prosecutors must obtain the approval of the supervising United States Attorney or Assistant Attorney General of both the corporate resolution and the memorandum addressing responsible individuals.

B. Foreign Prosecutions of Individuals Responsible for Corporate Crime

The prosecution by foreign counterparts of individuals responsible for cross-border corporate crime plays an increasingly important role in holding individuals accountable and deterring future criminal conduct. Cooperation with foreign law enforcement partners—both in terms of evidence-sharing and capacity-building—has become a significant part of the Department's overall efforts to fight corporate crime. At the same time, the Department must continue to pursue forcefully its own individual prosecutions, as U.S. federal prosecution serves as a particularly significant instrument for accountability and deterrence.

At times, Department criminal investigations take place in parallel to criminal investigations by foreign jurisdictions into the same or related conduct. In such situations, the Department may learn that a foreign jurisdiction intends to bring criminal charges against an individual whom the Department is also investigating. The Principles of Federal Prosecution recognize that effective prosecution in another jurisdiction may be grounds to forego federal prosecution. JM § 9-27.220. Going forward, before declining to commence a prosecution in the United States on that basis, prosecutors must make a case-specific determination as to whether there is a significant likelihood that the individual will be subject to effective prosecution in the other jurisdiction. To determine whether an individual is subject to effective prosecution in another jurisdiction, prosecutors should consider, *inter alia*: (1) the strength of the other jurisdiction's interest in the prosecution; (2) the other jurisdiction's ability and willingness to prosecute effectively; and (3) the probable sentence and/or other consequences if the individual is convicted in the other jurisdiction. JM § 9-27.240.

When appropriate, Department prosecutors may wait to initiate a federal prosecution in order to better understand the scope and effectiveness of a prosecution in another jurisdiction. However, prosecutors should not delay commencing federal prosecution to the extent that delay could prevent the government from pursuing certain charges (*e.g.*, on statute of limitations grounds), reduce the chance of arresting the individual, or otherwise undermine the strength of the federal case.

Similarly, prosecutors should not be deterred from pursuing appropriate charges just because an individual liable for corporate crime is located outside the United States.

## II. Guidance on Corporate Accountability

A. Evaluating a Corporation's History of Misconduct

As discussed in the October 2021 Memorandum, in determining how best to resolve an investigation of corporate criminal activity, prosecutors should, among other factors, consider the corporation's record of past misconduct, including prior criminal, civil, and regulatory resolutions,

both domestically and internationally.[4] Consideration of a company's historical misconduct harmonizes the way the Department treats corporate and individual criminal histories, and ensures that prosecutors give due weight to an important factor in evaluating the proper form of resolution.

Not all instances of prior misconduct, however, are equally relevant or probative. To that end, prosecutors should consider the form of prior resolution and the associated sanctions or penalties, as well as the elapsed time between the instant misconduct, the prior resolution, and the conduct underlying the prior resolution. In general, prosecutors weighing these factors should assign the greatest significance to recent U.S. criminal resolutions, and to prior misconduct involving the same personnel or management. Dated conduct addressed by prior criminal resolutions entered into more than ten years before the conduct currently under investigation, and civil or regulatory resolutions that were finalized more than five years before the conduct currently under investigation, should generally be accorded less weight as such conduct may be generally less reflective of the corporation's current compliance culture, program, and risk tolerance.[5] However, depending on the facts of the particular case, even if it falls outside these time periods, repeated misconduct may be indicative of a corporation that operates without an appropriate compliance culture or institutional safeguards.

In addition to its form, Department prosecutors should consider the facts and circumstances underlying a corporation's prior resolution, including any factual admissions by the corporation. Prosecutors should consider the seriousness and pervasiveness of the misconduct underlying each prior resolution and whether that conduct was similar in nature to the instant misconduct under investigation, even if it was prosecuted under different statutes. Prosecutors should also consider whether at the time of the misconduct under review, the corporation was serving a term of probation or was subject to supervision, monitorship, or other obligation imposed by the prior resolution.

Corporations operate in varying regulatory and other environments, and prosecutors should be mindful when comparing corporate track records to ensure that any comparison is apt. For example, if a corporation operates in a highly regulated industry, a corporation's history of regulatory compliance or shortcomings should likely be compared to that of similarly situated companies in the industry. Prior resolutions that involved entities that do not have common management or share compliance resources with the entity under investigation, or that involved conduct that is not chargeable as a criminal violation under U.S. federal law, should also generally receive less weight. Prior misconduct committed by an acquired entity should receive less weight if the acquired entity has been integrated into an effective, well-designed compliance program at the acquiring corporation and if the acquiring corporation addressed the root cause of the prior

---

[4] The term "resolution" covers both post-trial adjudications and stipulated non-trial resolutions, such as plea agreements, non-prosecution agreements, deferred prosecution agreements, civil consent decrees and stipulated orders, and pre-trial regulatory enforcement actions.

[5] Corporations should be prepared to produce a list and summary of all prior criminal resolutions within the last ten years and all civil or regulatory resolutions within the last five years, as well as any known pending investigations by U.S. (federal and state) and foreign government authorities. Attorneys for the government may tailor (or expand) this request to obtain the information that would be most relevant to the Department's analysis.

misconduct before the conduct currently under investigation occurred, and full and timely remediation occurred within the acquired entity before the conduct currently under investigation.

Department prosecutors should also evaluate whether the conduct at issue in the prior and current matters reflects broader weaknesses in a corporation's compliance culture or practices. One consideration is whether the conduct occurred under the same management team and executive leadership. Overlap in involved personnel—at any level—could indicate a lack of commitment to compliance or insufficient oversight of compliance risk at the management or board level. Beyond personnel, prosecutors should consider whether the present and prior instances of misconduct share the same root causes. Prosecutors should also consider what remediation was taken to address the root causes of prior misconduct, including employee discipline, compensation clawbacks, restitution, management restructuring, and compliance program upgrades.

Multiple non-prosecution or deferred prosecution agreements are generally disfavored, especially where the matters at issue involve similar types of misconduct; the same personnel, officers, or executives; or the same entities. Before making a corporate resolution offer that would result in multiple non-prosecution or deferred prosecution agreements for a corporation (including its affiliated entities), Department prosecutors must secure the written approval of the responsible U.S. Attorney or Assistant Attorney General and provide notice to the Office of the Deputy Attorney General (ODAG) in the manner set forth in JM § 1-14.000. Notice provided to ODAG pursuant to JM § 1-14.000 must be made at least 10 business days prior to the issuance of an offer to the corporation, except in extraordinary circumstances.

While multiple deferred or non-prosecution agreements are generally disfavored, nothing in this memorandum should disincentivize corporations that have been the subject of prior resolutions from voluntarily disclosing misconduct to the Department. Department prosecutors must weigh and appropriately credit voluntary and timely self-disclosures of current or prior conduct. Indeed, timely voluntary disclosures do not simply reveal misconduct at a corporation; they can also reflect that a corporation is appropriately working to detect misconduct and takes seriously its responsibility to instill and act upon a culture of compliance. As set forth in the next section of this Memorandum, when determining the appropriate form and substance of a corporate criminal resolution for any corporation, including one with a prior resolution, prosecutors should consider whether the criminal conduct at issue came to light as a result of the corporation's timely, voluntary self-disclosure and credit such disclosure appropriately.

B. Voluntary Self-Disclosure by Corporations

In many circumstances, a corporation becomes aware of misconduct by employees or agents before that misconduct is publicly reported or otherwise known to the Department. In those cases, corporations may come to the Department and disclose this misconduct, enabling the government to investigate and hold wrongdoers accountable more quickly than would otherwise be the case. Department policies and procedures must ensure that a corporation benefits from its decision to come forward to the Department and voluntarily self-disclose misconduct, through resolution under more favorable terms than if the government had learned of the misconduct

through other means. And Department policies and procedures should be sufficiently transparent such that the benefits of voluntary self-disclosure are clear and predictable.

Many Department components that prosecute corporate criminal misconduct have already adopted policies regarding the treatment of corporations who voluntarily disclose their misconduct. *See, e.g.*, Foreign Corrupt Practices Act ("FCPA") Corporate Enforcement Policy (Criminal Division); Leniency Policy and Procedures (Antitrust Division); Export Control and Sanctions Enforcement Policy for Business Organizations (National Security Division); and Factors in Decisions on Criminal Prosecutions (Environment & Natural Resources Division). Of course, voluntary self-disclosure only occurs when companies disclose misconduct promptly and voluntarily (*i.e.*, where they have no preexisting obligation to disclose, such as pursuant to regulation, contract, or prior Department resolution) and when they do so prior to an imminent threat of disclosure or government investigation.[6]

Through this memorandum, I am directing each Department of Justice component that prosecutes corporate crime to review its policies on corporate voluntary self-disclosure, and if the component lacks a formal, written policy to incentivize such self-disclosure, it must draft and publicly share such a policy. Any such policy should set forth the component's expectations of what constitutes a voluntary self-disclosure, including with regard to the timing of the disclosure, the need for the disclosure to be accompanied by timely preservation, collection, and production of relevant documents and/or information, and a description of the types of information and facts that should be provided as part of the disclosure process.[7] The policies should also lay out the benefits that corporations can expect to receive if they meet the standards for voluntary self-disclosure under that component's policy.

All Department components must adhere to the following core principles regarding voluntary self-disclosure. First, absent the presence of aggravating factors, the Department will not seek a guilty plea where a corporation has voluntarily self-disclosed, fully cooperated, and timely and appropriately remediated the criminal conduct. Each component will, as part of its written guidance on voluntary self-disclosure, provide guidance on what circumstances would constitute such aggravating factors, but examples may include misconduct that poses a grave threat to national security or is deeply pervasive throughout the company. Second, the Department will not require the imposition of an independent compliance monitor for a cooperating corporation that voluntarily self-discloses the relevant conduct if, at the time of resolution, it also demonstrates that it has implemented and tested an effective compliance program. Such decisions about the

---

[6] Voluntary self-disclosure of misconduct is distinct from cooperation with the government's investigation, and prosecutors should thus consider these factors separately. *See, e.g.*, JM § 9-28.900 (addressing voluntary disclosures generally); JM § 9-47.120 (describing credit for voluntary self-disclosure in FCPA matters).

[7] For example, the FCPA Corporate Enforcement policy sets forth the following requirements for a corporation to receive credit for voluntary self-disclosure of wrongdoing: the disclosure must qualify under U.S.S.G. § 8C2.5(g)(1) as occurring "prior to an imminent threat of disclosure or government investigation"; the corporation must disclose the conduct to the Department "within a reasonably prompt time after becoming aware of the offense," with the burden on the corporation to demonstrate timeliness; and the corporation must disclose all relevant facts known to it, "including as to any individuals substantially involved in or responsible for the misconduct at issue." JM § 9-47.120.

imposition of a monitor will continue to be made on a case-by-case basis and at the sole discretion of the Department.

C. Evaluation of Cooperation by Corporations

Cooperation can be a mitigating factor, by which a corporation—just like any other subject of a criminal investigation—can gain credit in a case that is appropriate for indictment and prosecution. JM § 9-28.700. Eligibility for cooperation credit is not predicated upon the waiver of attorney-client privilege or work product protection. JM § 9-28.720.[8]

Credit for cooperation takes many forms and is calculated differently based on the degree to which a corporation cooperates with the government's investigation and the commitment that the corporation demonstrates in doing so. The level of a corporation's cooperation can affect the form of the resolution, the applicable fine range, and the undertakings involved in the resolution.

Many existing Department policies discuss the Department's expectations for full and effective cooperation. *See, e.g.*, JM § 9-28.720 (Cooperation: Disclosing the Relevant Facts); JM § 9-47.120, ¶ 1.3(b) (Full Cooperation in FCPA Matters). The Department will update the Justice Manual to ensure greater consistency across components as to the steps that a corporation will need to take to receive maximum credit for full cooperation.

Companies seeking credit for cooperation must timely preserve, collect, and disclose relevant documents located both within the United States and overseas. In some cases, data privacy laws, blocking statutes, or other restrictions imposed by foreign law may complicate the method of production of documents located overseas. In such cases, the cooperating corporation bears the burden of establishing the existence of any restriction on production and of identifying reasonable alternatives to provide the requested facts and evidence, and is expected to work diligently to identify all available legal bases to preserve, collect, and produce such documents, data, and other evidence expeditiously.[9]

Department prosecutors should provide credit to corporations that find ways to navigate such issues of foreign law and produce such records. Conversely, where a corporation actively seeks to capitalize on data privacy laws and similar statutes to shield misconduct inappropriately from detection and investigation by U.S. law enforcement, an adverse inference as to the corporation's cooperation may be applicable if such a corporation subsequently fails to produce foreign evidence.

---

[8] Instead, the sort of cooperation that is most valuable to resolving allegations of misconduct by a corporation and its officers, directors, employees, or agents is disclosure of the relevant facts concerning such misconduct. In this regard, the analysis parallels that for a non-corporate defendant, where cooperation typically requires disclosure of relevant factual knowledge and not of discussions between an individual and the individual's attorneys. *Id.*

[9] This requirement now applies to all corporations under investigation that are seeking to cooperate. The requirement already applies to investigations involving potential violations of the FCPA. *See* JM § 9-47.120.

D. Evaluation of a Corporation's Compliance Program

Although an effective compliance program and ethical corporate culture do not constitute a defense to prosecution of corporate misconduct, they can have a direct and significant impact on the terms of a corporation's potential resolution with the Department. Prosecutors should evaluate a corporation's compliance program as a factor in determining the appropriate terms for a corporate resolution, including whether an independent compliance monitor is warranted.[10] Prosecutors should assess the adequacy and effectiveness of the corporation's compliance program at two points in time: (1) the time of the offense; and (2) the time of a charging decision. The same criteria should be used in each instance.

Prosecutors should evaluate the corporation's commitment to fostering a strong culture of compliance at all levels of the corporation—not just within its compliance department. For example, as part of this evaluation, prosecutors should consider how the corporation has incentivized or sanctioned employee, executive, and director behavior, including through compensation plans, as part of its efforts to create a culture of compliance.

There are many factors that prosecutors should consider when evaluating a corporate compliance program. The Criminal Division has developed resources to assist prosecutors in assessing the effectiveness of a corporation's compliance program. *See* Criminal Division, Evaluation of Corporate Compliance Programs (updated June 2020). Additional guidance has been provided by other Department components as to specialized areas of corporate compliance. *See, e.g.*, Antitrust Division, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (July 2019). Prosecutors should consider, among other factors, whether the corporation's compliance program is well designed, adequately resourced, empowered to function effectively, and working in practice. Prior guidance has identified numerous considerations for this evaluation, including, *inter alia*, how corporations measure and identify compliance risk; how they monitor payment and vendor systems for suspicious transactions; how they make disciplinary decisions within the human resources process; and how senior leaders have, through their words and actions, encouraged or discouraged compliance.

In addition to those factors, this Memorandum identifies additional metrics relevant to prosecutors' evaluation of a corporation's compliance program and culture.

1. Compensation Structures that Promote Compliance

Corporations can help to deter criminal activity if they reward compliant behavior and penalize individuals who engage in misconduct. Compensation systems that clearly and effectively impose financial penalties for misconduct can incentivize compliant conduct, deter risky behavior, and instill a corporate culture in which employees follow the law and avoid legal "gray areas." When conducting this evaluation, prosecutors should consider how the corporation

[10] At the same time, the mere existence of a compliance program is not sufficient, in and of itself, to justify not charging a corporation for criminal misconduct undertaken by its officers, directors, employees, or agents. *See* JM 9-28.800.

has incentivized employee behavior as part of its efforts to create a culture of ethics and compliance within its organization.

Corporations can best deter misconduct if they make clear that all individuals who engage in or contribute to criminal misconduct will be held personally accountable. In assessing a compliance program, prosecutors should consider whether the corporation's compensation agreements, arrangements, and packages (the "compensation systems") incorporate elements—such as compensation clawback provisions—that enable penalties to be levied against current or former employees, executives, or directors whose direct or supervisory actions or omissions contributed to criminal conduct. Since misconduct is often discovered after it has occurred, prosecutors should examine whether compensation systems are crafted in a way that allows for retroactive discipline, including through the use of clawback measures, partial escrowing of compensation, or equivalent arrangements.

Similarly, corporations can promote an ethical corporate culture by rewarding those executives and employees who promote compliance within the organization. Prosecutors should therefore also consider whether a corporation's compensation systems provide affirmative incentives for compliance-promoting behavior. Affirmative incentives include, for example, the use of compliance metrics and benchmarks in compensation calculations and the use of performance reviews that measure and reward compliance-promoting behavior, both as to the employee and any subordinates whom they supervise. When effectively implemented, such provisions incentivize executives and employees to engage in and promote compliant behavior and emphasize the corporation's commitment to its compliance programs and its culture.

Prosecutors should look to what has happened in practice at a corporation—not just what is written down. As part of their evaluation of a corporation's compliance program, prosecutors should review a corporation's policies and practices regarding compensation and determine whether they are followed in practice. If a corporation has included clawback provisions in its compensation agreements, prosecutors should consider whether, following the corporation's discovery of misconduct, a corporation has, to the extent possible, taken affirmative steps to execute on such agreements and clawback compensation previously paid to current or former executives whose actions or omissions resulted in, or contributed to, the criminal conduct at issue.

Finally, prosecutors should consider whether a corporation uses or has used non-disclosure or non-disparagement provisions in compensation agreements, severance agreements, or other financial arrangements so as to inhibit the public disclosure of criminal misconduct by the corporation or its employees.

The use of financial incentives to align the interests of the C-suite with the interests of the compliance department can greatly amplify a corporation's overall level of compliance. To that end, I have asked the Criminal Division to develop further guidance by the end of the year on how to reward corporations that develop and apply compensation clawback policies, including how to shift the burden of corporate financial penalties away from shareholders—who in many cases do not have a role in misconduct—onto those more directly responsible.

2. Use of Personal Devices and Third-Party Applications

The ubiquity of personal smartphones, tablets, laptops, and other devices poses significant corporate compliance risks, particularly as to the ability of companies to monitor the use of such devices for misconduct and to recover relevant data from them during a subsequent investigation. The rise in use of third-party messaging platforms, including the use of ephemeral and encrypted messaging applications, poses a similar challenge.

Many companies require all work to be conducted on corporate devices; others permit the use of personal devices but limit their use for business purposes to authorized applications and platforms that preserve data and communications for compliance review. How companies address the use of personal devices and third-party messaging platforms can impact a prosecutor's evaluation of the effectiveness of a corporation's compliance program, as well as the assessment of a corporation's cooperation during a criminal investigation.

As part of evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential violations of law, prosecutors should consider whether the corporation has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved. To assist prosecutors in this evaluation, I have asked the Criminal Division to further study best corporate practices regarding use of personal devices and third-party messaging platforms and incorporate the product of that effort into the next edition of its Evaluation of Corporate Compliance Programs, so that the Department can address these issues thoughtfully and consistently.

As a general rule, all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, should provide clear training to employees about such policies, and should enforce such policies when violations are identified. Prosecutors should also consider whether a corporation seeking cooperation credit in connection with an investigation has instituted policies to ensure that it will be able to collect and provide to the government all non-privileged responsive documents relevant to the investigation, including work-related communications (*e.g.*, texts, e-messages, or chats), and data contained on phones, tablets, or other devices that are used by its employees for business purposes.

## III. Independent Compliance Monitorships[11]

As set forth in the October 2021 Memorandum, Department prosecutors will not apply any general presumption against requiring an independent compliance monitor ("monitor") as part of a corporate criminal resolution, nor will they apply any presumption in favor of imposing one.

[11] In September 2021, the Associate Attorney General issued a memorandum concerning the use of monitorships in civil settlements involving state and local governmental entities. Memorandum from Associate Attorney General Vanita Gupta, "Review of the Use of Monitors in Civil Settlement Agreements and Consent Decrees Involving State and Local Government Entities," Sept. 13, 2021. That memorandum continues to govern the use of monitors in those cases.

Rather, the need for a monitor and the scope of any monitorship must depend on the facts and circumstances of the particular case.

A. Factors to Consider When Evaluating Whether a Monitor is Appropriate

Independent compliance monitors can be an effective means of reducing the risk of further corporate misconduct and rectifying compliance lapses identified during a corporate criminal investigation. Prosecutors should analyze and carefully assess the need for a monitor on a case-by-case basis, using the following non-exhaustive list of factors when evaluating the necessity and potential benefits of a monitor:[12]

1. Whether the corporation voluntarily self-disclosed the underlying misconduct in a manner that satisfies the particular DOJ component's self-disclosure policy;

2. Whether, at the time of the resolution and after a thorough risk assessment, the corporation has implemented an effective compliance program and sufficient internal controls to detect and prevent similar misconduct in the future;

3. Whether, at the time of the resolution, the corporation has adequately tested its compliance program and internal controls to demonstrate that they would likely detect and prevent similar misconduct in the future;

4. Whether the underlying criminal conduct was long-lasting or pervasive across the business organization or was approved, facilitated, or ignored by senior management, executives, or directors (including by means of a corporate culture that tolerated risky behavior or misconduct, or did not encourage open discussion and reporting of possible risks and concerns);

5. Whether the underlying criminal conduct involved the exploitation of an inadequate compliance program or system of internal controls;

6. Whether the underlying criminal conduct involved active participation of compliance personnel or the failure of compliance personnel to appropriately escalate or respond to red flags;

7. Whether the corporation took adequate investigative or remedial measures to address the underlying criminal conduct, including, where appropriate, the termination of business relationships and practices that contributed to the criminal conduct, and discipline or termination of personnel involved, including with respect to those with supervisory, management, or oversight responsibilities for the misconduct;

8. Whether, at the time of the resolution, the corporation's risk profile has substantially changed, such that the risk of recurrence of the misconduct is minimal or nonexistent;

[12] For components or U.S. Attorney's Offices that do not have extensive corporate resolution experience, consultation with DOJ components that more routinely assess such compliance programs, internal controls, and remedial measures is recommended.

9. Whether the corporation faces any unique risks or compliance challenges, including with respect to the particular region or business sector in which the corporation operates or the nature of the corporation's customers; and

10. Whether and to what extent the corporation is subject to oversight from industry regulators or a monitor imposed by another domestic or foreign enforcement authority or regulator.

The factors listed above are intended to be illustrative of those that should be evaluated and are not an exhaustive list of potentially relevant considerations. Department attorneys should determine whether a monitor is required based on the facts and circumstances presented in each case.

B. Selection of Monitors

In selecting a monitor, prosecutors should employ consistent and transparent procedures. Monitor selection should be performed pursuant to a documented selection process that is readily available to the public. *See, e.g.,* Memorandum of Assistant Attorney General Brian A. Benczkowski, Selection of Monitors in Criminal Division Matters, Oct. 11, 2018, Section E ("The Selection Process"); Environment and Natural Resources Division, Environmental Crimes Section, Corporate Monitors: Selection Best Practices (Mar. 2018); Antitrust Division, Selection of Monitors in Criminal Cases (July 2019).[13] Every component involved in corporate criminal resolutions that does not currently have a public monitor selection process must adopt an already existing Department process, or develop and publish its own selection process before December 31, 2022.[14] All new selection processes must be approved by ODAG and made public before their implementation as part of any corporate criminal resolution. The appropriate United States Attorney or Department Component Head shall also provide a copy of the process to the Assistant Attorney General for the Criminal Division, who shall maintain a record of such processes.

Any selection process must incorporate elements that promote consistency, predictability, and transparency. First, per existing policy, the consideration of monitor candidates shall be done by a standing or *ad hoc* committee within the office or component where the case originated. To the extent that such committees did not previously do so, every monitorship committee must now include as a member an ethics official or professional responsibility officer from that office or component, who shall ensure that the other members of the committee do not have any conflicts of interest in selection of the monitor. There shall be a written memorandum to file confirming that no conflicts exist in the committee prior to the selection process or as to the monitor prior to the commencement of the monitor's work. Second, monitor selection processes shall be conducted in keeping with the Department's commitment to diversity and inclusion. Third, prosecutors shall

[13] This requirement does not apply to cases involving court-appointed monitors, where prosecutors must give due regard to the appropriate role and procedures of the court.

[14] Unless they adopt and publish their own processes pursuant to the principles set forth herein, U.S. Attorney's Offices should follow the selection process developed by the Criminal Division, unless partnering with a Department component that has its own preexisting selection process.

notify the appropriate United States Attorney or Department Component Head of their decision regarding whether to require an independent compliance monitor. In order to promote greater transparency, any agreement imposing a monitorship should describe the reasoning for requiring a monitor.[15] ODAG must approve the monitor selection for all cases in which a monitor is recommended, unless the monitor is court-appointed.[16]

C. Continued Review of Monitorships

In matters where an independent corporate monitor is imposed pursuant to a resolution with the Department, prosecutors should ensure that the monitor's responsibilities and scope of authority are well-defined and recorded in writing, and that a clear workplan is agreed upon between the monitor and the corporation—all to ensure agreement among the corporation, monitor, and Department as to the proper scope of review.

For the term of the monitorship, Department prosecutors must remain apprised of the ongoing work conducted by the monitor.[17] Continued review of the monitorship requires ongoing communication with both the monitor and the corporation.[18]

Prosecutors should receive regular updates from the monitor about the status of the monitorship and any issues presented. Monitors should promptly alert prosecutors if they are being denied access to information, resources, or corporate employees or agents necessary to execute their charge. Prosecutors should also regularly receive information about the work the monitor is doing to ensure that it remains tailored to the workplan and scope of the monitorship. In reviewing information relating to the monitor's work, prosecutors should consider the reasonableness of the monitor's review, including, where appropriate, issues relating to the cost of the monitor's work. In certain cases, prosecutors may determine that the initial term of the monitorship is longer than necessary to address the concerns that created the need for the monitor, or that the scope of the monitorship is broader than necessary to accomplish the goals of the monitorship. For example, a corporation may demonstrate significant and faster-than-anticipated improvements to its compliance program, and this could reduce the need for continued monitoring. Conversely, prosecutors may determine that newly identified concerns require lengthening the term or amending the scope of the monitorship.

---

[15] The appropriate United States Attorney or Department Component Head shall, in turn, provide a copy of the agreement to the Assistant Attorney General for the Criminal Division at a reasonable time after it has been executed. The Assistant Attorney General for the Criminal Division shall maintain a record of all such agreements.

[16] *See* Morford Memorandum, at p. 3 (requiring, for cases involving the use of monitors in DPAs and NPAs, that "the Office of the Deputy Attorney General must approve the monitor").

[17] In cases of court-appointed monitors, the court may elect to oversee this inquiry.

[18] Per existing policy, any agreement requiring a monitor should also explain what role the Department could play in resolving disputes that may arise between the monitor and the corporation, given the facts and circumstances of the case. *See* Acting Deputy Attorney General Gary C. Grindler, "Additional Guidance on the Use of Monitors in Deferred Prosecutions and Non-Prosecution Agreements with Corporation," May 25, 2010.

## IV. Commitment to Transparency in Corporate Criminal Enforcement

Transparency regarding the Department's corporate criminal enforcement priorities and processes—including its expectations as to corporate cooperation and compliance, and the consequences of meeting or failing to meet those expectations—can encourage companies to adopt robust compliance programs, voluntarily disclose misconduct, and cooperate fully with the Department's investigations. Transparency can also instill public confidence in the Department's work.

When the Department elects to enter into an agreement to resolve corporate criminal liability, the agreement should, to the greatest extent possible, include: (1) an agreed-upon statement of facts outlining the criminal conduct that forms the basis for the agreement; and (2) a statement of relevant considerations that explains the Department's reasons for entering into the agreement. Relevant considerations may, for example, include the corporation's voluntary self-disclosure, cooperation, and remedial efforts (or lack thereof); the cooperation credit, if any, that the corporation is receiving; the seriousness and pervasiveness of the criminal conduct; the corporation's history of misconduct; the state of the corporation's compliance program at the time of the underlying criminal conduct and the time of the resolution; the reasons for imposing an independent compliance monitor or any other compliance undertaking, if applicable; other applicable factors listed in JM § 9-28.300; and any other key considerations related to the Department's decision regarding the resolution.

Absent exceptional circumstances, corporate criminal resolution agreements will be published on the Department's public website.

***

Robust corporate criminal enforcement remains central to preserving the rule of law—ensuring the same accountability for all, regardless of station or privilege. Thank you for the work you do every day to fulfill the Department's mission.

*Published in* Legaltech News

As eDiscovery practitioners cautiously resume in-person conferences and social gatherings, one topic is dominating conversations: the discovery challenges posed by "modern attachments" within the Microsoft 365 ("M365") environment. A dearth of jurisprudence and little practical guidance is available on this topic; yet the technology continues to rapidly evolve. We prepared this series of articles to provide guidance to discovery practitioners, in-house counsel, and service providers.

One of the foremost issues raised by this evolving technology is whether litigants can, should, or perhaps even *must* treat "modern attachments" like traditional email attachments. Historically, email attachments have been considered part of an email "family" in discovery because they are actually part of the .msg email file. With "modern attachments," however, the "attached" files are *not* part of the underlying message file; no "family" exists in the traditional sense. Litigants and their counsel are weighing any benefits against the risks and burdens associated with treating these documents like traditional email attachments for discovery purposes, where no such "family" relationship exists in the files as they are maintained in the ordinary course of business.

In this first article, we explain what "modern attachments" are and why they are keeping eDiscovery practitioners up at night. We will make a case for changing how our industry talks about these documents, why "pointer" is a more accurate term than the misleading "modern attachment," and why that change in terminology should have a positive impact on how we approach discovery of this information. Later articles will discuss specific discovery challenges posed by "modern attachments," from preservation through production, which depend in large part on which discovery tool or M365 licensing an organization is using. We also will identify emerging best practices and wrap up with a list of key takeaways. The authors recognize that "modern attachments" are not limited to M365 and are at issue in other enterprise platforms, like Slack, but given the prevalence of the platform, this article series will focus on M365.

**WHAT ARE "MODERN ATTACHMENTS" AND WHY SHOULD YOU CARE?**

Organizations deploying collaboration platforms with short messaging/chat functionality are likely to use "modern attachments." For example, the M365 tenant can be configured such that when users share documents, the files themselves are not transmitted with the message; instead, users are able to send messages that include a link that points to documents stored elsewhere. Users in Outlook or Teams can send messages containing a link that points to content stored in a separate location within the same M365 tenant, often in SharePoint or OneDrive. Storing the document separately from the message allows for ongoing collaboration among multiple users while eliminating the need for continually circulating many duplicate versions of a file.

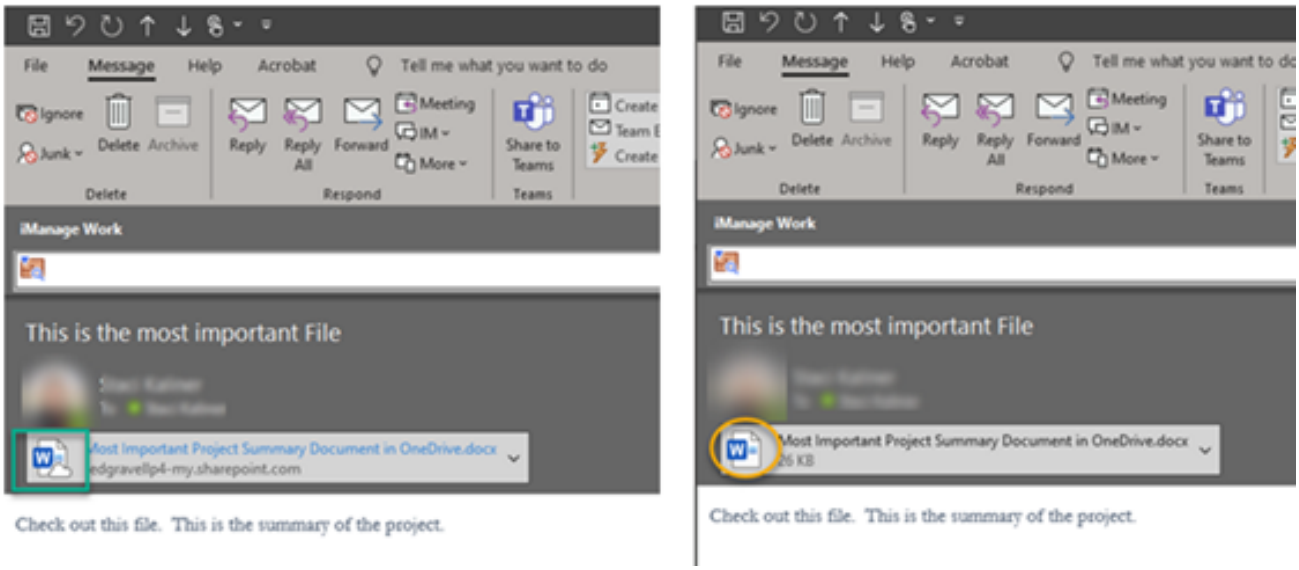
Microsoft generally refers to the referenced content as "modern attachments" or sometimes "cloud attachments," while others in the industry may refer to these as "linked files" or simply "attachments." Unlike traditional email file attachments that are saved within the email .msg container with the associated message body and metadata, the files referenced in Outlook or Teams messages that are stored elsewhere may not be static. This means that the version of the file that is referenced from the sender's message may have been edited or deleted when the recipient returns to the message and accesses the file, or may have been edited or deleted at a later time before the document is identified as subject to discovery.

Given the ubiquity of M365 and similar platforms, eDiscovery practitioners are grappling with whether the "as sent" version of the document that is referenced in the associated message can be retained, collected,

reviewed, and/or produced for discovery purposes, and perhaps even more importantly, are asking: Does it need to be? Whether and how it can be depends on what M365 discovery tools and M365 licensing an organization is using and the functionality of those tools, which Microsoft is updating in real time. Answering the fundamental question of "Do we need to do this?" is more complex and requires a multi-faceted risk analysis specific to the organization and its litigation profile. We plan to explore these technical and legal challenges in future articles but first need to address the terminology surrounding these documents.

**POINTERS NOT ATTACHMENTS**

As noted above, Microsoft generally refers to documents stored in a separate location from the associated message as "modern attachments" or "cloud attachments," but eDiscovery practitioners understand that these are not attachments at all; rather, they are links embedded in messages that reference files stored in the organization's M365 cloud. (While users also can send messages that include a link that references files stored outside the client's M365 cloud and/or outside the client's IT infrastructure, those pointers are beyond the scope of this article series). These "modern attachments" may present to the user like any other more traditional file attachment. In Outlook, for example, the only visual difference between a traditional attachment and a "modern attachment" to the user is that a message with a "modern attachment" includes a cloud icon:




"Modern attachment" (left) vs. Traditional attachment

We posit that the term "pointer" is a far more apt description of the functionality here. Senders are pointing the recipient of the message to a location in the cloud where a specific document or file is stored. Pointers are one-directional, meaning the message references data stored in another source or location, but the source or location does not point back to the message. Stated simply, pointers are *not* attachments. Adopting the use of pointer for these documents may facilitate a more robust discussion within our industry as to whether it makes sense to treat the message and referenced content separately for discovery purposes. With this new terminology, we can develop meaningful strategies for defensible workflows, rather than simply defaulting to treating the message and referenced content like the traditional "parent/child" or "family" relationships that historically have been central to modern discovery practices. As we continue this series, we will use the terms "pointer" and "referenced content" and encourage others in the industry to join us in adopting this terminology going forward.

***Authors' Note**: M365 is a cloud-based application that Microsoft is continually updating, which means the actual M365 functionality available in any tenant may differ from what is described in this article.*

*Staci Kaliner, Managing Director, routinely advises clients on the design and implementation of leading practice processes to support and reduce the eDiscovery related litigation risk, build efficacies into their operations, and identify and implement information governance best practices. She can be contacted at skaliner@redgravellp.com.*

*Monica McCarroll, Partner, is a trial attorney specializing in complex civil litigation and focuses her practice on providing advice and counsel on eDiscovery, information governance, and cybersecurity issues, including addressing the complicated discovery issues that often arise in litigation. She can be contacted at mmccarroll@redgravellp.com.*

*Ben Barnes, Counsel, has extensive experience in information law matters, and advises clients on eDiscovery, information governance, and data privacy issues and strategies. He can be contacted at bbarnes@redgravellp.com.*

*The view and opinions expressed herein are those of the authors and do not necessarily reflect the views of either Redgrave LLP or any client of the Firm.*

2022 WL 815818
Only the Westlaw citation is currently available.
United States District Court, D. New Jersey.

Antoinette Judy FAMULARE, Plaintiff,

v.

GANNETT CO., INC. et al., Defendants.

Civ. No. 2:20-cv-13991(WJM)
|
Signed 03/17/2022

**Attorneys and Law Firms**

David Zatuchni, Zatuchni & Associates, LLC, Lambertville, NJ, Hope A. Lang, Oradell, NJ, for Plaintiff.

Samuel J. Samaro, Zachary Aaron Levy, Pashman Stein Walder Hayden, P.C., Hackensack, NJ, James W. Boyan, III, The Prudential Insurance Company of America, Newark, NJ, for Defendants.

**OPINION**

WILLIAM J. MARTINI, United States District Judge

***1** Before the Court is Defendants Gannett Co., Inc., Gannett Satellite Information Network, LLC, and LocalIQ, LLC's (collectively, "Gannett" or "Defendants") appeal, ECF No. 27, pursuant to Federal Rule of Civil Procedure 72(a) and Local Civil Rule 72.1(c)(1)(A), of Magistrate Judge Michael A. Hammer's December 6, 2021 text order, ECF No. 23. The Court has reviewed the parties' submissions, ECF Nos. 27, 33, 34, 36, and decides the matter on the papers without oral argument. *See* Fed. R. Civ. P. 78(b); L. Civ. R. 78.1(b). For the reasons stated below, Defendants' appeal is **DENIED**.

The discovery dispute underlying this appeal concerns whether Defendants are obligated to produce screenshots of certain computer-generated reports from Defendants' online computer program known as Salesforce. According to Plaintiff Antoinette Famulare ("Plaintiff"), a former Gannett Account Executive, Salesforce maintains and memorializes various performance metrics of individual Account Executives and offers users the ability to generate reports of those metrics for a specified time period. Plaintiff generated and printed such reports of her own performance metrics and seeks in discovery the same reports for certain other Gannett employees for purposes of comparison. Defendants assert that the reports Plaintiff produced and printed are not free-standing, fixed reports, but are screenshots of the Salesforce "Dashboard" that displays the user's real-time data. As a result, Defendants argue they cannot generate or print out the reports that Plaintiff requests and can only provide her with Salesforce's underlying historical data exported to a Microsoft Excel spreadsheet. Defendants have already produced that Excel spreadsheet to Plaintiff.

On December 6, 2021, following a telephone conference with the parties, Judge Hammer entered the following text order on the docket:

> For the reasons set forth on the record on December 6, 2021, pursuant to Federal Rule of Civil Procedure 34(b)(2)(E)(i), to the extent possible, Defendant shall produce the reports in screenshot format in addition to the Excel spreadsheet format already produced. Counsel shall schedule and take the Rule 30(b)(6) deposition of a Defendant representative on this issue, if Defendant maintains that it cannot produce the screenshot format.

ECF No. 23 (abridged).

On the telephone conference, the parties presented to Judge Hammer the fundamental dispute concerning the functionality of Salesforce and whether the requested reports can be generated and printed as Plaintiff maintains they can be, or whether Salesforce is incapable of generating and printing the reports as Defendants maintain it is. *See generally* Dec. 6 Hr'g Tr., ECF No. 33. Upon hearing the parties' arguments, Judge Hammer concluded that a Rule 30(b)(6) deposition of an appropriate representative was "clearly going to have to happen" to allow Plaintiff to investigate why "all they can get in response to the document production request is the Excel spreadsheet." *Id.* 16:5-16:10; *see also id.* 13:9-13:11 ("[I]t seems fairly clear to me that this is going to have to go to that Rule 30(b)(6) deposition that

we were discussing."); *id.* 15:20-15:21 ("[W]e'll have to let the Rule 30(b)(6) deposition play out"). Judge Hammer then proceeded to twice clarify that to the extent Defendants can print and produce the individual screenshots of the reports because that is how the information is stored in the ordinary course of business, then Defendants have "that production obligation," but "[w]hether [Defendants] can actually do that will be ... capable of determination only after the deposition, the Rule 30(b)(6) deposition." *Id.* 16:11-16:19; *id.* 18:5-18:15 ("[I]t strikes me that that is exactly how they're kept in the ordinary course of business, since the employees in the ordinary course of business are accessing the information that way.... But, as we said, until the Rule 30(b)(6) deposition is completed ... we just don't know.").

***2** On December 20, 2021, Defendants appealed Judge Hammer's text order on the grounds that it requires them to produce electronically stored information ("ESI") in a second format in contravention of Federal Rule of Civil Procedure 34(b)(2)(E)(iii). [1] Def. Br. at 4-5, ECF No. 27-1.

A Magistrate Judge's non-dispositive order may be set aside if it is clearly erroneous or contrary to law. 28 U.S.C. § 636(b)(1)(A). In this District, when "the magistrate [judge] has ruled on a non-dispositive matter such as a discovery motion, his or her ruling is entitled to great deference and is reversible only for abuse of discretion." *Kresefsky v. Panasonic Communs. & Sys. Co.*, 169 F.R.D. 54, 64 (D.N.J. 1996). The appellant bears the burden of demonstrating that the standard for modifying or setting aside the Magistrate Judge's ruling has been met. *Marks v. Struble*, 347 F. Supp. 2d 136, 149 (D.N.J. 2004).

Defendants have not persuaded this Court that the December 6, 2021 text order is clearly erroneous, contrary to law, or an abuse of Judge Hammer's discretion. Indeed, Defendants have not presented a genuine conflict between the text order and their discovery obligations. On the one hand, they argue that the text order impermissibly requires them to produce ESI in a second format, Def. Br. at 4-5, ECF No. 27-1; but on the other, they continue to argue that "it is not possible to give Plaintiff this actual information in the form of screenshots of the Salesforce Dashboard due to the dynamic nature of the platform." Def. Reply at 7, ECF No. 36. It is precisely because of this latter argument that Judge Hammer afforded Defendants the option of providing an appropriate representative to testify at a Rule 30(b)(6) deposition on Salesforce's functionality and how it reports or maintains the data at issue. To the extent Defendants now argue "there is no basis to have a corporate representative deposed about whether Defendants have the capability to take screenshots," Def. Br. at 1, ECF No. 27-1, that position starkly contrasts their prior representations at the parties' meet-and-confer and on the December 6, 2021 telephone conference that they are "happy to have [Plaintiff] take [the deposition] and speak with our client representatives who can tell them about what's possible and what's not." Dec. 6 Hr'g Tr. 6:2-6:8, ECF No. 33.

Additionally, Defendants rely heavily on information drawn from certifications by Gannett employees and exhibits attached thereto to explain to this Court about Salesforce's functionality and how it maintains and stores data. *See* Def. Reply at 4-8, ECF No. 36. "Because the functionality of Salesforce is the core issue in this motion," Defendants "respectfully submit[ ] that the Court should decide it based on credible information." *Id.* at 3. The Court agrees, but as Defendants acknowledge, this information was not previously presented to or available to Judge Hammer for consideration. *See id.* at 12. This Court "may not take into consideration any evidence that was not put forth before the magistrate judge when reviewing the magistrate judge's factual determination." *Haines v. Liggett Group, Inc.*, 975 F.2d 81, 92 (3d Cir. 1992). That Defendants need to rely on outside evidence to explain the functionality of Salesforce only underscores the clear need for a Rule 30(b)(6) deposition and a more developed record on this topic, as Judge Hammer repeatedly stated to the parties on the December 6, 2021 telephone conference. The Court reiterates Judge Hammer's sentiments that until that deposition is completed, the nature of the Salesforce program and its capabilities are unknown.

***3** Accordingly, Defendants' appeal, ECF No. 27, is **DENIED** and Judge Hammer's text order, ECF No. 23, is **AFFIRMED**. An appropriate Order shall follow.

**All Citations**

Slip Copy, 2022 WL 815818

## Footnotes

1 Federal Rule of Civil Procedure 34(b)(2)(E)(iii) states "[a] party need not produce the same electronically stored information in more than one form."

End of Document

Consilio / ADVANCED LEARNING INSTITUTE

# EMOJI IN EDISCOVERY: TECHNICAL AND INTERPRETIVE CHALLENGES

*by Matthew Verga,*
*Director of Education*

As smartphones and social media communication channels have become more frequent sources, so too have emoji shown up more frequently in cases. In 2019, Santa Clara University Professor of Law Eric Goldman published "Emojis and the Law" in the Washington Law Review, which revealed that "[b]etween 2004 and 2019, there was an exponential rise in emoji and emoticon references in US court opinions, with **over 30 percent of all cases appearing in 2018**" [emphasis added]. Examples range from landlord disputes to sex trafficking cases.

As they increase in frequency, emoji are creating special challenges for eDiscovery and litigation – both technical challenges and challenges of interpretation.

## What Are Emoji and Why Do They Matter?

First came emoticons, which were representations of different facial expressions created using punctuation and other characters, like the classic smiley face 😀 or winking face 😉. These representations could be used to add an indication of tone or emotion to a short text message, or as a reaction message by themselves.

| Icon | | | | | | | | | | | Emoji |
|---|---|---|---|---|---|---|---|---|---|---|---|
| :-)<br>:) | :-]<br>:] | :-3<br>:3 | :->><br>:> | 8-)<br>8) | :-}<br>:} | :o) | :c) | :^) | =] | =) | ☺🙂😊😀😁 |
| :-D<br>:D | 8-D<br>8D | x-D<br>xD | X-D<br>XD | =D | =3 | B^D | c: | C: | | | 😃😄😆😍 |
| :-)) | | | | | | | | | | | |
| :-(<br>:( | :-c<br>:c | :-<<br>:< | :-[<br>:[ | :-\|\| | >:[ | :{ | :@ | :( | ;( | | ☹🙁😠😡😒😓😞😖😫 |
| :'-(<br>:'( | | | | | | | | | | | 😢😭 |
| :'-)<br>:') | | | | | | | | | | | 😂 |

As mobile devices and the software running on them became more sophisticated, emoticons were supplanted by emoji, which replaced the punctuation-based representations with tiny images of assorted facial expressions and, eventually, other things.


Adoption was rapid and widespread. In 2015, an emoji was selected was selected as Oxford Dictionaries' word of the year ("the crying-from-laughter / crying-from-happiness emoji — officially known as the Face with Tears of Joy emoji"). By 2019, according to a survey report from Adobe, more than 90% were using emoji in personal communications, and more than 60% were using emoji in work communications. For example, according to a Microsoft spokeswoman, emoji use in 2019 was "basically universal" among the 13 million daily active users of Microsoft Teams. And, as noted above, the dramatic increase in their usage has led to a corresponding increase in their appearance in litigation.

## What Technical Challenges Do They Cause?

Emoji carry with them a number of technical challenges for discovery and litigation. First, there are many of them, and the number grows every year. Today, there are more than 3,500 emoji recognized by the Unicode Consortium. Beyond those cross-platform emoji,

many platforms also include platform-specific emoji or allow for the creation of custom emoji. In popular collaboration tool Slack, for example, "26 million custom emojis have been created since the feature was introduced." This makes it a challenge for discovery tool developers attempting to support emoji to keep up with the increasing volume and growing diversity of emoji that may need to be collected, reviewed, and produced.

These myriad emoji also work in different ways. The cross-platform emoji recognized by the Unicode Consortium exist as alphanumeric codes that various software knows to replace by displaying a corresponding image. This is the same way that the display of various currency, language, and technical symbols has been handled since Unicode was first introduced in 1991. The platform-specific and user-created emoji, however, may be based on custom, platform-specific codes, or they may exist only as image files that function more like attachments. This further complicates the development challenges for makers of discovery tools.

These same challenges also affect legal practice in ways beyond just discovery tool development challenges. As Professor Goldman said:

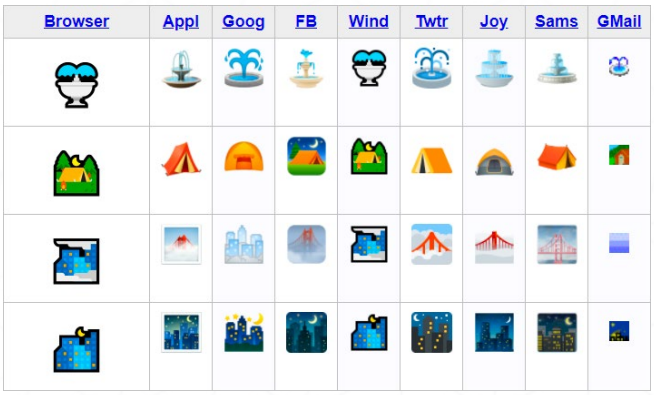
> Unfortunately, opinions still struggle with displaying Emoji. Opinions routinely omit the emoji altogether, or the judge imprecisely characterizes the emoji in evidence. (It doesn't help to call an emoji a 'smiley' because there are a dozen different smiling emoji symbols). Furthermore, Westlaw and Lexis still usually do not display emoji, and neither makes it possible to search for emoji in court opinions.

## What Interpretation Challenges Do They Cause?

Emoji create a few different interpretation challenges. First, communicating through an image or a series of images can be more ambiguous than communicating through words and sentences. It may not be clear to you later what a particular custodian in your case was attempting to communicate with a particular string of Emoji. Moreover, the message recipient's interpretation may have differed from the message sender's intention.

Second, there is a challenge associated with the contextual relationship between emoji and text when they are used together. As noted above, not all discovery tools are able to capture or display all the different emoji or all the different types of emoji, which can lead to material alterations to messages and their meaning. For example, a message might include an emoji indicating it was intended humorously or sarcastically. If that emoji is omitted during collection or not displayed during review, the message might appear misleadingly serious or literal.

On top of those issues, there is an additional challenge created by the way that the Unicode-based cross-platform emoji work. Although which emoji matches with which code is standardized, each developer gets to create its own version of the images that will actually be displayed in that software or on that device, so the same emoji will look different depending on where it is viewed. Apple, Google, Samsung, LG, and Microsoft, as well as Facebook, Twitter, Snapchat, and Instagram, all have their own versions of the Unicode emoji. For example:




These variations can be inconsequential, or they can exacerbate both of the interpretation challenges described above, depending on which emoji were used and how much those particular emoji vary in appearance across platforms. In some instances, the sender, recipient, and later reviewers might all be seeing different things that suggest different connotations.

## In What Kinds of Cases Have Emoticons or Emoji Appeared?

Emoticons and emoji have shown up in mobile, social, and email communications in a wide variety of case types over the past decade, such as:

- In the case of *Lenz v. Universal Music Corp.*, No. C 07-3783 JF (N.D. Cal. Feb. 25, 2010), the plaintiff won partial summary judgment, in part, because a winking smiley face emoticon was taken, in context, as an indication of the plaintiff's humor or sarcasm about the "stilted language" of lawyers.
- In the case of *Elonis v. United States*, in a February 14, 2014, Petition for a Writ of Certiorari to the Supreme Court, the petitioner argued, *inter alia*, that an allegedly threatening Facebook status update was "meant in 'jest'" as indicated by his having "ended the post with an 'emoticon' of a face sticking its tongue out."
- In the disability discrimination and retaliation case of *Apatoff v Munich Re Servs. Inc.*, No. 11-7570 (RBK/KMW) (D.N.J. August 1, 2014), the plaintiff survived summary judgment on certain claims, in part, because of emoticons used in email messages:

> The Court believes that a reasonable jury could find that the "emoticons," attached to the emails of two Munich Re managers late in the day on which Plaintiff was terminated, are evidence that the decision-makers at Munich Re were happy to be able to terminate Plaintiff.

- In the case of *United States v. Ulbricht,* No. 14-cr-68 (KBF) (S.D.N.Y. Jan. 13, 2015), a dispute arose over messages being read aloud to the jury without the inclusion of emoticons. The judge emphasized "[t]hat is part of the evidence of the document" and that it was important for the jury to get all of the relevant details for comprehension: "The jury should note the punctuation **and emoticons**" [emphasis added].
- In February 2015, a grand jury declined to indict a teenager for making a terroristic threat on Facebook by "posting an emoji of a police officer with three guns pointing at the cop."
- In 2017, in a small-claims court in Tel Aviv, Israel, a judge found that emoji used in a text message to a prospective landlord indicated intent:

> The…text message sent by Defendant…included a smiley, a bottle of champagne, dancing figures and more. These icons convey great optimism. Although this message did not constitute a binding contract between the parties, [it] naturally led to the Plaintiff's great reliance on the Defendants' desire to rent his apartment…These symbols, which convey to the other side that everything is in order, were misleading."

- In the sexual harassment case of *Harrison v. City of Tampa*, No. 8:17-cv-01369-T-02CPT (M.D. Fla. Jun. 4, 2019), evidence included messages in which the plaintiff's supervisor "sent her a number of emojis that can be read to indicate that [he] was romantically attracted to Plaintiff," including "emojis that show a face kissing, a face with hearts for eyes, and what appears to be a smiling dog with hearts next to it."

# ABOUT THE AUTHOR

Matthew Verga is an attorney, consultant, and eDiscovery expert proficient at leveraging his legal experience, technical knowledge, and communication skills to make complex eDiscovery topics accessible to diverse audiences. A sixteen-year industry veteran, Matthew has mastered every phase of the EDRM and worked at every level, from the project trenches to enterprise program design. As Director of Education for Consilio, he leverages this background to produce engaging educational content to empower practitioners at all levels with knowledge they can use to improve their projects, their careers, and their organizations.

**Matthew Verga, Esq.**
Director of Education

**m** +1.704.582.2192
**e** matthew.verga@consilio.com

**consilio.com**

Consilio / ADVANCED LEARNING INSTITUTE

# HOW SHOULD PRODUCTIONS OF MOBILE DEVICE MESSAGES BE FORMATTED?

*by Matthew Verga,*
*Director of Education*

Mobile devices have become frequent sources of relevant ESI in litigation. According to one litigation trends survey, roughly half of all litigation matters in 2015 and 2016 involved preservation and/or collection of mobile device data. Of the mobile device sources implicated in 2016, 93% were smartphones. In its 2019 Report on Industry Trends for Law Enforcement, Cellebrite (maker of forensic tools for mobile devices) found that smartphones were far and away from the most common source of digital evidence with 91% of "Investigator" respondents indicating that smartphones were "Very Frequent" (81%) or "Frequent" (10%) sources.

As mobile device sources have rapidly increased in number and importance, practitioners have struggled to adapt to these evolving expectations and challenges. Among those challenges is the question of what format to use for the production (or request) of mobile device data.

## What Kind of Data Is Being Produced from Mobile Devices?

In *Riley v. California*, 573 U. S. 373 (2014), the Supreme Court summed up the kind of all-encompassing data source that smartphones have become: ". . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate." A single smartphone will routinely contain thousands upon thousands of unique records, including: phone-specific materials, mobile application and Internet materials, and traditional office documents. Despite this great volume and diversity, however, it has so far been **text messages** (including SMS, MMS, and OTT messages) that have been relevant most often.

## What Makes Mobile Device Message Production Complicated?

Production of mobile device messages is complicated for three main reasons:

- First, mobile device data collection is accomplished using specialized collection kits akin to those used for forensic acquisitions from computers. After collection, the acquired files must be exported from the acquisition software for incorporation into your project workflow for assessment, review, and production. Unfortunately, it is common for these tools to output all of the files as a single exported document (e.g., a long multi-page PDF or large multi-tab spreadsheet). These files are not generally conducive to convenient review or production, and if you wish to break those concatenated records out into individual files, additional work (or a specialized software solution) is needed.
- Second, a clear standard has not yet emerged for how best to format such productions, with some parties and courts insisting on native files with metadata, others pushing for near-native options that are optimized for display and review (e.g., simulating chat bubbles or other contextual elements), and others seeking near-paper productions of page images with metadata and extracted text (like those used for email productions). On a technical level, there is also more variability among review platforms and providers with regard to text and chat message handling, with some treating them the same as other types of documents and others offering dedicated viewers with emoji support and specialized features.
- Third, a clear standard has not yet emerged for how best to handle the unitization of messages and threads. Should each individual message be treated as an individual document? Should

distinct threads be treated as individual documents instead? If so, should they be complete or broken into separate records by date? Should the whole message database be treated as a single record from which irrelevant messages can be redacted? Currently, litigants are working through these questions on a case-by-case basis (with limited guidance from the courts, as we will discuss below).

## What Do the Rules Say About ESI Production Formats?

Under the Federal Rules of Civil Procedure, litigants are directed (in FRCP 26(f)(3)) to negotiate about "the form or forms in which [ESI] should be produced" as part of their overall 26(f) meet and confer process. During this process, litigants are free to negotiate whatever stipulated production formats and specifications they wish for relevant mobile device messages.

If nothing is negotiated in advance, FRCP 34(b)(1)(C) allows the litigant requesting production of ESI to "specify the form or forms in which [ESI] is to be produced." The requesting litigant is free to ask for whatever production formats and specifications they wish, though the responding litigant is also free to object and propose an alternative (FRCP 34(b)(2)(D)).

When no ESI production format has been stipulated through negotiation or specified in the request, FRCP 34(b)(2)(E)(ii) specifies that "a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." This translates to a choice between producing ESI in its native format or in some other reasonably usable form or forms, which typically means near-paper or near-native format, accompanied by a load file with relevant metadata, searchable text, etc.

Courts have emphasized the importance of maintaining **searchability and sortability** in assessing whether a given production format is "reasonably usable" under the rules. In *David A. Johnson & Alda, Inc. v. Italian Shoemakers, Inc.*, Case No. 3:17-cv-00740-FDW-DSC (W.D.N.C. Oct. 22, 2018), the plaintiffs repeatedly produced emails in PDF format rather than in native format with metadata, as required by the applicable discovery order. In its analysis, the court explained that the requirement in FRCP 34(b)(2)(E)(ii) to produce ESI "in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms" is satisfied "when the party provides **documents that are searchable and/or sortable by metadata fields**" [emphasis added].

## What Have Cases Said About Mobile Device Message Production?

In, *Laub v. Horbaczewski*, 331 F.R.D. 516 (C.D. Cal. Apr. 22, 2019), several disputes arose related to the production of relevant text messages and "iNotes" from the defendant's iPhone, and among them was a dispute over the appropriate format in which to produce such materials. The Magistrate Judge reviewed the relevant rules and committee notes and came to the same conclusion as in the case above: that **searchability is central to reasonable usability** under the rules: "Further, '[i]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, **the information should not be produced in a form that removes or significantly degrades this feature**,'" [emphasis added; citation omitted].

In reaching this conclusion, the Magistrate Judge, also reviewed prior case examples in which parties were directed to "produce any relevant text messages in native format or in another format agreed to by the moving party" and to "produce these text messages in a form that shows the sender, recipient, time, and date the messages were sent, as required by the Federal Rules of Civil Procedure." She also stated a clear preference for producing in "aggregated" formats in which the various individual messages could be seen in context with each other, preserving "the **integrity of the threads of communication** reflected in the text messages" [emphasis added].

## So, How Should You Request Mobile Device Message Production?

Based on the limited guidance available, it is clear that a litigant could propose or request the production of mobile device messages in a few different ways that

would all preserve searchability and sortability, as well as thread relationships. When choosing how you wish to proceed from among these options, there are four main considerations to bear in mind:

1. You will want to request either native files, near-native files, or near-paper image files, and regardless of which, you will want to request with them a load file containing metadata and extracted text
2. You will want to request the inclusion of attachments (e.g., images, animations, etc.) and the documentation through metadata of their relationships to specific messages
3. You will want to request your preferred handling of message unitization and thread documentation (e.g., handling each message as an individual record with a custom metadata field documenting thread groupings, producing complete threads together as single documents, producing threads divided up by days, etc.)
4. You will want to request your preferred metadata fields to ensure you have the information you need to work with the produced materials in your preferred manner; kinds of fields to consider requesting include:
   - General Information Fields: Custodian, Attachments, Time Zone, From, To, Date/Time Sent, Date/Time Received, File Name, Message Text
   - Mobile Messaging Information Fields: Application, Account, User Name, Chat Room/Channel Name, Participants, Thread Group
   - Procedural Information Fields: Hash Value, Request Number(s), Search Term(s)

## ABOUT THE AUTHOR

Matthew Verga is an attorney, consultant, and eDiscovery expert proficient at leveraging his legal experience, technical knowledge, and communication skills to make complex eDiscovery topics accessible to diverse audiences. A sixteen-year industry veteran, Matthew has mastered every phase of the EDRM and worked at every level, from the project trenches to enterprise program design. As Director of Education for Consilio, he leverages this background to produce engaging educational content to empower practitioners at all levels with knowledge they can use to improve their projects, their careers, and their organizations.

**Matthew Verga, Esq.**
Director of Education
m +1.704.582.2192
e matthew.verga@consilio.com
consilio.com

December 13, 2022

# Takeaways from Georgetown Law's AEDI Keynote

Kevin Brzozowski, Stuart Claire, Jason Froehlich

TransPerfect Legal Solutions



The Georgetown Law Advanced eDiscovery Institute (AEDI) held in Washington, D.C., always presents as an outstanding educational experience even for the most sophisticated e-discovery attorney. This year was no exception. The Honorable David G. Campbell, Senior Judge, U.S. District Court for the District of Arizona, and the Honorable Paul Grimm, District Judge, U.S. District Court for the District of Maryland, opened the conference on November 17 with a discussion on proportionality and whether we are achieving proportionality in practice. Spoiler alert, we are not.

TransPerfect Legal Solutions was again onsite as a conference sponsor. Day one sessions covered hot topics in e-discovery, defensible data disposition, collaboration tools, TAR, privacy, and how to be a better advocate over Zoom. Day two presentations covered fabricated evidence, data transfer agreements, implications for preservation, collection and control of former (work-from-home) employee data, discovery in China, data security, and e-discovery training for non-e-discovery professionals. The conference ended with a "People's Court" where nine judges argued hypotheticals pertaining to a Rule 30(b)(6) deposition request, an attorney-guided self-collection, the scope of redactions, and production without review.

## Keynote: Proportionality Amendment Revisited

Federal Rules of Civil Procedure Rule 26(b)(1) were revised in 2015 where the predominant theme of relevance was replaced with proportionality. The text now reads in part, "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…" When it is not, the burden is on the party to timely raise the issue with the court.

Judges Campbell and Grimm reported that only a small number of parties are properly arguing proportionality (5% was suggested by Judge Campbell) and, while there is no shortage of tools to ascertain the efficiency of discovery, the parties are not providing the court with sufficient information as to why a request may not be proportional. For example, this may be because counsel is not fully versed in their client's IT systems and cannot articulate the technical limitations, or there may be no limits on the number of relevant custodians.

Judge Campbell went on to encourage the parties to address these limits and include them in a Case Management Order, but neither judge would like to see motion practice rather promptly address the disagreement with a phone call.

Both judges agreed that the sources of information that should be harvested and reviewed first are those that are target-rich environments. Perhaps that is key custodian email or mobile phone data. Regardless, the judges' point was to draw limits around the timeframe, sources, and the number of custodians and to work with opposing counsel if they can justify needing more data.

The other option suggested by Judge Campbell would be to scrap the discovery system and go to a method of judge-directed investigation. Otherwise, for our system to work, Judge Campbell said we need cooperation, proportionality, active management by the bench, and a meaningful spoliation rule.

The presentation explored the six factors in Rule 26(b)(1) needed for supporting a proportionality argument: (1) the importance of the issues at stake in the action, (2) the amount in controversy, (3) the parties' relative access to relevant information, (4) the parties' resources, (5) the importance of the discovery in resolving the issues, and (6) whether the burden outweighs the likely benefit. It also explored the guidelines and best practices published by the Bolch Judicial institute at Duke Law School and the Honorable Elizabeth D. Laporte's best practices taken from A Practical Guide to Achieving Proportionally Under New Federal Rule of Civil Procedure 26.

## Practical takeaways

- An overwhelming majority of litigants are omitting a potentially winnable proportionality argument.
- Judges are asking litigators to leverage Rule 16 or a similar conference to bring these issues and supporting information to their attention.
- When objecting on proportionality grounds, an affidavit or evidentiary proof of the time and/or expense is needed.
- To secure an affidavit or evidentiary proof, litigators need to understand and know about how their clients' IT systems create, store, and retain data, and what it takes to collect, process, and review that data.

## RELATED POSTS

- **Deploying TAR and Analytics in Merger Review Proceedings**
- **Searching Audio and Video Files: Are You Adequately Assessing Their Relevancy to Your Cases?**
- **The ESI Protocol Explained**

## LATEST POSTS

- **The Duty of Competence: How to Avoid E-Discovery Sanctions**
- **Moving from a Non-Compete Mindset to Protecting Company Trade Secrets**

See more »

**WRITTEN BY:**

TransPerfect Legal Solutions

Contact + Follow

Kevin Brzozowski + Follow


Stuart Claire + Follow


Jason Froehlich + Follow

**PUBLISHED IN:**

Discovery + Follow

e-Discovery Professionals + Follow

Electronically Stored Information + Follow

Federal Rules of Civil Procedure + Follow

Information Technology + Follow

Proportionality + Follow

Technology-Assisted Review + Follow

Electronic Discovery + Follow

Professional Practice + Follow

Science, Computers & Technology + Follow

more

**TRANSPERFECT LEGAL SOLUTIONS ON:**

# A Right to Privacy for Modern Discovery

ALLYSON HAYNES STUART
Issue 3
Volume 29
29 GEO. MASON L. REV.

**Introduction**

Twenty-first century civil discovery looks very little like it did even a few decades ago. The explosion in technology and digital storage, not to mention the rise of the internet, social media, and connected devices, has transformed American culture—and with it, our discovery system.

A recent case illustrates this phenomenon. *Hinostroza v. Denny's, Inc.*[1] No. 17-CV-02561, 2018 WL 3212014 (D. Nev. June 29, 2018). was a case the court referred to colloquially as a "slip and fall."[2] The plaintiff had suffered injuries in the accident in the defendant's restaurant and brought suit. In the past, the primary requests for discovery from the plaintiff would have included medical bills, proof of lost wages, and depositions of witnesses, including the plaintiff. Here, however, in addition to those requests, the defendant sought all text messages, emails, and other written communications between the plaintiff and certain individuals from the date of the accident to the present (no matter their subject); all text messages or emails sent by the plaintiff in the two-day period after the accident (no matter their subject or recipient); all data from any type of Fitbit or other activity tracker device the plaintiff may have used from five years prior to the accident to date; and all social media account information from five years prior to the accident to date.[3] It is no wonder that some have questioned whether the state of discovery would dissuade any plaintiffs from bringing claims for their injuries,[4] not to mention when they implicate personal issues like sexual harassment.[5]

The rise in electronic discovery led to substantial changes in the Federal Rules of Civil Procedure ("the Rules") in 2006 and again in 2015, aimed at problems posed by the format of electronic discovery ("e-discovery"), the problems with cost and accessibility, the risks of waiving attorney-client privilege, and the overbreadth of discovery requests.[6] The Rules highly encourage cooperation among counsel to discuss e-discovery issues early and resolve them without motions practice.[7] The Rules also encourage judges to be hands-on in controlling the discovery process and using their discretion to limit overreach.[8] An entire e-discovery industry has arisen to handle the vast amounts of data that often must be gathered, reviewed, culled, and produced.[9]

Amid all these changes, little attention has been paid to privacy as opposed to time and expense.[10] The Rules do not provide for explicit protection against discovery based on privacy,[11] with the exception of redaction of personal information under Rule 5.2.[12] There has long been the idea that privacy protection exists against government searches and seizures, but that there is no such concept in civil discovery.[13] However, close analysis of cases reaching back to the adoption of the Rules shows that federal courts have in fact used privacy rationales to protect against discovery in many areas. District courts in particular have developed an interpretation of the Rules that protects litigants and non-litigants from discovery; courts have developed certain categories of protected information based on a balancing of the right to privacy against the need for the information in the context of the litigation.[14] This law derives from Supreme Court precedent, from public policy represented in federal and state statutes, and from discretionary judicial application of the Rules. This Article unearths this body of law from its surprising obscurity. With a firm grounding in the foundations and justifications for federal protection of privacy in discovery, and in light of recent Supreme Court doctrine, the Article describes how privacy arguments can address increasingly intrusive discovery demands.

## I. Privacy in Federal Discovery

Civil discovery in federal courts largely began with the passage of the Rules in 1938. Prior to the promulgation of the Rules, "[i]nquiry into the issues and the facts before trial was narrowly confined and was often cumbersome in method."[15] As the Supreme Court noted in *Hickman v. Taylor*,[16] the new Rules switched focus from the pleadings to the discovery phase "as a device for ascertaining the facts, or information as to the existence or whereabouts of facts, relative to those issues" so that "civil trials in the federal courts no longer need be carried on in the dark," clearing the way, "consistent with recognized privileges, for the parties to obtain the fullest possible knowledge of the issues and facts before trial."[17] But with that increase in fact-finding ability came an increase in potential for invasions of privacy. *Hickman* itself recognized a form of privacy protection in the work product doctrine, finding it necessary to afford attorneys a zone of privacy within which to prepare their cases.[18]

Protections for privacy in discovery can be divided into two broad categories. One is protection for information or communications deemed confidential,[19] while not rising to the level of privilege.[20] Work product protection itself falls within this category.[21] In addition to *Hickman*, this privacy protection can be traced to common law doctrine recognizing "secrecy" in business processes and commercial information as well as legislative provisions protecting against disclosure to the public. This right to confidentiality in discovery was affirmed by Supreme Court case law and has evolved to protect many aspects of information privacy.

The second category giving rise to privacy protection for discovery is based on Supreme Court interpretation of the constitutional right to privacy in intimate or otherwise highly personal matters, including marriage, contraception, sexual activity, medical information, family relations, and other personal information. In addition, the Constitution protects against compelled disclosure of information that would violate a person's First Amendment rights, such as freedom of association. This Part describes that historical protection, which is also reflected in various stages in changes to the Rules.

A. *Early Privacy Protection in Discovery*

1. Trade Secrets and Confidential Business Records

Even before the Rules were promulgated, early case law recognized that there should be limits on discovery of private or "secret" matters.[22] One such early case was *E. I. Du Pont de Nemours Powder Co. v. Masland*,[23] where the Supreme Court found that a company should not have to disclose "secret processes" as part of the litigation to anyone other than opposing counsel and the judge.[24] Those secrets had been communicated to the defendant "through a special confidence that he accepted," and the defendant should not "fraudulently abuse the trust reposed in him."[25] The Court upheld an injunction against the disclosure of trade secrets "to experts or witnesses produced during the taking of proofs—but excepting the defendant's counsel," it being understood "that if, in the opinion of the trial judge, it is or should become necessary to reveal the secrets to others it will rest in the judge's discretion to determine whether, to whom, and under what precautions, the revelation should be made."[26]

Later cases cited *Du Pont de Nemours* as support for the discretion of the trial court to allow limits on disclosure of discovery to others to protect a litigant, including by the use of *in camera* proceedings.[27] When courts denied motions to prohibit discovery of trade secrets, they nonetheless emphasized limits to protect privacy, and the extent to which the lower court had discretion to condition disclosure.[28] When the Rules were promulgated twenty years after *Du Pont de Nemours*, Rule 30(b) (the equivalent of modern Rule 26(c)) included the right of a court to protect against discovery of "secret processes, developments, or research."[29]

Courts extended the rationale for protection of a business's secrets to its financial records.[30] As one court put it when denying a party's motion for production of extensive financial records:

> While i[t] may be true that, in the language of the vernacular, a party involved in a lawsuit under the present Federal Rules may be required, when entering Court, to "put all his cards upon the table", this is no basis for assuming that he must also put all his clothes upon the table. A litigant is entitled to some privacy on matters not directly relevant to the lawsuit.[31]

This protection for financial information was found to be particularly strong when documents were sought from third parties. In *Hecht v. Pro-Football, Inc.*,[32] the District Court for the District of Columbia quashed subpoenas seeking profit and loss statements of a non-party, noting that the requests "seek private financial records of persons who are not parties to this action."[33] Without attribution, the court noted that "[t]he right of privacy and the right to keep confidential one's financial affairs is well recognized."[34] While the Rules contemplate "liberal disclosure," discovery is not unlimited: "There must be restrictions to protect individuals in their natural privacy."[35]

The rationale for protecting confidentiality of business information extended to the context of employee evaluations and confidential business reports, shielding from disclosure to allow for candid evaluation. In *New York Stock Exchange, Inc. v Sloan*,[36] a court gave two reasons for preventing the discovery of an accounting firm's employee evaluations. "First, revealing the contents of these evaluations, which were prepared without input by their subjects, and which are the kind of materials which the employees justifiably expect to be kept confidential, would invade the employees' privacy."[37] The second "broader purpose" was that if discovery of such documents were "generally allowed [in civil litigation], firms might cease to frankly criticize and rate their own performance, for fear that any written evaluations they make might be used against them or their employees in a lawsuit."[38]

The court analogized this protection to that afforded by courts to hospital boards' records evaluating medical procedures and performance; of income tax returns; of a broker's confidential records of client names and transactions of clients; and of internal reports analyzing a corporation's affirmative action efforts in employment.[39] In each of these cases, "the

policies in favor of confidentiality—protecting individuals' expectations of privacy and/or promoting free communication of candid evaluations and criticisms within an organization—have been deemed strong enough to justify restrictions on liberal pretrial discovery."[40] The court found that this protection could be overcome only by a showing of clear relevance and exceptional necessity.[41]

*Sloan* was followed by *Stabilus, A Division of Fichtel & Sachs Industries, Inc. v. Haynsworth, Baldwin, Johnson & Greaves, P.A.*,[42] which declined the defendant law firm's discovery request for the plaintiff's employment records, citing confidentiality and burden. Like in *Sloan*, the discovery was not relevant to the main issue of the action, and was overly broad and unduly burdensome.[43] Modern cases too follow this precedent for protection of employee performance reviews based on the likelihood that they contain sensitive and private information.[44]

2. Tax Returns

Another early area of privacy in discovery was protection for income tax returns. This protection for individual financial records was based on the policy against public disclosure represented in the Internal Revenue Code. As the District Court for the Southern District of New York noted in *Kingsley v. Delaware, Lackawanna & Western Railroad Co.*,[45] "[t]he purpose of the [Internal Revenue Code of 1954, 26 U.S.C. § 6103,] is to prevent the disclosure of confidential information to those who do not have a legitimate interest in it."[46] However, disclosure is warranted where the plaintiff put his income at issue: "once a person has made the amount of his income an issue in litigation it becomes a legitimate subject of inquiry and he can no longer claim that the information contained in his returns is confidential."[47] In contrast, the court in *Wiesenberger v. W. E. Hutton & Co.*[48] 35 F.R.D. 556 (S.D.N.Y. 1964). denied a discovery request for the plaintiff's tax returns in a case alleging Securities Act violations where the plaintiff had not put his income at issue:

> There is no privilege for income tax returns but the courts have been reluctant to order their production. People are normally opposed to the invasion of their privacy by exposure of the details contained in an income tax return. In the hands of the Government, these returns are confidential. 26 U.S.C. § 7213(a). Unless clearly required in the interests of justice, litigants ought not to be required to submit such returns as the price for bringing or defending a lawsuit.[49]

As discussed below, this recognition of protection in discovery based on legislative confidentiality has been extended to other statutes in addition to the Income Tax Code.[50]

3. 1970 Rules Amendments

All of these protections recognized by early courts were adopted in subsequent amendments to the Rules, or approved by reference in the advisory committee notes. In 1970, the Rules were amended to include for the first time several general limitations on the scope of discovery.[51]

First, in adopting Rule 26's standard for scope, the Advisory Committee noted existing case law limiting discovery that is otherwise within its purview, including restrictions on discovery of tax returns.[52]

> Rule 26(c) (transferred from 30(b)) confers broad powers on the courts to regulate or prevent discovery even though the materials sought are within the scope of 26(b), and these powers have always been freely exercised. For example, a party's income tax return is generally held not privileged, and yet courts have recognized that interests in privacy may call for a measure of extra protection. Similarly, the courts have in appropriate circumstances protected materials that are primarily of an impeaching character. These two types of materials merely illustrate the many situations, not capable of governance by precise rule, in which courts must exercise judgment. The new subsections in Rule 26(b) do not change existing law with respect to such situations.

*Id*.

Second, in explaining a change to the Rules requiring disclosure of insurance coverage as conducive to settlement, the Advisory Committee noted that the disclosure would not extend to "other facts concerning defendant's financial status," partly because it "does not involve a significant invasion of privacy."[53] This acknowledges the invasion of privacy that courts had found from general disclosures of financial information.

Third, the new Rules added language to comport with work product protection found in *Hickman*, reflecting "the trend of the cases by requiring a special showing, not merely as to materials prepared by an attorney, but also as to materials prepared in anticipation of litigation or preparation for trial by or for a party or any representative acting on his behalf."[54]

Finally, the Rules were revised to add a specific reference for protection of trade secrets "and other confidential commercial information," again reflecting construction of protective orders by case law.[55]

> The new reference to trade secrets and other confidential commercial information reflects existing law. The courts have not given trade secrets automatic and complete immunity against disclosure, but have in each case weighed their claim to privacy against the need for disclosure. Frequently, they have been afforded a limited protection.[56]

Thus, rules revisions codified or approved of the protection shown by the courts for confidential commercial information based on case law and public policy represented by legislative disclosure limitations.

B. *Constitutional Privacy*

Next, the series of Supreme Court cases recognizing a constitutional right to privacy led to lower courts' protection for discovery requests that implicate that right.

1. Freedom from Compelled Disclosure of Association: *NAACP v. Alabama* and *Seattle Times v. Rhinehart*

The first Supreme Court case to find a constitutional dimension to the protection of privacy in discovery was *NAACP v. Alabama*.[57] There, the Supreme Court found a constitutional right to privacy which allowed the National Association for the Advancement of Colored People ("NAACP") to refuse to disclose membership lists.[58] Alabama sought an injunction against the NAACP to prevent it from doing further business in the state, and sought an order requiring the group to produce its membership lists.[59] The state supreme court upheld sanctions against the NAACP for refusing to comply with that order.[60] In reversing those sanctions, the U.S. Supreme Court found that the Due Process Clause protects a litigant from compelled disclosure of membership in an organization pursuant to a state court discovery order:

> It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the "liberty" assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech. . . . Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[61]

Therefore, the Court held that the NAACP was not required to comply with a discovery order where that order would conflict with its members' rights "to pursue their lawful private interests privately and to associate freely with others in so doing."[62]

*In Seattle Times Co. v. Rhinehart*,[63] the Court considered whether a newspaper had a right to disseminate lists of a religious group's donors and members that had been compelled in discovery in a defamation case against the newspaper.[64] The trial court ordered the group to identify the donors, and issued a protective order that prohibited public dissemination of the information.[65] The Supreme Court affirmed the protective order against public disclosure, noting the breadth of discovery often allowed in civil court and the necessity for protection against further dissemination:

> 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. The Rules do not distinguish between public and private information. . . .
>
> There is an opportunity, therefore, for litigants to obtain—incidentally or purposefully—information that not only is irrelevant but if publicly released could be damaging to reputation and privacy.[66]

Where sensitive information is disclosed in discovery, public dissemination may be limited in the court's discretion.

Courts have followed these decisions in protecting from disclosure information protected by the First Amendment like the names of a day laborers' organization.[67] In addition, courts have cited *Seattle Times* as authority for limitations on discovery pursuant to Rule 26(c) based on privacy concerns, whether or not they have a constitutional basis.[68]

2. Privacy of Intimate Matters: *Griswold v. Connecticut*, *Whalen v. Roe*, and *Roe v. Wade*

A series of Supreme Court cases recognizing a constitutional right to privacy in certain intimate relationships and personal decisions led courts to deny compelled disclosure related to litigants' personal lives. First, in *Griswold v. Connecticut*,[69] the Court struck down a law prohibiting married couples from using contraception, and first recognized the Constitution's "zones of privacy," which include the right of association, the right to be free from unreasonable searches and seizures, among others:

> The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. And it concerns a law which, in forbidding the *use* of contraceptives rather than regulating their manufacture or sale, seeks to achieve its goals by means having a maximum destructive impact upon that relationship. [70]

Later cases helped clarify what was included in that "zone of privacy." In considering whether a New York Act violated constitutionally protected privacy between doctor and patient, the Court in *Whalen v. Roe* [71] 429 U.S. 589 (1977). recognized that the individuals whose information was required to be shared by their doctors had two interests that implicated privacy. [72] They included both "the individual interest in avoiding disclosure of personal matters, and . . . the interest in independence in making certain kinds of important decisions." [73] With respect to the former, the Court noted that the Act implicated "the right of an individual not to have his private affairs made public by the government" and "the right of an individual to be free in action, thought, experience, and belief from governmental compulsion." [74] As to the second interest, the Court quoted Justice Brandeis's famous dissent in *Olmstead v. United States*, [75] characterizing "'the right to be let alone' as 'the right most valued by civilized men,'" and quoted the finding in *Griswold* that "the First Amendment has a penumbra where privacy is protected from governmental intrusion." [76]

In *Roe v. Wade*, [77] the Court summarized its previous decisions determining that, while the Constitution does not explicitly mention any right of privacy, such a right does exist and applies to "personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty,'" and "has some extension to activities relating to marriage; procreation; contraception; family relationships; and child rearing and education." [78] "This right of privacy, [based] in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action . . . is broad enough to encompass a woman's decision whether or not to terminate her pregnancy." [79]

Courts have cited to *Whalen* in refusing to allow discovery. In *Mann v. University of Cincinnati*, [80] the university improperly issued subpoenas for the plaintiff's medical records in a sexual harassment suit. [81] The court found that the plaintiff had a constitutionally protected interest in her medical records, and after an *in camera* review, found that the highly personal records were not entitled to discovery:

> There can be no question that the aforementioned information is of such a private nature that a constitutional right to privacy exists. In a civilized society in the year 1993, where vast amounts of personal information are contained not only in medical files but in computerized data banks or other massive government files, much of which is personal in character and potentially embarrassing or harmful if disclosed, the constitutional right to privacy is surely as significant as the protection of commercial information specifically recognized by Rule 45(c)(3)(B)(i). [82]

Courts also rely upon this case law to delineate rough boundaries for the type of privacy interest that is protected from disclosure. In addition to privacy rights against discovery of medical records, [83] courts have protected the identity of parties involved in claims about contraception rights; [84] personal information concerning medical, sexual, and contraceptive histories and practices; [85] the identity of participants in medical studies; [86] the identity of blood donors in cases alleging disease from transfusions; [87] personal letters between a father and child; [88] diagnostic and mental evaluation files of children; [89] records of employee drug use; [90] and a party's sexual history. [91]

3. Freedom from Compelled Disclosure of Personal Matters: *Whalen v. Roe*, *Nixon*, and *Reps. Comm*.

While *Whalen* concerned disclosure of information regarding drug prescriptions, which arguably is included in the intimate matters protected generally in the cases above, *Whalen* also indicated that the right to avoid disclosure of personal information went beyond those intimate spaces:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. *Recognizing that in some circumstances that duty arguably has its roots in the Constitution*, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. [92]

This passage suggests that the Constitution protects not only information concerning intimate relationships and decisions, but also personal and potentially embarrassing information relating to finances, government benefits, military service, and criminal activity.

In *United States Department of Justice v. Reporters Committee for Freedom of Press*,[93] the Court confirmed that *Whalen*'s recognition of a constitutional privacy interest included "keeping personal facts away from the public eye," and that protected facts went beyond the zone of intimacy.[94] Just as *Whalen* recognized that a centralized computer file of names and addresses of people obtaining prescription drugs "posed a 'threat to privacy,'" so too did the publication of a person's rap sheet information.[95] This "substantial" privacy interest was implicated by the Constitution in addition to the Freedom of Information Act's ("FOIA") privacy exemption.[96]

In addition, the Supreme Court's decision in *Nixon v. Administrator of General Services*[97] 433 U.S. 425 (1977). affirmed a constitutional right to privacy in personal communications. There, the former president challenged a law requiring that he turn over documents and tape recordings accumulated during his terms of office.[98] While affirming the constitutionality of the law, the Court nevertheless recognized that "a very small fraction" of Nixon's papers were in fact private and deserved protection.[99] Those included "extremely private communications between him and, among others, his wife, his daughters, his physician, lawyer, and clergyman, and his close friends."[100]

Subsequent courts have read these cases as authority for privacy against disclosure of personal matters that are not strictly "intimate."[101] In *Tavoulareas v. Washington Post Co.*,[102] the Court of Appeals for the District of Columbia reviewed a lower court order unsealing a number of discovery documents in a libel action.[103] The court reviewed decisions from the Fifth Circuit finding a right to financial privacy,[104] and from the Third Circuit finding a right to privacy in medical records.[105] The court then found that the plaintiff had a constitutionally protected privacy interest in avoiding public disclosure of the discovery material:

> The significance in this context of the Supreme Court's decisions in *Whalen* and *Nixon v. A.G.S.*, and of the Third and Fifth Circuits' respective decisions in *Westinghouse* and *Plante*, lies in their explicit recognition of the constitutional right to avoid disclosure of personal matters. In the discovery process, individuals are often forced by the court to disclose the kind of personal information deserving privacy protection under these decisions. An individual's constitutional privacy interest can thus be implicated by the discovery process to the same extent it is implicated by disclosure requirements of statutes. In both instances, the government is forcing disclosure of personal information.[106]

That right to privacy in the discovery process outweighed any First Amendment right the newspaper may have to publicize the information.

C. *Public Policy of Privacy in Discovery*

1. Statutory Publication Shelters

Protection for privacy has evolved as the legislature has instituted new privacy laws, including what many courts refer to as "statutory publication shelters."[107] These ordinarily apply where legislation requires the production of information to the government or to the public, but places limitation on further disclosure or carves out exceptions to public disclosure.[108] Courts deem such legislative determinations of confidentiality to be worthy of privacy protection against discovery.[109] It is possible for such statutes to create privileges.[110] More commonly, they instead give rise to protection to be balanced against the need for the discovery. As the Court of Appeals for the District of Columbia put it:

> *[S]tatutory publication shelters may have some application to discovery. These protected interests reflect a congressional judgment that certain delineated categories of documents may contain sensitive data which warrants a more considered and cautious treatment. In the context of discovery of government documents in the course of civil litigation, the courts must accord the proper weight to the policies underlying these statutory protections, and to compare them with the factors supporting discovery in a particular lawsuit.*[111] *Friedman*, 738 F.2d at 1344.

One such statutory publication shelter is represented by the exceptions to required disclosure under FOIA. The statute shines light onto government operations by requiring agencies to provide documents on request, with some important exemptions. An agency need not provide "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," or "records or information compiled for law enforcement purposes, but only to the extent that the production of such [materials] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[112] FOIA exemptions have been persuasive to courts considering privacy arguments against discovery. As the District of Columbia Court of Appeals found in *Friedman v. Bache Halsey Stuart Shields, Inc.*,[113] in the context of subpoenas directed to the Securities and Exchange Commission and the Commodity Futures Trading Commission for investigatory files, exemption from disclosure under FOIA does not automatically mean that "the information is privileged within the meaning of rule 26(b)(1) and thus not discoverable in civil litigation."[114] Instead, the district court may consider such FOIA exceptions "as congressional underscoring of the government's interest in protecting sensitive investigatory information."[115]

Courts also find a public policy of protection from discovery represented by the Privacy Act,[116] which protects against disclosure information prepared for government agencies.[117] In *Laxalt v. McClatchy*,[118] the Court of Appeals for the District of Columbia Circuit addressed the discovery of Federal Bureau of Investigation ("FBI") files. Defendants sought the records to help prove the truth of allegedly libelous statements they had printed suggesting that the plaintiff's associates had ties to organized crime.[119] The court rejected the argument that the Privacy Act created a privilege against discovery, but found that because records are subject to the Act, the district court's use of its discretion under Rule 26(c) "may in many cases be weightier than in the usual discovery context."[120] Specifically, "when the District Court considers a request for a Privacy Act order in the discovery context it must consider the use of protective orders and the possibility of *in camera* inspection," and should also consider notifying any affected nonparties.[121]

Finally, courts have protected disclosure of medical records based both on Supreme Court precedent for protection of medical privacy[122] but also based on the Health Insurance Privacy Authorization Act ("HIPAA"). In *St. John v. Napolitano*,[123] an action alleging employment discrimination on the basis of national origin and age and retaliation, the defendant Department of Homeland Security sought the production of the plaintiff employee's medical records for a nine-year period.[124] The court required disclosure of only a portion of those records having a logical connection to the employee's claims of injury:

> [M]edical records are likely to contain sensitive personal information, a fact underscored by the existence of statutory confidentiality provisions, like those of the HIPAA Privacy Rule. Accordingly, the plaintiff has demonstrated that the burden of producing such records and the harm to the plaintiff's privacy interests from the disclosure significantly outweighs any marginal relevance for the majority of the time period for which the defendant seeks records.[125]

Other relevant federal statutes that protect against disclosure include the Children's Online Privacy Protection Act;[126] the Fair Credit Reporting Act;[127] the Family Education Rights and Privacy Act;[128] the Gramm-Leach-Bliley Act;[129] the Cable Communications Policy Act;[130] the Video Privacy Protection Act;[131] the Employee Polygraph Protection Act;[132] the Stored Communications Act;[133] the Genetic Information Nondiscrimination Act;[134] and the Right to Financial Privacy Act.[135] Statutory publication shelters do not ordinarily create privileges against discovery production, but they are strong evidence of congressional intent to protect certain personal or otherwise confidential information.[136] Courts therefore require a stronger showing for the production of such information.[137]

2. Persuasive State Law

When a federal court sits in diversity, it applies federal procedural law but otherwise applies the law of the state, including the state's privilege law.[138] Protection of privacy in discovery is treated as a subset of privilege law; therefore, when a federal court sits in diversity, it applies the privacy law of the state where it sits.[139] In contrast, where federal and state claims are joined, all privacy objections are governed by federal law.[140] Even when federal law applies, however, courts often take into consideration state laws and policies protecting privacy interests.[141] For example, in *In re Sealed Case* (*Medical Records*),[142] the District of Columbia Court of Appeals reviewed a decision ordering production of files of a mentally disabled man in the possession of the city's agency for disabilities.[143] In addition to finding that some of the records were protected by the psychotherapist-patient privilege, the court found that non-privileged records also presented an intrusion into the man's legitimate privacy interests.[144] The court found persuasive a decision from the Seventh Circuit that relied on a state evidentiary privilege in protecting against the disclosure of medical records: "Particularly relevant here, the Seventh Circuit held that '[t]he fact that quashing the subpoena comports with Illinois' medical-records privilege' was a 'factor in favor of the district court's action.'"[145] The Third Circuit too had found that, while inapplicable to a federal claim, a state mental health records privilege was persuasive in the application of limits on discovery under Rule 26(c).[146] Therefore, on remand, the district court was ordered to weigh the need for the records against the substantial privacy interests that were implicated.[147]

Many states have a robust history of privacy protection in discovery. First, there are more appellate decisions in state courts regarding discovery disputes where litigants are permitted interlocutory appeals from adverse decisions.[148] Second, many states have rights to privacy pursuant to their state constitutions and apply that law to limit disclosure of personal information.[149]

For example, California's constitution provides that one of its people's inalienable rights is "pursuing and obtaining . . . privacy."[150] Pursuant to that provision, California protects against disclosure of, among other things, sexual information;[151] tenure files and related discussions;[152] and non-party contact information.[153] In *Valley Bank of Nevada v. Superior Court*,[154] the Supreme Court of California considered whether a litigant could obtain discovery of confidential customer bank information. The court found that such information was discoverable in a proper case, but that the bank must first take measures to locate the customer and give him an opportunity to challenge the discovery.[155] The

court construed its constitution to protect "one's confidential financial affairs as well as . . . the details of one's personal life."[156] Because the state's rules of civil procedure providing for protective orders offered inadequate protection against disclosure of third party bank records implicating that right to privacy, the court instituted the additional notice requirement.[157]

Florida's constitution protects every person's "right to be let alone and free from governmental intrusion into the person's private life."[158] The Florida Supreme Court has noted, in the context of discovery, that "[a]lthough the general concept of privacy encompasses an enormously broad and diverse field of personal action and belief, there can be no doubt that the Florida amendment was intended to protect the right to determine whether or not sensitive information about oneself will be disclosed to others."[159] Litigants have successfully argued for the privacy of blood donors' identities,[160] financial records of taxpayers,[161] employee records,[162] and other confidential materials like ethics committee records.[163]

Colorado state courts restrict discovery on the basis of the federal constitution and have protected personnel files, computers, sexual history, tax returns, and financial records.[164] Texas courts recognize privacy rights in discovery based on the federal and state constitutions, which protects medical records and personal records.[165] Washington,[166] Alaska,[167] and Montana[168] also protect privacy based on their state constitutions.

3. Balancing the Privacy and Litigation Interests

a. *Clear Relevancy Rather Than Mere Impeachment*

Federal courts have developed balancing tests under Rule 26(c) in deciding whether to order discovery when requests implicate privacy interests described above.[169] Where discovery does implicate privacy, it will only be granted where there is compelling need and inability to obtain the discovery elsewhere.[170] To overcome privacy interests, some courts require that the discovery be "clearly" relevant,[171] or that it go to the "heart of the case."[172]

On the other hand, courts often deny discovery where the requested information merely goes to impeachment.[173] The 1970 advisory committee note to Rule 26, referring to "broad powers o[f] the courts to regulate or prevent discovery," noted that "the courts have in appropriate circumstances protected materials that are primarily of an impeaching character."[174] In early cases, the party in possession of impeaching materials sometimes argued that they did not need to disclose those materials to the other party.[175] More commonly, parties have been successful in opposing discovery when the requesting party is seeking it for purposes of impeachment.[176]

In one case arising out of questionable practices of a religious non-profit corporation, a defendant sought numerous documents from the plaintiff regarding examination of candidates for priesthood and correspondence with the local Archdiocese.[177] The court noted that the information "is obviously intended for use in impeaching the credibility of the plaintiff," and discussed case law regarding such discovery.[178] While previous decisions questioned whether impeachment material was relevant to the action under Rule 26(b)(1),[179] the court found that it was a proper subject for discovery, albeit subject to protection as going to collateral matters.[180]

Another court noted that when a party seeks discovery of employee performance reviews, the party's purpose made a difference in the determination of whether to order disclosure of such "sensitive and private information."[181] In the context of an Employee Retirement Income Security Act disability benefits case, where performance reviews are sought "as evidence of employee credibility, training or qualifications," courts are less likely to allow discovery than if there is an allegation of historical bias.[182]

b. *Evidentiary Influences*

In balancing privacy against the need for discovery, courts have also been persuaded by policy represented in the Federal Rules of Evidence ("FRE"). In *Cook v. Yellow Freight System, Inc.*,[183] the court denied a request for the production of confidential settlement negotiations, in part based on the policy underlying FRE 408 that makes inadmissible evidence regarding offers of compromise in order to show liability.[184] While FRE 408 is addressed to admissibility at trial rather than discoverability, the court found the same considerations applicable, including the public policy in favor of promoting voluntary resolution of disputes by respecting confidentiality of such discussions.[185]

In *Bottomly v. Leucadia National*,[186] the court denied discovery from a sexual harassment plaintiff where the request went to the plaintiff's character under FRE 404[187] and would violate the prohibition on admission of evidence of victims' sexual history under FRE 412.[188] The court found that the Rules of Evidence "are directly pertinent as to what matter is calculated to lead to admissible evidence," and that, under FRE 404, "matter that is not related to causation and extent of

damage, but which merely goes to plaintiff's character is outside of proper bounds of discovery."[189] Other courts have also limited discovery requests that would violate the restriction on use of evidence of other sexual relations embodied in FRE 412.[190]

c. *Third Party Protection*

Finally, many courts provide special protection when discovery requests implicate the privacy of third parties.[191] The Supreme Court in *Seattle Times* noted the need for protecting against discovery abuse that could harm privacy interests of third parties.[192] So even when a plaintiff's rights in her sexual history are outweighed by the defendant's right to discovery, the court may limit that discovery to protect the identity of third party sexual partners.[193] Third party financial records are given greater protection,[194] as are files concerning non-party students.[195] Courts also protect the identity of non-parties from counsel seeking class members.[196]

d. *Protective Measures*

Courts have broad discretion under Rule 26(c) in making determinations regarding discovery that implicates privacy.[197] Courts may find that discovery should be denied completely.[198] Alternatively, courts may also fashion protective orders,[199] order redactions of personally identifiable or private information,[200] order a phased discovery process,[201] or view potential discovery *in camera* before allowing disclosure.[202] The flexibility of these measures lends itself to the ever-evolving technology that has changed the face of discovery.

## II. Privacy in Modern Discovery

This Part traces the principles of privacy just discussed into the current era of discovery. Section A focuses on changes to discovery across the 2006 and 2015 Amendments to the Rules and how they apply to cell phones, social media, fitness tackers, and other internet-based technologies. Section B explains the Fourth Amendment case law surrounding the constitutional right to privacy over one's digital life, which has shaped how courts address similar privacy questions in discovery proceedings. Section C applies these principles more precisely to modern discovery requests. Ultimately, courts should be more protective of requested material when those requests concern personal, intimate matters, require a higher showing of relevance for that information, and apply the mosaic theory of privacy to limit requests of broad, aggregate sets of data.

### A. *Discovery Today*

1. E-Discovery and Proportionality

Discovery in both federal and state courts faced a sea change[203] with the advent of electronically stored information ("ESI").[204] The focus of civil discovery first changed with the proliferation of email in the 1990s.[205] In the *Zubulake* line of cases, Judge Scheindlin in the Southern District of New York addressed this issue in a systemized manner, delineating the obligations of counsel and litigants as to preservation and issuance of a litigation hold;[206] readily accessible ESI and form of production;[207] spoliation of ESI;[208] and sanctions for abuse.[209] In the meantime, the Sedona Conference was bringing together judges, scholars and practitioners to best address the wave of ESI.[210] This, along with five years of study by the Civil Rules Advisory Committee ("Advisory Committee"), led to changes in the Rules in 2006 that "recognize some fundamental differences between paper-based document discovery and the discovery of [ESI, and] continue a trend . . . since the 1980's of expanding the role of judges in actively managing discovery to sharpen its focus, relieve its burdens, and reduce costs on litigants and the judicial system."[211]

After those changes, complaints about ESI persisted, leading the Advisory Committee to convene a conference in 2010 ("the Duke Conference").[212] A subcommittee from that event summarized the complaints:

> *[S]erious, even grave problems persist in enough cases to generate compelling calls for further attempts to control excessive discovery. The geometric growth in potentially discoverable information generated by electronic storage adds still more imperative concerns.*[213] Advisory Committee on Civil Rules, *Report to the Standing Committee*, *in* Committee on Rules of Practice and Procedure 226 (2013), https://perma.cc/UVY8-HEK3.

The Duke Conference, including judges, lawyers and academics, came to the conclusion that the system should be improved in four areas: "increased cooperation among litigants during the pretrial process; greater proportionality in discovery; earlier and more active management of cases by judges; and improved guidance on the preservation and loss of [ESI]."[214] This resulted in Rules amendments in 2015 to address these four areas.

Proportionality has been a part of the Rules since 1983, when Rule 26(b) first required that courts consider whether "the discovery sought [was] unreasonably cumulative or duplicative" and whether "the discovery [was] unduly burdensome or expensive, taking into account the needs of the case, the amount in controversy, limitations on the parties' resources, and the importance of the issues at stake in the litigation."[215] In 1993, two additional proportionality factors were added, regarding burden or expense and importance of the proposed discovery.[216] But that same amendment divided the proportionality factors into a separate section of Rule 26(b), lending the impression that they were separate limitations on discovery, to be considered apart from the primary rule governing scope.[217] This was remedied in 2015, when the Rules were again revised to put proportionality back in prominence as an element of scope under 26(b). The current version of the Rule provides for three threshold elements of scope:

> Parties may obtain discovery regarding any [(1)] *nonprivileged* matter that is [(2)] *relevant* to any party's claim or defense and [(3)] *proportional* to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.[218]

While the Rules revisions generally addressed the tremendous rise in ESI volume and costs with emphasis on judicial intervention, cooperation, and reduction in scope, they did not give specific attention to issues of privacy.[219] However, as discovery's intrusiveness has pervaded not just vast storage databases and email but chronicles of individuals' personal lives, privacy has received more attention. Commentators have advocated for privacy to be a factor in the proportionality equation,[220] and courts have followed suit.[221] Privacy has also featured prominently in recent Fourth Amendment case law, which has in turn influenced discovery decisions.

2. Modern Subjects of Discovery

As in the slip and fall case discussed in the Introduction, modern 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. This Section discusses current case law involving privacy of some common types of modern discovery.

a. *Cell Phones*

As the Supreme Court has recognized, cell phones are ubiquitous.[222] Courts find a strong privacy interest in the content of those devices, particular when a party seeks a forensic examination of the phone.[223] Like inspection of litigants' hard drives and other computer systems,[224] inspection of cell phones implicates privacy rights, privileged communications, and non-relevant information.[225] Courts are therefore reluctant to order litigants to submit their cell phones to their opponent for purposes of forensic examination absent necessity for purposes of finding highly relevant evidence, or proof of spoliation.[226] Courts also find a strong privacy interest in cell phone records.[227] Courts have been strongly persuaded by recent Supreme Court Fourth Amendment doctrine in finding privacy rights in this data.[228]

b. *Social Media*

Social media use has grown from 5% of American adult users in 2005 to 72% in 2021.[229] The nature of social media, including the candid quality of comments and photographs, make it catnip for all sorts of litigants,[230] particularly defendants seeking to impeach the credibility of injured plaintiffs.[231]

Courts apply traditional discovery rules to the social media context, while noting the challenge of a medium both public and private.[232] 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."[233] For that reason, courts have granted tailored requests for relevant social media content, but deny requests for a litigant's entire social media over a period of time.[234] Many courts have required a "threshold showing" that social media content available to the public is inconsistent with a litigant's claims of injury or otherwise before allowing broader discovery into non-public content.[235] Courts also limit such discovery to the extent it pertains to highly personal and intrusive matters like sexual content.[236] They also exclude from discovery certain categories of personal information included in social media profiles, like "Religious Views."[237]

In one case, *Coates v. Mystic Blue Cruises, Inc.*,[238] the plaintiff in a sexual harassment suit objected to producing Facebook messages that revealed intimate conversations between her and other employees.[239] The District Court for the Northern District of Illinois found the point well-taken, as the advisory committee notes state that "[c]ourts should presumptively issue protective orders barring discovery unless the party seeking discovery makes a showing that the

evidence sought to be discovered would be relevant under the facts and theories of the particular case, and cannot be obtained except through discovery."[240] The court noted that the evidence could only have a slight bearing on the events at issue and allowed only limited discovery at that time.[241]

c. *Fitbits and Other Smart Trackers*

Third, the rise in the use of personal activity devices[242] has created a new category of discovery.[243] Information from such devices is now a regular part of form interrogatories and document requests.[244] Like social media, such trackers may contain evidence that is helpful in impeaching the credibility of plaintiffs claiming to be limited in movement.[245] Information from such devices has assisted law enforcement in criminal investigations.[246]

In the few reported cases that have considered requests for smart tracker information, courts have attempted to balance requests for relevant evidence against overbroad fishing expeditions. In *Bartis v. Biomet, Inc.*,[247] a case out of the Eastern District of Missouri, plaintiff Hollins was one of many who sued a manufacturer of artificial hips, alleging substantial injuries from implantation of the device, including pain and lack of mobility.[248] After Hollins admitted in discovery that he consistently wears a Fitbit which tracks his steps, defendants requested production of all data from the Fitbit and any other wearable device.[249] Noting the "surprisingly little precedent on this issue given the ubiquitous presence of wearable devices,"[250] the court considered the relevance of the data regarding Hollins' activity levels compared to the "extremely low burden of production."[251] Also relevant was the fact that Hollins had been inconsistent as to whether he had difficulty walking.[252] In all, "[c]onsidering the liberal discovery rules, minimal burden of production, and limited privacy risks,"[253] the court found in favor of production of a portion of the Fitbit data:

> A plaintiff's wearing of an activity tracker like a Fitbit does not warrant a fishing expedition into the data from such device. But in this case, the extent of Hollins' physical activity is relevant to his claims of long-term physical injury. Hollins broadly alleges that he suffers long-term pain and lack of physical mobility due to the allegedly defective hip implant. Hollins' supposed ability to walk or jog short distances without discomfort does not render the Fitbit data completely irrelevant, as the data could reveal that Hollins is walking or jogging substantial distances.[254]

In contrast, a New York state court denied a request for Fitbit data from a plaintiff who claimed injuries arising out of a motor vehicle accident resulting in impairment of quality of life and ability to enjoy leisure activities.[255] The defendant sought all data pertaining to the plaintiff's Fitbit device, in addition to all photographs the plaintiff had posted to social media since the accident. While authorizing some of the discovery, the court denied the request for plaintiff's Fitbit records, as defendant "failed to meet the threshold standard that such disclosure was reasonably calculated to yield information material and necessary to her defense."[256] While defendant justified the request based on deposition testimony from the plaintiff that he had lost weight since the accident, plaintiff had also testified that he very rarely checked his Fitbit: "As diet, not just exercise, is a more important component of weight loss, this argument had little 'weight.' On this record, it appeared to the court that this request was merely an overly broad 'fishing expedition,' not based upon any supportable evidence."[257]

d. *Other Discovery from the Internet of Things*

Wearables like Fitbit are only one category of the immense market known as the Internet of Things ("IoT").[258] Researchers expect the number of IoT devices in 2021 to reach 46 billion, a 200% increase compared to 2016.[259] The total number of IoT connections will reach 83 billion by 2024.[260] Experts predict that by 2025 we will have an "Internet of Medical Things" with sensors and devices for patient health monitoring and a "flying Internet of Things" with drones in wide use for surveillance, exploration and delivery tasks.[261]

Law enforcement have used data from the wider IoT to help with their investigations. They have sought data from smart speakers to recreate a crime scene,[262] and have used alarm systems[263] and pacemakers[264] to confirm the veracity of a suspect's story.[265] 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 and have added to draft interrogatories questions about the existence of such devices.[266]

All of these subjects of modern discovery push the boundaries of privacy. Technology enables the gathering and storage of vast amounts of information that create digital chronicles of individuals' personal lives. This phenomenon has been the focus of recent Supreme Court decisions in the Fourth Amendment context.

B. *Supreme Court Case Law on Privacy and Technology*

Under the discovery rules, there is no concept of "reasonable expectation of privacy."[267] A diary entry is perfectly discoverable if it is relevant.[268] A statement shouted from a rooftop is *not* discoverable if irrelevant. Instead, the rules speak in terms of privilege.[269] Federal courts recognize that privacy interests are implicated in the discovery rules and that courts should protect privacy interests as part of their issuance of protective orders,[270] but do not treat discovery as constrained by the Fourth Amendment. However, concepts of privacy have inevitably overlapped. Many courts refer to "expectations of privacy" in the context of civil discovery.[271]

In addition, recent Supreme Court cases construing the Fourth Amendment in the context of Global Positioning System ("GPS") trackers and cell phone search and surveillance have influenced courts' view of civil discovery as to those devices.[272] These decisions have two broad implications for civil discovery. First, discovery as to devices with GPS technology and vast amounts of information, like cell phones, is fundamentally different from other kinds of discovery. Second, the view of privacy as vitiated by any third-party communication is outdated in today's technology world.

In *United States v. Jones*,[273] the Supreme Court found that the attachment of a GPS tracking device to an individual's vehicle constituted a search within the meaning of the Fourth Amendment.[274] Justice Scalia's opinion for the majority declined to decide whether the subsequent use of the GPS device to monitor the vehicle's movements on public streets would alone have violated the Fourth Amendment in the absence of the physical trespass.[275] In her concurrence, Justice Sotomayor made clear that she believed such surveillance to implicate Fourth Amendment concerns given its pervasive nature:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . .
>
> . . . .
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[276]

In addition, Justice Sotomayor expressed the view that previous Supreme Court precedent finding an individual has no reasonable expectation of privacy in information voluntarily conveyed to third parties, like bank records, is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[277] She analogized to the intrusiveness of data concerning the web sites searched by an individual or purchases made online, and stated that "all information voluntarily disclosed to some member of the public for a limited purpose" should not, for that reason alone, be devoid of Fourth Amendment protection.[278]

Two years later, in *Riley v. California*,[279] the Court found that officers' warrantless search of digital information on a suspect's cell phone incident to an arrest was unreasonable under the Fourth Amendment.[280] In distinguishing the search of a cell phone from a pat-down search for weapons or other personal property necessary to preserve as evidence, Chief Justice Roberts noted how different the cell phone is from any technology that was part of its previous Fourth Amendment jurisprudence, and adopted Justice Sotomayor's reasoning in her *Jones* concurrence.[281]

The Court noted that cell phones "are in fact minicomputers that also happen to have the capacity to be used as a telephone," and also function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[282] The quantity of data capable of being stored on such devices is "immense," with the average 16-gigabyte phone able to hold "millions of pages of text, thousands of pictures, or hundreds of videos."[283] The implications of this storage capacity are profound:

> 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.[284]

In addition to the quantity a cell phone is capable of storing, the quality of data that many users' phones contain implicates all sorts of privacy interests. This includes the concerns about GPS technology, internet search, and browsing history that Justice Sotomayor noted in *Jones*. There is also a wealth of applications ("apps") on a cell phone which "offer a range of tools for managing detailed information about all aspects of a person's life:"

> There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. [285]

In sum, the degree to which a search of a cell phone implicates its owner's privacy interests is out of all proportion to that implicated by the search of a physical object, [286] since cell phones "place vast quantities of personal information literally in the hands of individuals." [287]

Most recently, in *Carpenter v. United States*, [288] the Court considered whether the Government's actions in accessing historical cell phone records was merely gathering of data in which the suspects had no reasonable expectation of privacy, or instead constituted a search under the Fourth Amendment. In finding the actions constituted a search, the Court was strongly influenced by the fact that this was not ordinary surveillance of a suspect's movements, or gathering of traditional records provided to a third party, but instead a "comprehensive chronicle of the user's past movements." [289] The nature of the information produced by cell-site location technology is "a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." [290] Indeed, the information here raised even greater privacy concerns than the GPS monitoring in *Jones* because of the reality of cell phone usage. [291] Individuals "compulsively carry cell phones with them all the time," beyond just public places, "into private residences, doctor's offices, political headquarters, and other potentially revealing locales." [292]

Second, the Court addressed concerns about the third-party doctrine that were raised in *Jones*. [293] It found that the waiver of privacy protection dictated by *Smith* [294] Smith v. Maryland, 442 U.S. 735 (1979). and *Miller* [295] United States v. Miller, 425 U.S. 435 (1976). was not simply a question of whether information was "knowingly shared" with another. [296] Also important is "the nature of particular documents sought" and the capabilities of the information contained therein. [297] Applying the third-party doctrine here would constitute an extension of that doctrine "to a distinct category of information" that goes beyond the "limited capabilities" of bank checks or telephone call logs:

> [T]his case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*. [298]

Thus, *Carpenter* finds that the intrusive, comprehensive nature of the information contained in records generated by new technology requires a new way of approaching the Fourth Amendment. Government seizure of ordinary paper records is simply not analogous.

Commentators have described this way of viewing privacy as the "mosaic theory," since individual bits of information that may themselves not implicate privacy in the aggregate add up to a comprehensive chronicle of a person's life. [299] In 1989, the Supreme Court recognized that a compilation of information that was publicly available could nonetheless be considered private in the context of a FOIA exemption. In *Reporters Committee*, the Supreme Court considered whether the exemption for law enforcement records which could constitute an invasion of personal privacy could extend to a person's "rap sheet" held by the FBI. [300] In finding that it could, the Court rejected the argument that the events summarized in a rap sheet have been previously disclosed to the public, and therefore have no privacy attributes:

> According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public." Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole. The very fact that federal funds have been spent to prepare, index, and maintain these criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be "freely available" either to the officials who have access to the underlying files or to the general public. Indeed, if the summaries were "freely available," there would be no reason to invoke the FOIA to obtain access to the information they contain. [301]

There are implications of this theory too in the civil discovery context. In addition to discovery of cell phone information, where courts have already applied recent Supreme Court doctrine in protecting against broad examination, [302] other types of discovery should be viewed through this lens, including social media, health tracker data, and other information from devices connected to the IoT.

C. *A Modern Framework for Privacy Protection in Discovery*

The historical analysis discussed above offers some important insights for current arguments about privacy in discovery. First, privacy 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. Second, when such privacy rights are implicated, courts should require a higher showing of relevance as opposed to discovery that is solely for purposes of impeachment or is otherwise "collateral." Courts should apply higher limits still when private information is sought from or implicates the rights of third parties. And third, even where information sought does not fall within traditional notions of confidentiality or constitutional zones of intimacy, the totality of what is comprised within broad sets of data may implicate privacy pursuant to the mosaic theory. All three of these bases for restriction are proper subjects for arguments that discovery is not proportional under Rule 26(b), or should be protected under Rule 26(c).

1. Privacy Interests

a. *Association*

Courts should restrict discovery that implicates privacy interests based on the Constitution and public policy. First, a litigant's right to privacy is implicated by compelled disclosure of her association—be it political, economic, religious or cultural affiliation.[303] Associational indicators abound in a person's smartphone, where website browsing history, GPS location information, and apps can indicate membership in political or religious organizations.[304] As Justice Sotomayor noted in her *Jones* concurrence, GPS data can disclose "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[305] As Chief Justice Roberts described in *Riley*, "[t]here are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life."[306] While *Jones*and *Riley* dealt with GPS information on a tracking device or cell phone, such technology is also available on wearable fitness trackers like Fitbit[307] and smart watches like Apple Watch.[308]

Social media content can also reveal protected association, be it in a person's profile, groups she follows, or posts she likes.[309] While a lot of this information is freely shared, at least with "friends," there are instances in which people use privacy settings to conceal associations they do not wish to share. Professor Woodrow Hartzog has written about two students at the University of Texas whose use of Facebook resulted in their sexual preferences being inadvertently revealed to other users, including their parents.[310] Despite their use of privacy settings, Facebook revealed to all their "friends" that they had been added to the student Facebook group "Queer Chorus."[311] Social media groups are as wide-ranging as the apps described by Chief Justice Roberts in *Riley*.[312] Some of those groups are limited in membership and maintain confidentiality.[313] The simple question or interrogatory asking what social media accounts a person uses can implicate associational interests, as there are social media networks based on religion,[314] sexuality,[315] and gender identification.[316]

b. *Zones of Intimacy*

Second, discovery should be protected where it implicates constitutional zones of intimacy, including marriage, procreation, contraception, family relationships, child rearing and education, health, and sexuality.[317] Smartphones are the primary communication tool for most people, who use their phones to send emails, text messages, or mobile app messages to spouses, children, and other family members and loved ones. Some of those communications can be quite explicit.[318] Health or medical information is stored on smartphone apps or web browsing history.[319]

Discovery of social media content can also reveal very personal information such as sexual orientation.[320] Wearable devices and other health sensors have the capacity to reveal a great deal about a person.[321] Many such devices track blood pressure, blood sugar levels, body temperature, heart rate, and breathing activity, all of which can indicate problems like disease.[322] Wearables, somewhat notoriously, can also track sexual activity.[323] More cutting-edge digestible and implantable devices provide information about all manner of bodily functions.[324] And information from smart speakers and home security cameras could reveal information only limited by the imagination.[325]

c. *Other Privacy Interests*

Third, discovery is subject to protection when it implicates other personal information protected by the Constitution or by public policy. This includes financial information, employee files, criminal activity files, military service files, personnel and medical files, and credit information.[326] Many people use banking apps or store personal medical or financial files on

their smartphones.[327] Fitbits and other health trackers clearly risk disclosure of medical information.[328]

2. Clear Relevance and Limitation on Impeachment

Discovery requests for private information should generally be justified by a clear showing of relevance to a party's claim or defense and compelling need. Courts should limit discovery where it would go to impeachment or violate a policy of the Rules of Evidence. This should be an aspect of proportionality: the greater the connection between the discovery and the "heart of the claim," the more likely it is to be granted. In contrast, when discovery is less connected to the claim, the balance tips in favor of privacy and against disclosure.

One case shows a court properly weighing the use of the discovery in determining whether to allow a broad, invasive request. In *Hedenburg v. Aramark American Food Services*,[329] a gender discrimination claim, the defendant sought a "mirror image" of the plaintiff's home computer in the effort to "probe the veracity" of her claims.[330] The court distinguished other cases where courts had allowed such a search as being "where the contents of the computer go to the heart of the case."[331] In contrast, the defendant here was "hoping blindly to find something useful in its impeachment of the plaintiff."[332]

In a recent decision from the Northern District of California, *Henson v. Turn, Inc.*,[333] plaintiff subscribers to Verizon's cellular and data services brought a data-privacy class action alleging that defendant Turn engaged in an illegal practice of placing "zombie cookies" on users' devices to track their web browsing and application use in order to tailor advertisements to them.[334] Turn sought production from the plaintiffs of all mobile devices they used during the class period to access the internet (or complete forensic images of the devices), data regarding their web browsing history, and data regarding any cookies stored on or deleted from their devices.[335] The court first noted the importance of a person's cell phone to his or her daily life:

> Users increasingly use a single mobile device — a smartphone or a tablet — for their online activities, including web browsing, reading the news, listening to radio content, accessing their banking information and managing their finances, shopping online, using GPS for directions and traffic updates, communicating over email and social networks, and reading sites like WebMD to assess their medical condition.[336]

Web browsing information in particular is "inextricably linked to personal information" since it "can reveal her location, interests, purchases, employment status, sexual orientation, financial challenges, medical conditions, and more."[337]

In denying the request for production of the phones for inspection, the court found the request called for information that is both not relevant and is disproportional to the needs of the case.[338] As to relevance, the request "threatens to sweep in documents and information that are not relevant to the issues in this case, such as the plaintiffs' private text messages, emails, contact lists, and photographs."[339] As to proportionality, the court noted the growing number of cases and commentators to recognize that privacy interests can be an important consideration, "particularly in the context of a request to inspect personal electronic devices."[340] The court quoted widely from *Riley*.[341] In particular, the court found that Turn's request for production of web browsing history and cookie data implicated "significant privacy concerns."[342]

Similarly, in a decision from the District of Connecticut, the court denied a plaintiff's motion to inspect the cell phone of a supervisor in a racial discrimination suit, without first using other discovery devices.[343] While the plaintiff had an interest in discovery regarding racists jokes and texts shared via the phone, the defendant's privacy interest in the data stored there outweighed the interest in disclosure.[344] Again, the court was persuaded by the Supreme Court's opinion in *Riley*, "which recognized, albeit in the criminal context, the privacy concerns implicated by the modern cell phone."[345]

In contrast, a Florida court upheld an order allowing a defendant to examine the cell phone of a woman killed in a car accident in litigation brought by her family.[346] The court recognized the decedent's privacy interests in the cell phone, but found the order narrowly tailored its request to allow discovery based on the highly relevant issue of whether the decedent was texting at the time of the accident.

> [W]here personal information is involved as in this case, the trial courts' discretion to permit discovery "must be balanced against the individual's competing privacy interests to prevent an undue invasion of privacy." Courts have reversed rulings for not adequately accounting for privacy interests in the inspection of electronic storage devices. . . .
>
> But, contrary to Petitioner's argument, privacy rights do not completely foreclose the prospect of discovery of data stored on electronic devices. Rather, limited and strictly controlled inspections of information stored on electronic devices may be permitted.[347]

In this context, therefore, the narrowly tailored order was appropriate because of the close nexus between the relevant private data and the heart of the case.

A primary reason many litigants seek social media discovery and data from wearables or smart speakers is to attack credibility. Defense attorneys freely recommend to each other to seek information from a plaintiff's social media, Fitbit, or Alexa for purposes of impeachment.[348] Such requests should carry less weight in the proportionality balance than when the discovery is relevant to the claim.

Finally, as part of its balancing, courts should be careful to protect against discovery that implicates privacy of third parties. All the modern subjects of discovery have the potential to reveal a great deal of information about people other than the owner of the phone, social media account, activity tracker, or smart speaker. Cell phones contain communications with and photographs of other parties. Social media content reveals interactions, associations, and photographs with friends who may be using privacy settings or interacting in a "group" that promised privacy.[349] Fitness trackers may be used to share fitness and health information with others.[350] It goes without saying that smart speakers and cameras do not choose to record only certain users and could capture conversations and images of any person in proximity to the device.

3. Mosaic Theory

Lastly, courts should recognize that modern discovery may not fit traditional notions of privacy as secrecy.[351] Clearly, Supreme Court case law provides strong support for privacy rights in cell phones, GPS data, and cell site location information, particularly when requests span a long period of time. GPS capability can be found not only in smartphones but in other devices like fitness trackers and Apple watches.[352]

In addition, the mosaic theory can apply to other types of discovery that have been seen as deserving of no privacy protection. Social media in particular, even when protected by privacy settings,[353] has been described by courts as having no privacy interest because of its communicative and public nature.[354] But not all social network sites are as "public" as others.[355] In addition, when aggregated, a person's social media content becomes a picture of that person's entire life.[356]

In a thoughtful opinion from the District of Wyoming, the court considered a broad request by defendants in a motor vehicle accident for social media directed against the plaintiff, who sought damages based on physical injuries, traumatic brain injury, posttraumatic stress disorder, anxiety and depression.[357] The court noted the changes in discovery wrought by broad increases in data, and by social media in particular:

> Social media presents some unique challenges to courts in their efforts to determine the proper scope of discovery of relevant information and maintaining proportionality. While it is conceivable that almost any post to social media will provide some relevant information concerning a person's physical and/or emotional health, it also has the potential to disclose more information than has historically occurred in civil litigation. While we can debate the wisdom of individuals posting information which has historically been considered private, we must recognize people are providing a great deal of personal information publicly to a very loosely defined group of "friends," or even the entire public internet. People have always shared thoughts and feelings, but typically not in such a permanent and easily retrievable format. No court would have allowed unlimited depositions of every friend, social acquaintance, co-employee or relative of a plaintiff to inquire as to all disclosures, conversations or observations. Now far more reliable disclosures can be obtained with a simple download of a social media history.[358]

The court looked to previous decisions for guidance in balancing against overbroad discovery all while recognizing the defendants' "legitimate interest in discovery which is important to the claims and damages it is being asked to pay," including information "which reveals that the plaintiff is lying or exaggerating his or her injuries."[359] Tying the analysis to the proportionality requirement in Rule 26, the court denied discovery of the plaintiff's entire Facebook history, but ordered production of "relevant history which addresses Plaintiff's *significant* emotional turmoil, any mental disability or ability, or relate *significant* events which could reasonably be expected to result in emotion distress."[360] Social media requests should be limited to avoid revealing an aggregate chronicle of a person's life.

Moreover, discovery requests of different media can themselves combine to create an exceedingly comprehensive picture of a person's life over a span of time. In the *Hinostroza* case discussed in the Introduction, the defendant sought five years of Fitbit and social media data, which could reveal the plaintiff's movements, religious and political associations, dating habits, sexual preferences, fertility, health, exercise and sleeping habits—a mosaic of her entire life for a five-year period.[361] The court in fact limited the social media discovery to one year (still a much longer period than the GPS tracking at issue in *Jones*), and ordered further information about plaintiff's search for Fitbit data.[362]

**Conclusion**

As in the Fourth Amendment context, discovery has been upended by changes in technology. Information that was not capable of creation is now saved automatically in vast databases. Formerly private communications are now shared in semi-public fora. People's movements, bodily functions—indeed, their entire lives—are chronicled by devices on their wrists or their countertops. Courts can and should apply privacy protections when this data is sought in discovery.

Text messages and other communications may be private if they implicate personal relationships or otherwise intrude on the zone of intimacy. Fitbit data intrudes on privacy of medical and other personal information, and may include GPS data that gives a detailed record of a user's activity every day. Social media account information too could offer a detailed portrait of a user's life, and could implicate associational and other constitutional privacy rights. Finally, all of these discovery requests risk the privacy of third parties. These considerations are appropriate for a court in balancing the need for the discovery—including how relevant it is to the claim—against the intrusion into the privacy of the party and others. The law gives courts the discretion to say this comprehensive, intrusive discovery is not proportional.

2022 WL 972401
Only the Westlaw citation is currently available.
United States District Court, D. Minnesota.

IN RE PORK ANTITRUST LITIGATION
This Document Relates To: All Class Actions

Case No. 18-cv-1776 (JRT/HB)
|
Signed 03/31/2022

**ORDER ON MOTION TO COMPEL HORMEL AND HORMEL CUSTODIANS TO PRODUCE RESPONSIVE TEXT MESSAGE CONTENT**

HILDY BOWBEER, United States Magistrate Judge

***1** This matter is before the court on Class Plaintiffs' Motion to Compel Hormel to Produce Responsive Text Message Content and to Enforce Subpoenas to Hormel Custodians. [ECF No. 883.] Plaintiffs seek an order: (1) compelling defendant Hormel Foods Corporation to produce the text message content of its currently employed custodians, including backup content stored on cloud services; (2) declaring Hormel had at the outset of the litigation an obligation to image text message content from all of its custodians' mobile devices and cloud backups, and an accompanying order for Hormel to do so now; and to the extent necessary (3) enforcing the subpoenas to the Hormel custodians for the same material. For the reasons set forth below, the Court grants in part and denies in part the motion.

**I. Background**

Plaintiffs in this coordinated multidistrict litigation, which includes several putative plaintiff classes and a number of "direct action plaintiffs," allege that Defendants, among America's largest pork producers and integrators, conspired to limit the supply of pork and thereby fix prices in violation of federal and state antitrust law. (See Oct. 20, 2020 Am. Mem. Op. & Ord. at 2 [ECF No. 520].) They allege Defendants were able to carry out the conspiracy in two ways: 1) by exchanging detailed, competitively sensitive, and closely guarded non-public information about prices, capacity, sales, volume, and demand through Agri Stats—a private service that gathers data from Defendants and produces market reports for paying subscribers; and 2) by signaling the need to cut production through public statements aimed at one another. (*Id.* at 6.) Plaintiffs allege that through these mechanisms, Defendants stabilized or increased the price of pork products from 2009 to the present.

In 2018, Class Plaintiffs requested that Hormel preserve data from personal cell phones of five company executives, James Snee, Jim Sheehan, Thomas Day, Steven Binder, and Cory Bollum, through forensic imaging. (Hormel Ex. 2 [ECF No. 929-1].) After objecting on several grounds, Hormel agreed to forensically image the phones. (Hormel Ex. 3 [ECF No. 929-2]; Hormel Ex. 4 [ECF No. 929-3].)

In 2019, Hormel and the Plaintiffs agreed to an ESI Protocol [ECF No. 292] and a Protocol for Preservation of Phone Records (Hormel Ex. 5 [ECF No. 929-4]). The Preservation Protocol applied to Hormel and its document custodians. Hormel initially identified seven document custodians. (Hormel Ex. 6 at 4 [ECF No. 929-5].) As a result of negotiations concluding in November 2020, the custodians now number thirty. (*See* Hormel Ex. 9 [ECF No. 929-8].) Seventeen are current employees; thirteen are former employees. (Custodians' Mem. at 2 [ECF No. 925].)

In November 2018, Plaintiffs served their first requests for production, in part seeking communications and meetings between the Defendants or related to the lawsuit's subject matter, and information regarding supply, demand, and price of pork products. (Bourne Decl. Ex. 5 at Requests 3–8, 14–19 [ECF Nos. 888-2].) It defined "document" to include text messages and cloud backups or archived text message data. (Bourne Decl. Ex. 5 at Definitions ¶¶ 8, 10.) Hormel objected that it did not have possession, custody, or control of the custodians' personal cell phone data. (Bourne Decl. Ex. 13 at 20 [ECF No. 888-2].) Hormel responded to the same effect to Plaintiffs' November 2020 interrogatories, which sought further information about the make, model, and use of the custodians' cell phones, though Hormel did provide the cell phone numbers of the custodians. (Bourne Decl. Ex. 4 at 20–23 [ECF 887-1].) On April 19, 2021, Plaintiffs asked whether Hormel had produced the text messages of two custodians' cell phones, to which Hormel responded that it did not have possession, custody, or control over those phones, so it would not produce those messages. (Bourne Decl. Ex. 6 [ECF No. 888-2].) Plaintiffs complained that Hormel had not alerted them earlier that it disclaimed control over those cell phones and insisted that Hormel produce the texts. (Bourne Decl. Exs.

7, 9 [ECF No. 888-2].) Hormel replied that it had complied with its duties under the phone record preservation protocol and general preservation obligation related to the personal cell phones outside its control. (Bourne Decl. Exs. 8, 10 [ECF No. 888-2].)

***2** While disagreeing with Hormel, Plaintiffs also subpoenaed the custodians directly for the information. (Bourne Decl. Ex. 17 [ECF No. 888-2].) The custodians' counsel interviewed each custodian to determine whether they might have potentially responsive communications on their cell phones. (Stephens Decl. ¶ 5 [ECF No. 926].) All of the custodians responded that they were currently using different phones from the phones they had used during the relevant time-period (January 1, 2008 – August 17, 2018). (Bourne Decl. Ex. 2.)[1] As summarized by the custodians' counsel,

> Of the thirty Subpoena Recipients, only a small group reported using their personal cell phones for work-related text communications external to Hormel during the relevant time period. More than half of those reported having their devices previously imaged. None of the Subpoena Recipients reported having any text communications with anyone outside of Hormel regarding supply and demand conditions in the pork industry. The vast majority of the Subpoena Recipients either did not use text messaging for work related communications or only used text messaging for communications with other Hormel employees.

(Stephens Decl. ¶ 8.) Somewhat more detail is provided in the information that was attached to the declaration of Plaintiffs' counsel. For purposes of this motion, the custodians' responses to the question of whether and to what extent they used their personal cell phones for work purposes and/or texted for work purposes, generally fell into five categories:

- Rarely communicated by text message for work-related matters: Cory Bollum, Donald Temperley, Eric Steinbach, Glenn Leitch, Holly LaVallie, James Fiala, and Jose Rojas.
- Did not communicate by text outside Hormel: Paul Bogle, Nathan Annis, Jerry Aldwell, Mark Coffey, Neal Hull, Steven Binder, Steven Venenga, and William Snyder, and Al Lieberum.
- Did not use text for communications of the nature sought by the subpoena: Jim Sheehan, Thomas Day, Jeff Ettinger, Jody Feragen, and James Snee.
- Never texted about work-related matters: Paul Peil, Lance Hoefflin, Alan Meiergerd, Jana Haynes, Jennifer Johnson, Michael Gyarmaty, Bryan Farnsworth, and Jesse Hyland.
- Never used their personal cell phone at all for work-related communications: Jessica Chenoweth.

(Bourne Decl. Ex. 1.) All custodians objected to the subpoenas. (Bourne Decl. Ex. 2.)

In further negotiations, Plaintiffs and the custodians discussed imaging the phones and allowing a forensic search with mutually agreed upon search terms. (Stephens Decl. ¶ 10.) Plaintiffs proposed that all phones be searched for all text messages sent to or received from 781 phone numbers associated with individuals affiliated with Hormel or any other Defendant or any of the other identified pork integrators, plus remaining texts containing any of 330 keywords, following which the custodians' counsel would review the results and produce relevant messages. (*Id.*, Ex. B [ECF No. 926-2]; Bourne Decl. ¶ 12 [ECF No. 887], Ex. 16 [ECF No. 888-2].) Plaintiffs demanded, however, that all "inter-defendant" text messages be produced without a further relevance review, on the ground that all such messages were relevant. (Stephens Decl. Ex. B.)

***3** Ultimately, the custodians maintained that Plaintiffs had not shown that all thirty custodians were likely to have texts responsive to the subpoenas, and that the proposed searches were overly broad and unduly burdensome. (Stephens Decl. ¶ 17.) The two sides also disagreed about which of them would bear the costs of the proposed searches. (Stephens Decl. ¶¶ 10, 17, Ex. B.)

Failing to reach an agreement with Hormel or the custodians, Plaintiffs filed this motion. Plaintiffs move this Court to compel Hormel to produce text message content relevant to its conspiracy claims within Hormel's possession, custody,

or control, in response to its requests for production seeking that information. They seek the same relief with regard to the custodians they subpoenaed.

Plaintiffs also seek a declaration that Hormel had from the outset of the litigation an obligation to image text message content from all of its custodians' mobile devices and cloud backups, and an accompanying order for Hormel to do so now.

**II. Whether Hormel Can Be Compelled to Produce Its Employees' Text Message Data**

Parties may obtain discovery that is

> relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

Fed. R. Civ. P. 26(b)(1). Rule 34 requires the production of any relevant and responsive documents in the responding party's possession, custody, or control, including text message content. *See, e.g.*, *Paisley Park v. Boxill*, 330 F.R.D. 226, 234 (D. Minn. 2019). Here, Hormel alleges that it does not have the requisite "possession, custody, or control" over the text messages sent by and to its employees on their personally-owned cell phones.

**A. The Meaning of "Control"**

Plaintiffs claim Hormel has failed to identify and produce relevant text message content from its document custodians over which Hormel has control. (Pls.' Mem. at 8 [ECF No. 885].) Hormel disputes control. While the Eighth Circuit has not weighed in, district courts in this Circuit have applied varying definitions of "control." Some have interpreted "control" to mean the legal right to obtain the documents. *See, e.g., Beyer v. Medico Ins. Group,* Case No. 08-CV-5058, 2009 WL 736759, at *5 (D.S.D. Mar. 17, 2009) ("The rule that has developed is that if a party 'has the legal right to obtain the document' then the document is within that party's 'control' and, thus, subject to production under Rule 34." (internal citation omitted)).

Other courts, including courts in this District, have held that "control" may also include the "practical ability" to obtain the documents. *See, e.g., Afremov v. Sulloway & Hollis, P.L.LC.*, Case No. 09-cv-03678 (PSJ/JSM), 2011 WL 13199154, at *2 (D. Minn. Dec. 2, 2011) (" 'Control' encompasses actual physical possession of the documents, but also the legal right or practical ability to demand the documents from a third party."); *In re Hallmark Cap. Corp.*, 534 F. Supp. 2d 981, 982 (D. Minn. 2008) ("documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action"); *Prokosch v. Catalina Lighting, Inc.*, 193 F.R.D. 633, 636 (D. Minn. 2000) (stating that "under Rule 34, control does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability, to obtain the documents from a non-party to the action" (quotations omitted), and directing the defendant to produce not only documents in its physical possession but also those that it was "capable of obtaining upon demand"); *New Alliance Bean & Grain Co. v. Anderson Commodities, Inc.,* Case No. 8:12-CV-197, 2013 WL 1869832, at *3 (D. Neb. May 2, 2013) ("documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action"); *Handi-Craft v. Action Trading, S.A.,* Case No. 4:02-CV-1731, 2003 WL 26098543, at *6 (E.D. Mo. Nov. 25, 2003) (holding that "the appropriate test is not of legal entitlement, but of control or practical ability to obtain the documents").

***4** Where the practical ability test is applied, the burden of demonstrating that the party from whom discovery is sought has the practical ability to obtain the documents at issue lies with the party seeking discovery. *New Alliance Bean & Grain,* 2013 WL 1869832, at *5. In assessing whether a party has the practical ability to obtain documents from a non-party, courts have focused on the "mutuality" of the responding party's relationship with the document owner, including whether the documents sought are considered records which the party is apt to request and obtain in the normal course of business, or whether the prior history of the case demonstrates cooperation by the non-party, including the production of documents and other assistance in conducting discovery, and the non-

party has a financial interest in the outcome of the litigation. *See Afremov*, 2011 WL 13199154, at *2 (D. Minn. Dec. 2, 2011) (collecting cases). The undersigned has also applied a practical ability analysis in ruling on a motion seeking to compel a U.S.-based party to produce documents in the possession of a Brazilian affiliate. Order, *M-I Drilling Fluids UK Ltd. v. Dynamic Air Inc.*, 14-cv-4857 (D. Minn. Nov. 13, 2015) [ECF No. 171].

That said, the Eighth Circuit has never decided whether the "legal right" or "practical ability" standard should govern, and other circuits are split on the issue. *See generally,* The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," 17 Sedona Conf. J. 467, 482-92 (2016) (collecting cases). Indeed, in part because of that variability, the Sedona Conference has urged adoption of a consistent, "reliable, objective approach" that defines control "as the legal right to obtain and produce the Documents and ESI on demand." *Id.* at 528. The Sedona Conference has criticized the "practical ability" standard on several grounds, including that its imprecision "has resulted in inconsistent and, at times, inequitable results in many contexts." *Id.* It describes the standard as "inherently vague," "unevenly applied," having the potential to lead to "disparate results," and potentially leading to inequitable or even "futile" results. To that last point, the commentary cites by way of example one court's observation that even if it were to order a party employer to collect and turn over personal emails of its employees, the moving party had not identified any authority under which the employer could *force* the employees to turn them over. *Id.* at 542 n. 126, citing *Matthew Enter., Inc. v. Chrysler Grp. LLC,* Case No. 13-cv-04236-BLF, 2015 WL 84982256 (N.D. Cal. Dec. 10, 2015).

Relatedly, the Ninth Circuit has recognized that "[o]rdering a party to produce documents that it does not have the legal right to obtain will oftentimes be futile, precisely because the party has no certain way of getting those documents." *In re Citric Acid Litig.*, 191 F.3d 1090, 1108 (9th Cir. 1999). And yet, a strong argument can be made that if a party's relationship with a non-party is such that the former routinely obtains certain kinds of documents from the latter in the ordinary course of business, and perhaps has already even leveraged that access to obtain documents for its own use in the litigation, fairness would require that it also be required to do so for purposes of responding to discovery. Order, *M-I Drilling*, 14-cv-4857, at 7–9.

In this case, however, the Court need not choose between the "legal right" and "practical ability" standard because, for the reasons discussed below, it finds that regardless of the standard applied, Plaintiffs have not shown that Hormel has control over text messages on the personally-owned phones of its employees.

### B. Whether Hormel's BYOD Policy Gives Hormel Control Over Text Messages on Personally-Owned Cell Phones

Plaintiffs argue that Hormel has control of the custodians' personal text messages because its "bring your own device" (BYOD) requires employees to use their cell phones to conduct business, and Hormel controls all data on those phones through the BYOD policy and the ability afforded as a result of that policy to wipe all data on personally-owned phones whenever it deems necessary. (Pls.' Mem. at 9–11.) Hormel responds that the BYOD policy does not give it the legal authority to access, view, image, or control the text messages, and therefore it lacks control over those messages. (Hormel Mem. at 12–13.)

***5** Hormel has had a BYOD policy since at least 2011.[2] (*See* Bourne Decl. Ex. 14 [ECF No. 887-1]; Hormel Ex. 1 [ECF No. 930].) The policy allows employees to use their personally-owned cell phones to interact remotely with certain Hormel corporate systems. (*See* Hormel Ex. 1 § A.) It also provides for employees who have a defined business need to be reimbursed for mobile device service for a personally-owned phone, although the employee is responsible for all costs associated with purchasing and maintaining the phone and any accessories, as well as the costs of any application downloads or purchases. (Hormel Ex. 1 at 4, 5 § B; Morrison Decl. ¶¶ 10, 15–16 [ECF No. 928].) Hormel claims ownership of all "data that is sourced from Hormel systems and synced between the mobile device and its servers." (*See* Hormel Ex. 1 at 6 § F; Morrison Decl. ¶¶ 7–8.) Such data "primarily consists of company email, calendars, and contacts (if set up through an employee's corporate email account)," but does not include "text messages or other information on a personally-owned device." (Morrison Decl. ¶¶ 8–9.) The policy does not explicitly assert ownership, control, or ability to access, inspect, copy, image, or limit personal text messages. (*See* Hormel Ex. 1 § F.)

Hormel requires an employee who accesses Hormel data using their personal phone to install the MobileIron application. (Morrison Decl. ¶¶ 11, 14, 18.) MobileIron

prevents an employee from copying or backing up Hormel-owned data residing on their phone. (Morrison Decl. ¶¶ 13–14.) It does not interfere with or limit the employee's ability to copy, delete, or back up text messages, nor does it enable Hormel to access or image text messages. (Morrison Decl. ¶¶ 18–20.) Through the BYOD policy, Hormel reserves the right to remotely remove MobileIron and the company data controlled by MobileIron, or to remotely wipe (i.e. factory reset) the phone in order to wipe all Hormel-owned data, but the policy warns that such a wipe may delete all data the phone, including personal data such as text messages. (Hormel Ex. 1 § F; Morrison Decl. ¶¶ 11–12.) However, following a wipe, the employee may freely restore any personal data he or she had previously backed up to external storage. (Morrison Decl. ¶ 17.)

Plaintiffs read the BYOD policy's provision that "[a]ll approved employees will be expected to use a personally-owned mobile device" to mean that all Hormel employees are required to own personal cell phones and to use them for business. (Pls.' Mem. at 8.) Plaintiffs misconstrue the policy by taking this statement out of its context. An employee must request Hormel's permission to use a personally-owned cell phone to access Hormel's systems, and may request that Hormel reimburse the employee for monthly carrier service charges. Hormel will approve such a request if it concludes the employee has a "defined business need" to use the phone in the ordinary course of his or her work for the company. (*See* Hormel Ex. 1 § A, App. A.) However, nothing in the policy appears to require any employee to use a personally-owned phone to conduct work, and nothing in the policy requires any employee who uses a personally-owned phone to use text messaging to conduct work.

Plaintiffs next argue Hormel's remote wipe ability gives it control over employee texts, but the Court disagrees. The MobileIron application does not give Hormel the ability to access, inspect, copy, or image text messages; it only gives Hormel the ability to wipe those messages as part of a remote factory reset of the phone if Hormel concludes the security of its own data on the phone has been put at risk and if it cannot limit the wipe to only company data. Similarly, the BYOD policy does not assert Hormel's ownership over any data other than data "sourced from Hormel systems and synced between the mobile device and its servers"—which does not include text messages (except, perhaps, if the employee copied data sourced from a Hormel system and embedded it in a text)—nor does it assert Hormel's right to demand that its employees allow it to access or inspect any other data. Hormel's right and ability to remotely wipe an entire phone is for the sole and express purpose of removing company data—such as in response to the phone being lost or stolen. The company's ability to wipe personal data from a personally-owned device by resetting the device to a factory floor state in order to purge company data does not give the company control—legal or practical—over that personal data. The Sedona Conference has taken the position that an employer does not legally control personal text messages despite a BYOD policy when the policy does not assert employer ownership over the texts and the employer cannot legally demand access to the texts. The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 Sedona Conf. J. 495, 531 (2018).

***6** The Court is not persuaded otherwise by *H.J. Heinz Co. v. Starr Surplus Lines Ins. Co*. Case No. 2:15-cv-00631-AJS, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015), *report and recommendation adopted*, 2015 WL 12792025 (W.D. Pa. July 31, 2015). (Pls.' Mem. at 9–10.) The special master in *Heinz* concluded that since Heinz's BYOD program provided that all company information and emails on both company-owned and personally-owned mobile devices were the sole property of the company, the company had custody and control of its own data on those devices. The special master did not, however, suggest that the control extended to any personal data on the phone. 2015 WL 12791338 at *4. Notably, the special master was not required to resolve the question of whether Heinz had control over text messages on personally-owned phones because the only such custodian specifically before the special master stated he did not use his personal phone to send or receive text messages related to substantive Heinz business. And while the special master recommended that the company be required to interview other custodians about the existence of any potentially relevant text messages on their phones and to produce such messages if they existed, it is not clear whether that requirement was limited to the scope of the underlying reasoning—i.e., text messages on company-owned phones and text messages on personally-owned phones that contained company data—or whether the special master assumed Heinz could require that its employees produce for inspection, review, and production text messages on personally-owned phones that did not include company-owned data (and if so, on what legal basis). Nothing in the special master's report and recommendation suggested, as Plaintiffs do here, that the company had overall control over text messages on an personally-owned cell phones.

Therefore, the Court is not persuaded by Plaintiffs' arguments that the BYOD policy gives Hormel control over the text messages on personally-owned cell phones.

**C. Whether the Relationship Between Hormel and the Custodians Gives Hormel Control Over Text Messages on Personally-Owned Cell Phones**

Plaintiffs argue that even if the BYOD policy did not give Hormel the legal right to demand access to text messages on personally-owned phones, the relationship between it and its employees gives it the practical ability to demand access to that data. Plaintiffs argue Hormel could have asked all of its custodians to give it access to text messages and all custodians likely would have agreed. They base that argument in part on the fact that Hormel had previously asked for and received permission to *image* (although not to inspect, copy, or produce the content of) the personal cell phones of five executive custodians: James Snee, Jim Sheehan, Thomas Day, Steven Binder, and Cory Bollum. (Tr. at 15–16 [ECF No. 945].) (Hormel Exs. 2–3; Bourne Ex. 1.)

The Court disagrees. It is one thing to show that a responding party may *ask* for documents in the possession of someone with whom it has a relationship, but quite another to conclude that the party has the practical ability to *demand* such documents, and therefore has "control" over them. The Court is particularly sensitive to this distinction in the context of the employment relationship. While one might argue that the employees' fear for their job security or interest in the financial well-being of the company will incentivize them to say "yes" to turning over their text messages for inspection and possible production is not, in the opinion of the undersigned, the kind of "practical ability" contemplated by that standard. Practical ability to demand access to documents has generally been found where the relationship between the party and non-party, and the types of data or documents at stake, give rise to the conclusion that the non-party would give (and often, has given) the party access to those data and documents in the ordinary course of business. *See, e.g.,* Order, *M-I Drilling*, 14-cv-4857, at 7–9; *Camden Iron & Metal, Inc. v. Marubeni Amer. Corp.,* 138 F.R.D. 438, 443 (D.N.J. 1991) ("The proper inquiry here is whether the documents sought are considered records which [the defendant subsidiary] is apt to request [from the non-party parent] and obtain in its normal course of business."); *Cooper Indus., Inc. v. British Aerospace,* 102 F.R.D. 918, 919–20 (S.D.N.Y. 1984) (holding that where the defendant was the distributor and servicer of the non-party affiliate's planes, it must produce certain documents in the possession of the affiliate, and noting that the documents sought "all relate to the planes that defendant works with every day; it is inconceivable that defendant would not have access to these documents and the ability to obtain them for its usual business.").

***7** Here, there is no evidence that in the ordinary course of business Hormel seeks, needs, or expects to gain access to the content of employees' text messages on their personally-owned phones. That five executives agreed to have their phones imaged for the purpose of preserving the data does not establish that Hormel has the practical ability to demand that it be allowed to inspect or produce the data, and it is no evidence at all that other custodians would be amenable to doing so. Plaintiffs contend that at least those custodians who are currently employed by Hormel will wish to help their employer in this case. (Tr. at 15–16.) But while those custodians may feel a sense of company loyalty and/or have an interest in the company's financial health, it goes too far to extrapolate from that a practical ability on Hormel's part to demand access to the data on their phones. *Cf. U.S. Intern. Trade Com'n v. ASAT, Inc.,* 411 F.3d 245, 255 (D.C. Cir. 2005) (rejecting the "untenable position" that simply because the parent may have a financial interest in the outcome of litigation involving its subsidiary, the subsidiary has the ability to control its parent's documents).

Similarly, the fact that Hormel employees willingly responded to questions from Hormel's counsel regarding whether and to what extent they conducted company business by use of personal text messages, (Tr. at 30–31), does not establish a practical ability to demand that the data on those telephones be turned over to Hormel for imaging, review and production. While Hormel owns, and therefore may have a legal right to demand, company data that resides on a personal cell phone—even if that data may reside in a text message—what Plaintiffs are demanding here is that Hormel leverage that putative right in order to demand access to *all* text messages so that it can review and produce those deemed responsive to discovery in this case, regardless of whether they include company data over which Hormel claims ownership per the BYOD policy. The Court shares the Sedona Conference's view that "organizations should not be compelled to terminate or threaten employees who refuse to turn over their devices for preservation or collection." 19 Sedona Conf. J. at 531.

Accordingly, the Court denies Plaintiff's motion insofar as it seeks to compel Hormel to collect, review, and produce

responsive text messages on its employees' personally-owned cell phones.

**III. Whether Plaintiffs' Subpoenas to Hormel's Employees and Former Employees Should Be Enforced**

Plaintiffs also move that the Court enforce their subpoenas directed to the custodians for text message information in their phones and cloud backups. (Pls.' Mem. at 14.) The scope of discovery for a Rule 45 subpoena is the same as the scope of discovery under Rules 34 and 26 and is subject to the same constraints on relevance and proportionality. *See* Fed. R. Civ. P. 34(c), 45; *Mille Lacs Band of Ojibwe v. Cty. of Mille Lacs*, No. 17-cv-5155 (SRN/LIB), 2020 WL 1847574, at *5 (D. Minn. Apr. 13, 2020); *Shukh v. Seagate Tech., LLC*, 295 F.R.D. 228, 236 (D. Minn. 2013). A person subject to a subpoena may object to the subpoena, as the custodians did here, in which case the requesting party may move the court to compel production. Fed. R. Civ. P. 45(d)(2)(B). (Custodians' Mem. at 7–8 [ECF No. 925].)

Under Rule 45(d)(1), even if the subpoena seeks relevant information, discovery is not permitted where it imposes an undue burden on the subpoenaed person, considering the same factors as those relied on for proportionality in Rule 26(b). *See Misc. Docket Matter No. 1 v. Misc. Docket Matter No. 2*, 197 F. 3d 922, 925 (8th Cir. 1999); *see also Deluxe Fin. Servs., LLC v. Shaw*, Case No. 16-cv-3065 (JRT/HB), 2017 WL 7369890, at *4 (D. Minn. Feb. 13, 2017) ("These considerations are echoed in the proportionality factors set forth in the amended Rule 26(b)(1)."). Concern for the burden on a non-party subject to a subpoena carries special weight when balancing competing needs. *Id.* The Court must quash or modify a subpoena that imposes an undue burden on the non-party or requests irrelevant information. Fed. R. Civ. P. 45(c)(3)(A)(iv).

***8** Neither party bears a rigid evidentiary burden in this dispute. The advisory committee notes for the 2015 amendments to Rule 26 advise that the parties and the Court bear "collective" responsibility to consider relevance and proportionality/undue burden. A party requesting production should be able to explain the ways the requested information bears on the issues of the case, while the person resisting production will ordinarily have much better or the only information about the burden and expense of production. *Id.* The Court does not place the burden of proving relevance or proportionality/undue burden on any party, but instead considers all the information brought by the parties to determine the appropriate scope of the subpoenas. *Deluxe Fin. Servs., LLC v. Shaw*, Case No. 16-cv-3065 (JRT/HB), 2017 WL 7369890, at *4 (D. Minn. Feb. 13, 2017). [3]

Plaintiffs' subpoenas made seven requests, and all custodians gave substantively the same response to each. (*See* Bourne Decl. Ex. 2.) Plaintiffs do not identify the specific requests for which they seek the motion to compel, but their arguments address the information requested by Requests 1 and 5, and they do not raise any issues with the custodians' responses to the other requests. (*Compare* Pls.' Mem. at 14-16, *with*, Bourne Decl. Ex. 17 Requests 1–7.) The Court accordingly confines its review to Requests Nos. 1 and 5. Those requests and the custodians' responses are as follows:

> **Request No. 1**: Produce a copy of each Text Message that you sent or received during the Relevant Time Period with an Employee or Representative of a Pork Integrator, or any other individual with whom you communicated about supply and demand conditions in the Pork industry.
>
> **Response:** [The custodian] objects to this request as vague and ambiguous, and overbroad and unduly burdensome to the extent it seeks information not relevant to any party's claims or defenses in this litigation, and is disproportionate to the needs of the case. [The custodian] objects to this request to the extent it imposes an undue burden on a non-party by seeking "each Text Message" exchanged with the identified individuals over a ten-year period that ended three years ago. [The custodian] further objects to this request to the extent it seeks information equally available from another source that would be less burdensome and more appropriate under the circumstances. Subject to and without waiving the foregoing objections, [the custodian] is not aware of any documents responsive to this request.
>
> ***9 Request No. 5**: Documents sufficient to show, and provide access to the forensic vendor for collection purposes, the location, date, and scope of any archived copies of your cellphone data, such as iTunes archives or iCloud archives.
>
> **Response**: [The custodian] objects to this request as vague and ambiguous, and overbroad and unduly burdensome to the extent it seeks information not relevant to any party's claims or defenses in this litigation, and is disproportionate to the needs of the case. [The custodian] objects to this request to the extent it imposes an undue burden on a non-party by seeking all archived cellphone data over an unreasonably long period of time.

(Bourne Decl. Ex. 2.) The custodians' explained their objections further in letters attached to the responses and during the motion hearing and in their memorandum opposing Plaintiffs' motion. (*Id.*; Custodians' Mem. at 10; Tr. at 45–48.) They objected that the subpoenas seek irrelevant information, are ambiguous and vague, and that information sought was equally available from their cell phone service providers; the subpoenas imposed an undue burden on them; the definition of "pork integrator" was overbroad and unduly burdensome; Plaintiffs had not shown that responsive texts were likely to exist on their phones or data backups; and there was no adequate protective order to protect private and confidential information on their phones. [4] (*See, e.g.*, Bourne Decl. Ex 2 at ECF 13–14, 18–19. *See also* Custodians' Mem. at 9–11; Tr. at 45–48.)

**A. Whether the Custodians' Have Adequately Demonstrated That They Do Not Have Responsive Texts**

Counsel for the custodians argue they have undertaken reasonable steps to investigate whether unique responsive information exists on any custodian's cell phone; both Hormel and the custodians argue that those inquiries have suggested that no such information exists, while Plaintiffs have not shown reason to conclude to the contrary. (Hormel Mem. at 25–28; Custodian's Mem. at 9–10; *see generally* Stephens Decl.)

A court may deny a motion to compel when the information sought is "almost certainly nonexistent or the object of pure speculation." *Struzyk v. Prudential Ins. Co. of Am.*, Case No. 99-1736 (JRT/FLN), 2003 WL 21302966, at *2 (D. Minn. May 16, 2003). A court will do so when evidence shows that the responding party has searched for the information but cannot find it or disclaims its existence after the search, and the movant shows no evidence to suggest the information exists. *See id.* (denying motion to compel where responding party argued that it produced all responsive documents and presented detailed affidavits of its efforts to locate any responsive documents, while the movant presented no contrary evidence); *Johnson v. Charps Welding & Fabricating, Inc.*, Case No. 14-cv-2081 (RHK/LIB), 2017 WL 9516243, at *11 (D. Minn. Mar. 3, 2017) (denying in part motion to compel where responding party agreed to produce certain responsive documents, argued that no additional related documents existed, and presented an affidavit describing the creation and storage of the documents, while the movant presented no contrary evidence); *compare Farmers Ins. Exch. v. West*, Case No. 11-cv-2297 (PAM/JJK), 2012 WL 12894845, at *5 (D. Minn. Sept. 21, 2012) (granting in part motion to compel where responding party disclaimed the existence of responsive documents, but the record failed to show that the party searched for them and the movant presented evidence suggesting that the documents existed).

***10** This standard strikes a balance between two interests in discovery. A responding party has a duty under the Federal Rules of Civil Procedure to affirmatively, reasonably search for responsive information available to it. *Farmers Ins. Exch.*, 2012 WL 12894845, at *5. But once it fulfills that responsibility, "[t]he Court must accept, at face value, a party's representation that it has fully produced all materials that are discoverable ... because the Court has no means to test the veracity of such avowals." *Bombardier Recreational Prod., Inc. v. Arctic Cat, Inc.*, Case No. 12-cv-2706 (MJD/LIB), 2014 WL 5685463, at *7 (D. Minn. Sept. 24, 2014).

Here, the custodians' counsel interviewed the custodians to ascertain whether it was likely that potentially relevant and responsive texts would be on their phones. They represent that in those interviews, all of the custodians disclaimed on one basis or another having any texts that might be responsive. (Bourne Decl. Exs. 1, 2; Stephens Decl. ¶¶ 5–8.) But with the exception of Jessica Chenowith, who stated unequivocally that she *never* used her personal cell phones for work-related communications, the Court cannot conclude from the responses that adequate steps were taken to describe to the custodians what kinds of communications might be relevant and responsive information in the context of this complex litigation, or to test the accuracy of their recall about whether, at some point over the relevant period or periods, they sent or received relevant or responsive texts.

Granted, the evidence that responsive texts *do* exist is quite weak. Plaintiffs declare under oath that they obtained records from a telephone service provider showing custodians Eric Steinbach, Holly LaVallie, James Fiala, Michael Gyarmaty, and Steven Venenga texted work-related contacts. (Pls.' Mem. at 15–16; Bourne Decl. ¶¶ 18–20.) But the provider had no information about the content of the messages, and the fact that the texts were sent to or from work-related contacts does not mean the content of the texts was work-related, let alone that the content was relevant to the claims or defenses in this case. Plaintiffs also argue that certain of the custodians —Paul Bogle, Corwyn Bollum, Jessica Chenoweth, Lance Hoefflin, Paul Peil, Jose Rojas, and Donald Temperley— worked with Agri Stats and/or managed the throughput of

pork in Hormel's operations, suggesting that they are more likely to have responsive texts. (Hormel Exs. 6, 8 at 2.) Several of them—Bogle, Bollum, Rojas, and Temperley—also implied or acknowledged in their subpoena responses that they used text messaging for business to some degree. (Bourne Decl. Ex. 1.)

Provided Chenowith submits to Plaintiffs a sworn declaration reiterating her unequivocal representation that she did not use her personal cell phone for work related communications at all, the Court concludes Chenowith has adequately shown that responsive texts on her cell phone or in her archived data are "almost certainly nonexistent or the object of pure speculation." *Struzyk*, 2003 WL 21302966, at *2. Unlike the other custodians, Chenowith alone appears to have observed a clear boundary about the use of her personal cell phone, and could say without qualification that she did not use it in any manner for work purposes. Plaintiffs have offered no evidence to the contrary. Accordingly, the Court will not enforce the subpoena directed to Chenowith with regard to Requests Nos. 1 and 5.

But as to the remaining custodians, the Court is not satisfied that the inquiries made by counsel and the resulting representations by the custodians adequately demonstrate that there was a reasonable search for responsive texts such that the Court can conclude such texts are almost certainly nonexistent. *See Farmers Ins. Exch.*, 2012 WL 12894845, at *5. All custodians but Chenowith either acknowledge they might have used their cell phones for work related communications, even if only minimally, or they made no representations at all on that subject. Nothing suggests the custodians did, or were asked to do, anything beyond consulting their memories about whether they might have sent or received responsive or relevant texts, or even that they understood the full scope of what kinds of communications that might encompass. No evidence suggests that anything was done to test their memories, which is particularly problematic given that the time periods are in some instances years in the past and text-messaging is by its very nature short, quick, often reactive, and therefore unlikely to be particularly memorable.

***11** Since for all custodians other than Chenowith, the evidence does not show a reasonable search or that responsive texts are "almost certainly nonexistent or the object of pure speculation" *Struzyk*, 2003 WL 21302966, at *2, this argument does not provide a basis for the Court to decline to enforce Requests Nos. 1 and 5 as to those custodians.

### B. Whether the Court Should Decline to Enforce the Requests Because They Are Vague or Ambiguous, or Because the Information is Available From Other Sources

The Court overrules the custodians' objections regarding vagueness and ambiguity, including with respect to the definition of "pork integrator," because they provide no arguments, explanation, or evidence to support those objections. *Mead Corp. v. Riverwood Nat. Res. Corp.*, 145 F.R.D. 512, 515 (D. Minn. 1992) ("[A]n objection to a discovery request cannot be merely conclusory, and ... intoning the 'overly broad and burdensome' litany, without more, does not express a valid objection.") Though the Court does not place an evidentiary burden on those objections, the Court cannot determine the grounds on which the custodians base these objections without some explanation to support them. Moreover, vagueness and ambiguity objections, even if otherwise well-taken, can be addressed in a meaningful meet-and-confer. These objections are therefore overruled.

The Court also overrules the objection that the information sought is equally available from the cell phone providers. Plaintiffs declare under oath that they obtained records from a telephone service carrier showing that custodians Eric Steinbach, Holly LaVallie, James Fiala, Michael Gyarmaty, and Steven Venenga sent texts to work-related contacts. (Pls.' Mem. at 15–16; Tr. at 13; Bourne Decl. ¶¶ 18–20.) The carrier did not record the content of any text messages, so the information is not available from that source. (Tr. at 14.) Plaintiffs also point out that carrier data would not reveal iMessage to iMessage content, as that content is only available on the respective iPhones. (Tr. at 51.) The custodians do not offer any concrete support for their claim that the content of any relevant and responsive text messages would be available from any other source. Thus, the record fails to substantiate this objection.

### C. Whether Imaging the Phones and Searching the Data Imposes an Undue Burden and is Disproportionate to the Needs of the Case

The custodians object that the very imposition of the requests for cell phone data imposes an undue burden on the custodians that is disproportionate to the needs of the case. (*See, e.g.*, Bourne Decl. Ex. 2 at ECF 13–14, 18–19. *See also* Custodians' Mem. at 9–11; Tr. at 45–48.). Undue burden in the subpoena context relies on similar factors to proportionality in the broader context of a motion to compel,

though courts have heightened concern for and reluctance to impose discovery burdens on a non-party compared to a party. *Deluxe Fin. Servs.*, 2017 WL 7369890, at *4. Any order compelling compliance with a subpoena "must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance." Fed. R. Civ. P. 45(d)(2)(B)(ii).

> An objection that discovery is overly broad and unduly burdensome must be supported by affidavits or offering evidence revealing the nature of the burden and why the discovery is objectionable. It is not sufficient to simply state that the discovery is overly broad and burdensome, nor is a claim that answering the discovery will require the objecting party to expend considerable time and effort analyzing 'huge volumes of documents and information' a sufficient factual basis for sustaining the objection.

***12** *Abhe & Svoboda, Inc. v. Hedley*, Case No. 15-cv-1952 (WMW/BRT), 2016 WL 11509914, at *3 n.5 (D. Minn. Mar. 15, 2016). Though the non-party resisting a subpoena is often in the best position to provide information to sustain its objection, the Court will examine all evidence in the record. *Id.* at *3.

The custodians argue burden along several lines. They allege that they have an estimate of between $65,000 and $85,000 in total to image all thirty phones [5], that imaging each phone will take between three hours and more than a day based on the amount of data on the phone, and that some number of them live out of state or in rural Minnesota and will have to mail their phones to Hormel's third-party forensic imaging provider. (Custodians' Mem. at 10; Tr. at 45–48.) They also argue the production will capture significant amounts of private and confidential information unrelated to this case. (*Id.*) The Court addresses these concerns in order.

First, as to the costs or time to image the phones, there are no affidavits or other evidence of record establishing the amount of data on any individual custodian's phone or the estimated time or cost to image it. Furthermore, it is not entirely clear to the Court that the cell phones would need to be imaged in their entirety, or whether text messages in particular can be extracted more economically. Nor is it clear to the Court that all cell phones would need to be imaged, given that currently used cell phones were not in use during the period from January 1, 2008 – August 17, 2018 and messaging data from prior phones may not have been carried over to the new phone. Furthermore, the custodians acknowledge that they have no estimate of the number of texts that might be captured and reviewed for relevance under Plaintiffs' proposed search method, nor do they seem to have explored other means of capturing and filtering the data more cost-effectively, so the Court cannot assess the time or cost for that aspect of the production process. The Court accepts in the abstract that the imaging may be costly, but it has no information on how custodians calculated their cost estimate or how much it might cost any particular custodian.

That said, the Court agrees with the custodians that of all the players in this mix, the individual custodians are least equipped to bear the financial burden of having their cell phones imaged. As discussed below in Section III.D., the Court will compel the custodians to search for and produce text messages within certain parameters, and to preserve data in the event this production, or other discovery, reveals a basis to expand the search. Consequently, the Court directs Plaintiffs' counsel, Hormel's counsel, and the custodians' counsel to meet and confer regarding which devices should be imaged, or from which devices text messaging data should be extracted by other means, taking into account the time period during which those devices were in service and whether older data was carried over.

***13** In addition, to the extent the result of those discussions results in the imaging of any cell phones, or the forensic extraction of text messaging data by other means, the Court exercises its discretion and orders that the reasonable costs associated with that imaging or data extractions must be split equally between the Class Plaintiffs, on the one hand, and Hormel, on the other. The Court further orders that the reasonable costs associated with conversion and storage of any data obtained from those phones as well as conversion and storage of any data obtained from archives or cloud storage be borne equally by the Class Plaintiffs and Hormel. The Court finds this cost-sharing arrangements appropriate as to Plaintiffs because Rule 45(d)(1) clearly places on the party serving the subpoena the obligation to avoid imposing undue burden or expense on the person subject to the subpoena. It finds this arrangement appropriate as to Hormel because its BYOD policy not only allowed but to some extent financially supported the use of personal cell phones for work purposes, and so it is appropriate that it share in the cost of harvesting and storing the data so that it can be ascertained whether there are relevant and responsive work-related texts.

The Court also recognizes that being deprived of a phone for more than a day either to mail it in and image it, or simply

image it, may be inconvenient, and perhaps burdensome. But no evidence suggests which custodians will have to mail their phones rather than drop them off in person, or that it will take more than a day rather than three hours to image any custodian's phone. Nor is it clear that the custodians have explored alternatives to "mailing in" their phones. [6] . In short, the Court cannot sustain these aspects of each custodian's burden in the absence of evidence showing how the burden actually, rather than theoretically, would fall on the custodians and that the custodians have diligently explored alternatives that would reduce that burden.

As for the privacy concerns, the Court accepts as a matter of common knowledge that modern smart phones store a tremendous amount of their owner's personal, private, or confidential information. But the custodians have not persuaded the Court that that concern cannot be managed through targeted searches. Plaintiffs allege that forensic imaging vendors can target specific phone applications or types of data, in which case a vendor could image only the messages saved in communication apps on the phone. (Tr. at 52.) The custodians have done nothing to persuade the Court that they have explored the options for more targeted data extraction and come up empty-handed. Furthermore, the Court is aware that reputable forensic imaging vendors employ strict protocols to protect data within their control, and in any event, as will be discussed below, the Court's order will provide that only relevant and responsive information will be delivered to Plaintiffs, reducing the risk that a custodian's personal confidential information will be transmitted. Finally, the information may be produced subject to the protective order in this case, further minimizing any risk of public disclosure of private information. Thus, the Court finds the custodians' privacy concerns, while understandable, are manageable and not a basis for declining to enforce Requests Nos. 1 and 5 of the subpoenas.

**D. Whether the Court Should Decline to Enforce Requests Nos. 1 and 5 on the Grounds That They Are Overly Broad and Seek Irrelevant Information**

The Court concludes that while Requests Nos. 1 and 5 seek some relevant information, they extend beyond the bounds of relevance and must therefore be narrowed to target relevant and proportional information.

The Court observes at the outset that it is unclear on the face of Request No. 1 whether it seeks the production of all texts on the custodians' phones exchanged with other Hormel employees, Defendants' employees, and employees of other pork integrators (defined as any of the Defendants and any of over sixty other named companies), regardless of content, or whether the phrase "about supply and demand conditions in the Pork industry" at the end of the request qualifies and limits not only the second clause of the request but the first as well. (Bourne Decl. Ex. 17 Definitions ¶ 14, Request 1.) Request No. 5 does not, on its face, actually seek texts, but seeks information from which a "forensic vendor" could gain access to all archived copies of the custodians' cell phone data, including relevant text messages, in locations like cloud backups, older cell phones, or non-internet archives, without regard to subject matter. (Bourne Decl. Ex. 17 Request 1.)

***14** Plaintiffs proposed a search method that sheds some light on their intended scope. Plaintiffs propose that *all* texts exchanged with any number on a list of 781 phone numbers associated with individuals affiliated with Hormel or any other Defendant or any of the other identified pork integrators, be produced without regard to content. As to all other texts, they propose a key term search, the results of which would be reviewed for relevance by the custodians' counsel. (Bourne Decl. ¶ 12 [ECF No. 887], Ex. 16 [ECF No. 888-2].) This same protocol would, presumably, be applied to both data residing on the cell phones and data gathered from other locations pursuant to Request No. 5. Plaintiffs argue that all texts exchanged with any of the 781 numbers are presumptively relevant as "work-related texts," so they do not need relevance review before production, while any other texts are less likely to be relevant, so a keyword search to narrow the universe, followed by a relevance review of all "hits" is appropriate. (Pls.' Mem. at 15.)

Unquestionably some of the information encompassed by each request is relevant. Request No. 1 seeks text messages between Defendants' employees about pork supply, demand, and pricing (the subject matter of the conspiracy) during the relevant time-period, and between Defendants and other pork integrators. Plaintiffs argue these messages are relevant to help Plaintiffs understand the tone, language, and content of Defendants' communications about that subject matter, and potentially to reveal substance of the alleged conspiracy, and neither Hormel nor the custodians argue persuasively to the contrary. Request No. 5 similarly includes within its scope some relevant information, insofar as the custodians have changed phones and prior relevant messages may be saved in the custodians' archives, cloud backups, or older phones. While Hormel and the custodians dispute whether it is likely that any relevant texts will be found on the cell phones, they

do not seriously disagree that *if* there are texts pertaining to pork supply, demand, and pricing, that were sent during the relevant time period among Hormel employees, or between Hormel employees and other pork integrators, those texts would likely be relevant and responsive to discovery in this case.

But not all texts to all individuals on the 781 phone numbers connected to Defendants and pork integrators will involve this subject matter, and Plaintiffs do not satisfactorily explain why the Court should presume otherwise. The evidence does not show that the custodians texted those numbers only (if at all) about the relevant subject matter, as opposed to other work-related topics or even non-work topics like social plans. Just because there may be some relevant texts within a data set does not make all texts within that set presumptively relevant.

For the same reasons, Request No. 5 also sweeps too broadly in effectively demanding access to all archived text messaging data from all of the custodians' phones.

Furthermore, the time-period of the requested production, January 1, 2008 – August 17, 2018, was not tailored to the job responsibilities of the individual custodians, and therefore also is overly broad. The custodians held different job duties at different times throughout this period, and some of them retired during that period. (*See, e.g.*, Hormel Ex. 10 at 5, Ex. 11 [ECF Nos. 929-9, -10].) The parties designated each custodian based on relevant job duties held during specific subsets of the period of the alleged conspiracy. (*See, e.g.*, Hormel Ex. 8 at 2, Ex. 10 at 5, Ex. 11 [ECF Nos. 929-7, - 9, -10].) Their text data within those time periods are potentially a source of relevant communications, but those distinctions were ignored by Plaintiffs' subpoena requests, which were "one-size-fits-all." While that uniform time frame makes good sense for efficient conduct of party discovery, it is not as appropriate for individual custodians whose confidential personal information is at stake, nor is it proportional in view of the narrower time periods within which these individuals were in relevant roles and therefore may have had relevant communications (if at all).

***15** Accordingly, the Court will enforce the subpoenas as to Requests Nos. 1 and 5 (for all custodians except Chenowith) and orders the custodians (other than Chenowith) to search for and produce relevant text messages within a modified scope and subject to a modified search protocol, as follows: Each subpoena will be limited to the time period or periods within which that custodian held the position that resulted in his or her being identified as a custodian. Plaintiffs' counsel, Hormel's counsel, and the custodian's counsel shall meet and confer to confirm they have a common understanding on that subject. The text messaging data, including data extracted from the custodians' current phones, older phones, or archive or backup data from those phones, must be searched first to identify all texts that were sent to or received from any number on the list of 781 phone numbers identified by Plaintiffs within the time period or periods pertaining to that custodian. The number of resulting texts for each custodian must be reported to Plaintiffs' counsel. The custodian's counsel may then choose to manually review all of the resulting texts for that custodian for relevance; however, the custodian's counsel may meet and confer with Plaintiffs' counsel about a threshold volume of messages for a custodian that would trigger the application of search terms (to be negotiated between counsel), the results of which further filtering would then be reviewed for relevance by the custodian's counsel.

The Court does not rule out the possibility that review by Plaintiffs of the resulting text message production, or other discovery in this case, may provide a more concrete basis upon which to justify an expanded search for relevant messages beyond what the Court has permitted here. Accordingly, the custodians are further ordered to preserve all text messaging data and all archived and cloud-stored text messaging data for the period January 1, 2008 – August 17, 2018, until December 31, 2022, or until such other date as may be agreed upon by the parties or ordered by the Court. Relatedly, Chenowith is also ordered to preserve all text messages, including all archived and cloud-stored messages, from the period January 1, 2008 – August 17, 2018 (or, in the alternative, to arrange at Hormel's and Plaintiffs' shared expense to have such text messages imaged and preserved).

## IV. Hormel's Preservation Duty Did Not Extend to Imaging Personally-Owned Cell Phones and Archiving Cloud Backups

Plaintiffs assert that Hormel knew or should have known that its custodians were conducting substantive work-related business over text message so that it was under an obligation to image those phones and preserve cloud backups at the start of the litigation; they request a declaration that Hormel had an obligation at the start of litigation to preserve its custodians' text message content by imaging their phones and preserving their cloud backup data, and an order compelling Hormel to do so now. (Pls.' Mem. at 11–14.) The duty to preserve evidence arises when a party knows or should have

known that the evidence in its control is relevant to current or reasonably foreseeable litigation, at which point the party must take reasonable steps to preserve it. *Paisley Park*, 330 F.R.D. at 232; Fed. R. Civ. P. 37(e). "The duty to preserve relevant evidence must be viewed from the perspective of the party with control of the evidence." *Paisley Park*, 330 F.R.D. at 232. The duty "extends to those persons likely to have relevant information – the key players in the case, and applies to unique, relevant evidence that might be useful to the adversary." *Id.* at 233.

Whether a party has taken reasonable steps to preserve information is a factual inquiry considering the context of the case, the information sought, and the steps taken. *See id.* at 233–35 (holding that the defendants unreasonably failed to preserve their personal text messages by purging their phone data even though they texted for work purposes and knew of pending litigation involving their business); *In re Petters Co., Inc.*, 606 B.R. 803, 822 (Bankr. D. Minn. 2019).

Here, however, the Court has found Hormel did not control the text messages on the personally-owned cell phones of its custodians. It did communicate litigation holds to reasonably anticipated custodians and Plaintiffs have not shown that those holds were inadequate to communicate to those custodians that they should preserve relevant information under their own control, including text messaging data. (Hormel Mem. at 21–22.) The Court therefore denies Plaintiffs' motion for a "declaration" that Hormel had a duty to do more than it did. [7] Plaintiffs' concerns for preservation going forward are addressed by the Court's order described above in Section III.D.

***16** Accordingly, based on all the files, records, and proceedings, **IT IS HEREBY ORDERED** that Class Plaintiffs' Motion to Compel Hormel To Produce Responsive Text Message Content and to Enforce Subpoenas to Hormel Custodians [ECF No. 883] is **GRANTED IN PART** and **DENIED IN PART** as described fully herein.

**All Citations**

Slip Copy, 2022 WL 972401

## Footnotes

1 Exhibit 2 to the Bourne Declaration [ECF No. 888-2 at 12–162] are the full letters and objections transmitted to Plaintiffs' counsel by the custodians through their counsel. Exhibit 1 to that declaration [ECF No. 888-2 at 1–11] is a chart created by Plaintiffs' counsel summarizing the responses. The Court notes that none of the subpoena responses included (or were required to include) sworn declarations by the custodians.

2 The conspiracy allegedly began in 2009 and none of the parties address pre-BYOD policy communications.

3 Hormel and the custodians object at the outset that Plaintiffs did not engage in good faith meet-and-confer efforts prior to filing this motion. (Hormel Mem. at 27; Custodians' Mem. at 10–11 [ECF No. 925].) "Before filing a motion ... the moving party must, if possible, meet and confer with the opposing party in a good-faith effort to resolve the issues raised by the motion," and certify the same to the Court alongside its motion. D. Minn. L.R. 7.1, 37.1; *see also* Fed. R. Civ. P. 37(a)(1). This obligation is only fulfilled when parties have engaged in a genuine and good-faith discussion about each discovery request that is in dispute. *Mgmt. Registry, Inc. v. A.W. Companies, Inc.*, Case No. 17-cv-05009 (JRT/KMM), 2019 WL 2024538, at *1 (D. Minn. May 8, 2019).

Based on the record of the parties' communications, the Court overrules this objection. Before this motion was filed, Plaintiffs and Hormel exchanged numerous emails and letters arguing their opposing positions regarding whether Hormel had control over its custodians' personal cell phones, whether it met its obligations to preserve text message data, and whether it had to produce that data. (*See* Bourne Decl. Exs. 6–10 [ECF No. 888-2].) In addition, the record reflects that after the custodians received the subpoenas, their counsel "participated in meet and confer communications with opposing counsel including four letters, several e-mails, and two telephone conferences" on June 1 and August 2. (Stephens Decl. ¶¶ 9–18.) The parties'

descriptions of their telephone meetings, and the letters and emails in the record, show an effort by both to explain their positions and concerns, and explore possible compromises, but finally conclude that they were too far apart. (*Id.*; Exs. A–G.) The exchanges show both sides engaged in a genuine discussion over these issues but refused to concede their positions after bringing factual and legal arguments to bear. This satisfies the meet-and-confer requirement.

4 Hormel raises objections to the subpoenas in its memorandum. (Hormel Mem. at 28–29.) Hormel is not subject to the subpoenas nor moving for a protective order, so it lacks standing to quash or modify the subpoenas. *Shukh v. Seagate Tech., LLC*, 295 F.R.D. 228, 236 (D. Minn. 2013). The Court will consider its arguments only to the extent they shed additional light or support for or against the custodians' objections.

5 The Court assumes that this estimate does not include the cost for imaging the five phones that were already imaged by Hormel. Obviously, if it does, this total cost estimate overstates that aspect of the burden.

6 Plaintiffs suggest, for example, that it is possible to mail imaging kits to custodians for whom mailing their phone or travelling to Hormel would be burdensome. (Tr. at 50.) To the extent the custodians are arguing that having to mail in their phones is the necessary result of working with Hormel's vendor, it undercuts their complaint regarding monetary burden, as it suggests strongly that Hormel and not the individual custodians will be paying for the imaging in any event.

7 The Court does not address Hormel's argument that Plaintiffs did not follow proper procedure to request a declaratory judgment. (Hormel Mem. at 18.)

End of Document

2021 WL 831025
Only the Westlaw citation is currently available.
United States District Court, C.D. California.

BENEBONE LLC

v.

PET QWERKS, INC., et al.

Case No. 8:20-cv-00850-AB-AFMx
|
Filed 02/18/2021

**Attorneys and Law Firms**

Andrea Levenson, Jason T. Lao, Haynes and Boone LLP, Costa Mesa, CA, Joseph Lawlor, Pro Hac Vice, Richard Rochford, Pro Hac Vice, Haynes and Boone LLP, New York, NY, Kenneth G. Parker, Gibson Dunn and Crutcher LLP, Irvine, CA, for Benebone LLC.

Ali Razai, Adam R. Aquino, Steven J. Nataupsky, Knobbe Martens Olson and Bear LLP, Lewis E. Hudnell, III, Natalya Vasyuk, Rolando Javellana Tong, Manning and Kass Ellrod Ramirez Trester LLP, Irvine, CA, Benjamin B. Anger, Knobbe Martens Olson and Bear LLP, San Diego, CA, Daniel I. Hwang, Pro Hac Vice, Joseph F. Arand, Pro Hac Vice, Michael T. Murphy, Pro Hac Vice, Global IP Counselors LLP, Washington, DC, for Pet Qwerks, Inc., et al.

**Proceedings (In Chambers): Order Granting Defendants Pet Qwerks, Inc. and Doskocil Manufacturing Company, Inc. D/B/A Petmate's Motion to Compel Plaintiff Benebone LLC's Production of Slack Communications (ECF No. 88)**

The Honorable: ALEXANDER F. MacKINNON, U.S. Magistrate Judge

***1** Defendants Pet Qwerks, Inc. and Doskocil Manufacturing Company, Inc. d/b/a Petmate (collectively, "Defendants"), have filed a motion seeking to compel Plaintiff Benebone LLC ("Benebone") to be required to produce Slack communications responsive to Defendants' document requests. For the reasons provided below, Defendants' motion is **GRANTED** to the extent set out herein.

## I. Background

Slack is a cloud-based software system that allows a company to organize its electronic discussions into user-defined categories called "channels." Plaintiff Benebone uses Slack, as well as standard email, for its internal communications.

During the parties' early discussions regarding discovery of electronically stored information, Defendants sought to include Benebone's Slack messages in the parties' Stipulated ESI Order, and Benebone took the position that Slack messages should be excluded from discovery. The parties requested a telephonic discovery conference with the Court to address this, and each side submitted a short brief outlining its position. (*See* ECF Nos. 60-63.) Defendants included a declaration from Michael Gutierrez, Director of Forensic Services at Xact Data Discovery, an e-discovery vendor that Defendants have engaged for this case. During the telephonic discovery conference on November 23, 2020, the Court concluded that Benebone's Slack messages are relevant, but it lacked sufficient information to determine whether Slack discovery would be proportional to the needs of the case. Accordingly, the Court ordered the parties to meet and confer further regarding possible Slack production after Benebone had obtained additional information about its Slack account and what would be required to search and produce responsive Slack messages.

As part of the meet and confer process, Benebone informed Defendants that its Slack account contains approximately 30,000 messages. Benebone also estimated that it would cost $110,000 to $255,000 to extract, process, and review these 30,000 messages. Based on these cost estimates, Benebone maintained that searching and producing documents from Slack would be an undue burden and would not be proportional to the needs of the case. Defendants disagreed and filed the present motion to compel Benebone to produce its responsive Slack messages. (ECF No. 88.) The parties filed a joint stipulation pursuant to L.R. 37-2, as well as supplemental memoranda. (*See* ECF Nos. 89-92, 102-104.)

In connection with the motion to compel, Defendants submitted a second declaration from Mr. Gutierrez. In his declarations, Mr. Gutierrez stated that he has been involved in multiple lawsuits where Slack messages have been produced. He described a number of tools that software vendors have developed to streamline review and production of Slack messages and explained how extracting, processing, and reviewing Slack messages could take place using currently

available software tools. He also provided a cost estimate for doing so in this case. Mr. Gutierrez stated that Xact offers contract review attorneys at a rate of $40 per hour to conduct the first level review of Slack messages, and he provided a cost estimate of $22,000 for Benebone to find and produce its responsive Slack messages. Benebone, on the other hand, stood by its prior estimate of $110,000 to $255,000 based on a blended attorney rate of $400 per hour for Slack review. Benebone did not provide a declaration from an e-discovery expert to support its conclusions or respond to the evidence provided by Mr. Gutierrez.

***2** The Court held a Zoom hearing on February 3, 2021 regarding Defendants' motion to compel. Mr. Gutierrez attended the hearing and answered the parties' and the Court's questions under oath.

## II. Discussion

Federal Rule of Civil Procedure 26(b)(1) provides that a party 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[.]" Factors to consider include "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." *Id.* Discovery need not be admissible in evidence to be discoverable. *Id.* However, a court "must limit the frequency or extent of discovery otherwise allowed by [the Federal] rules" if "(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)." Fed. R. Civ. P. 26(b)(2)(C). Boilerplate or general objections are not appropriate, and a party's objections should be specific to each particular discovery request and be supported by evidence. *See* Fed. R. Civ. P. 34(b)(2). "Upon a motion to compel discovery, the movant has the initial burden of demonstrating relevance. In turn, the party opposing discovery has the burden of showing that discovery should not be allowed, and also has the burden of clarifying, explaining and supporting its objections with competent evidence." *United States v. McGraw-Hill Cos.*, 2014 WL 1647385, at *8 (C.D. Cal. Apr. 15, 2014) (citations and internal quotation marks omitted)). The Federal Rules of Civil Procedure must be "construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding." Fed. R. Civ. P. 1. [1]

Here, because Benebone uses Slack as part of its internal business communications, there is no real dispute that Benebone's Slack messages are likely to contain relevant information. The crucial issue is whether requiring Benebone to search for and produce responsive Slack messages would be unduly burdensome and disproportional to the needs of this case. In this regard, the Court relies on Mr. Gutierrez's testimony regarding the estimated cost and level of effort necessary for producing the Slack messages. Mr. Gutierrez was a knowledgeable and credible witness on this subject, and his declarations and testimony at the hearing were not rebutted by a Benebone witness.

***3** Mr. Gutierrez testified that third-party tools have been developed over the past several years for collecting and reviewing Slack messages and that review and production of Slack messages has become comparable to email document production through use of these tools. Mr. Gutierrez further testified that it likely would not be necessary for Benebone to search all its Slack messages. Instead, searches likely could be limited to certain Slack channels, users, or custodians – which could significantly reduce the volume of Slack messages requiring review. For instance, in this intellectual property case, it may not be necessary to extract and review messages in a Slack channel dealing with human resources issues.

Moreover, Mr. Gutierrez's declarations and testimony indicate that it is possible to conduct first level review of the pertinent Slack messages via contract attorneys for far less than Benebone's estimated blended rate of $400 per hour. Mr. Gutierrez testified that contract reviewers are available who are licensed attorneys at a rate as low as $40 per hour for first-level review. As discussed during the hearing, Mr. Gutierrez did not include any time or expense for second-level review by more experienced counsel. It is also possible that contract attorneys may cost somewhat more than the hourly rate used in his estimate. Thus, the Court finds that Mr. Gutierrez's estimate of $22,000 for Benebone to review and produce Slack messages is on the low side. However, Benebone's cost estimate of $110,000 to $255,000 for producing the Slack messages is substantially inflated due to its assumption of attorney review of all 30,000 Slack messages at a rate of $400 per hour. As noted above, Benebone did not provide an e-discovery declaration or testimony to support its cost estimate

or its position that producing the Slack messages represents an undue burden and is disproportional to the needs of this case.

**III. Conclusion**

Based on the evidence presented in the parties' briefing and at the hearing, the Court finds that requiring review and production of Slack messages by Benebone is generally comparable to requiring search and production of emails and is not unduly burdensome or disproportional to the needs of this case – if the requests and searches are appropriately limited and focused. Defendants' evidence supports this conclusion, and Benebone has responded largely with attorney argument but no witness or declarant on the e-discovery issues. E-discovery tools are available for this process, and the Slack messages to be reviewed can be narrowed based on the channels or users likely to have responsive information given the relevant issues in this case. Although Benebone makes cursory reference to other proportionality factors (*see* ECF No. 89 at 22.), its focus has been on the purported burdens associated with production of Slack documents and the fact that Benebone is a small company compared to Defendants. Nevertheless, Benebone seeks the full range of monetary damages in this case, plus injunctive relief against Defendants' accused products – sales of which are allegedly in the millions of dollars. As discussed herein, a focused search for and production of Slack messages is proportional to the needs of this case where Benebone regularly uses Slack messaging for internal business communications and users of Slack include Benebone's marketing director, COO, and CEO (who is also a named inventor on the three asserted design patents). Thus, the Court agrees with Defendants that e-discovery in this case shall include Benebone's Slack messages.

To be clear, the parties have not fully briefed, and the Court has not resolved by this order, the question of specific request categories and search methodologies to be used for identification, review and production of Benebone's Slack messages. To address what will be searched for and how the search will take place, the parties shall meet and confer no later than **March 5, 2021**. At least seven days before this meet and confer, Benebone shall provide to Defendants a list of its Slack channels, including the title and a brief description of each Slack channel, the number of messages in each Slack channel, the users associated with each Slack channel, and any other data that will assist the parties in tailoring the Slack review and production.

***4 IT IS SO ORDERED.**

**All Citations**

Slip Copy, 2021 WL 831025

## Footnotes

1 Slack is a relatively new communication tool, but a few published cases have addressed production of Slack messages. For example, in *Calendar Research LLC v. Stubhub, Inc.*, 2019 WL 1581406, at *4 (C.D. Cal. Mar. 14, 2019), the court granted the plaintiff's motion to compel production of defendants' remaining relevant Slack messages. Similarly, in *BidPrime, LLC v. SmartProcure, Inc.*, 2018 WL 6588574, at *2 (W.D. Tex. Nov. 13, 2018), the Court ordered production of remaining Slack messages because "they may be relevant and SmartProcure has not provided a specific objection to the contrary." *Id.* In *Milbeck v. Truecar, Inc.*, 2019 WL 4570017 at *3 (C.D. Cal. May 2, 2019), the court denied the plaintiff's motion for Slack production without prejudice, because of an imminent trial date.

End of Document

# Rule 502. Attorney-Client Privilege and Work Product; Limitations on Waiver

The following provisions apply, in the circumstances set out, to disclosure of a communication or information covered by the attorney-client privilege or work-product protection.

**(a) Disclosure Made in a Federal Proceeding or to a Federal Office or Agency; Scope of a Waiver.** When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if:

**(1)** the waiver is intentional;

**(2)** the disclosed and undisclosed communications or information concern the same subject matter; and

**(3)** they ought in fairness to be considered together.

**(b) Inadvertent Disclosure.** When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:

**(1)** the disclosure is inadvertent;

**(2)** the holder of the privilege or protection took reasonable steps to prevent disclosure; and

**(3)** the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26 (b)(5)(B).

**(c) Disclosure Made in a State Proceeding.** When the disclosure is made in a state proceeding and is not the subject of a state-court order concerning waiver, the disclosure does not operate as a waiver in a federal proceeding if the disclosure:

**(1)** would not be a waiver under this rule if it had been made in a federal proceeding; or

**(2)** is not a waiver under the law of the state where the disclosure occurred.

**(d) Controlling Effect of a Court Order.** A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding.

**(e) Controlling Effect of a Party Agreement.** An agreement on the effect of disclosure in a federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

**(f) Controlling Effect of this Rule.** Notwithstanding Rules 101 and 1101, this rule applies to state proceedings and to federal court-annexed and federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if state law provides the rule of decision.

**(g) Definitions.** In this rule:

**(1)** "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and

**(2)** "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.

### Notes

(Added Pub. L. 110–322, §1(a), Sept. 19, 2008, 122 Stat. 3537; Apr. 26, 2011, eff. Dec. 1, 2011.)

### Explanatory Note on Evidence Rule 502

The following explanatory note was prepared by the Judicial Conference Advisory Committee on Evidence Rules, revised Nov. 28, 2007:

This new rule has two major purposes:

1) It resolves some longstanding disputes in the courts about the effect of certain disclosures of communications or information protected by the attorney-client privilege or as work product—specifically those disputes involving inadvertent disclosure and subject matter waiver.

2) It responds to the widespread complaint that litigation costs necessary to protect against waiver of attorney-client privilege or work product have become prohibitive due to the concern that any disclosure (however innocent or minimal) will operate as a subject matter waiver of all protected communications or information. This concern is especially troubling in cases involving electronic discovery. *See, e.g., Hopson v. City of Baltimore*, 232 F.R.D. 228, 244 (D.Md. 2005) (electronic discovery may encompass "millions of documents" and to insist upon "record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation").

The rule seeks to provide a predictable, uniform set of standards under which parties can determine the consequences of a disclosure of a communication or information covered by the attorney-client privilege or work-product protection. Parties to litigation need to know, for example, that if they exchange privileged information pursuant to a confidentiality order, the court's order will be enforceable. Moreover, if a federal court's confidentiality order is not enforceable in a state court then the burdensome costs of privilege review and retention are unlikely to be reduced.

The rule makes no attempt to alter federal or state law on whether a communication or information is protected under the attorney-client privilege or work-product immunity as an initial matter. Moreover, while establishing some exceptions to waiver, the rule does not purport to supplant applicable waiver doctrine generally.

The rule governs only certain waivers by disclosure. Other common-law waiver doctrines may result in a finding of waiver even where there is no disclosure of privileged information or work product. *See, e.g., Nguyen v. Excel Corp.*, 197 F.3d 200 (5th Cir.

1999) (reliance on an advice of counsel defense waives the privilege with respect to attorney-client communications pertinent to that defense); *Ryers v. Burleson*, 100 F.R.D. 436 (D.D.C. 1983) (allegation of lawyer malpractice constituted a waiver of confidential communications under the circumstances). The rule is not intended to displace or modify federal common law concerning waiver of privilege or work product where no disclosure has been made.

*Subdivision (a)*. The rule provides that a voluntary disclosure in a federal proceeding or to a federal office or agency, if a waiver, generally results in a waiver only of the communication or information disclosed; a subject matter waiver (of either privilege or work product) is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary. *See, e.g., In re United Mine Workers of America Employee Benefit Plans Litig.*, 159 F.R.D. 307, 312 (D.D.C. 1994) (waiver of work product limited to materials actually disclosed, because the party did not deliberately disclose documents in an attempt to gain a tactical advantage). Thus, subject matter waiver is limited to situations in which a party intentionally puts protected information into the litigation in a selective, misleading and unfair manner. It follows that an inadvertent disclosure of protected information can never result in a subject matter waiver. *See* Rule 502(b). The rule rejects the result in *In re Sealed Case*, 877 F.2d 976 (D.C.Cir. 1989), which held that inadvertent disclosure of documents during discovery automatically constituted a subject matter waiver.

The language concerning subject matter waiver—"ought in fairness"—is taken from Rule 106, because the animating principle is the same. Under both Rules, a party that makes a selective, misleading presentation that is unfair to the adversary opens itself to a more complete and accurate presentation.

To assure protection and predictability, the rule provides that if a disclosure is made at the federal level, the federal rule on subject matter waiver governs subsequent state court determinations on the scope of the waiver by that disclosure.

*Subdivision (b)*. Courts are in conflict over whether an inadvertent disclosure of a communication or information protected as privileged or work product constitutes a waiver. A few courts find that a disclosure must be intentional to be a waiver. Most courts find a waiver only if the disclosing party acted carelessly in disclosing the communication or information and failed to request its return in a timely manner. And a few courts hold that any inadvertent disclosure of a communication or information protected under the attorney-client privilege or as work product constitutes a waiver without regard to the protections taken to avoid such a disclosure. *See generally Hopson v. City of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), for a discussion of this case law.

The rule opts for the middle ground: inadvertent disclosure of protected communications or information in connection with a federal proceeding or to a federal office or agency does not constitute a waiver if the holder took reasonable steps to prevent disclosure and also promptly took reasonable steps to rectify the error. This position is in accord with the majority view on whether inadvertent disclosure is a waiver.

Cases such as *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) and *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323, 332 (N.D.Cal. 1985), set out a multifactor test for determining whether inadvertent disclosure is a waiver. The stated factors (none of which is dispositive) are the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issue of fairness. The rule does not explicitly codify that

test, because it is really a set of non-determinative guidelines that vary from case to case. The rule is flexible enough to accommodate any of those listed factors. Other considerations bearing on the reasonableness of a producing party's efforts include the number of documents to be reviewed and the time constraints for production. Depending on the circumstances, a party that uses advanced analytical software applications and linguistic tools in screening for privilege and work product may be found to have taken "reasonable steps" to prevent inadvertent disclosure. The implementation of an efficient system of records management before litigation may also be relevant.

The rule does not require the producing party to engage in a post-production review to determine whether any protected communication or information has been produced by mistake. But the rule does require the producing party to follow up on any obvious indications that a protected communication or information has been produced inadvertently.

The rule applies to inadvertent disclosures made to a federal office or agency, including but not limited to an office or agency that is acting in the course of its regulatory, investigative or enforcement authority. The consequences of waiver, and the concomitant costs of pre-production privilege review, can be as great with respect to disclosures to offices and agencies as they are in litigation.

*Subdivision (c)*. Difficult questions can arise when 1) a disclosure of a communication or information protected by the attorney-client privilege or as work product is made in a state proceeding, 2) the communication or information is offered in a subsequent federal proceeding on the ground that the disclosure waived the privilege or protection, and 3) the state and federal laws are in conflict on the question of waiver. The Committee determined that the proper solution for the federal court is to apply the law that is most protective of privilege and work product. If the state law is more protective (such as where the state law is that an inadvertent disclosure can never be a waiver), the holder of the privilege or protection may well have relied on that law when making the disclosure in the state proceeding. Moreover, applying a more restrictive federal law of waiver could impair the state objective of preserving the privilege or work-product protection for disclosures made in state proceedings. On the other hand, if the federal law is more protective, applying the state law of waiver to determine admissibility in federal court is likely to undermine the federal objective of limiting the costs of production.

The rule does not address the enforceability of a state court confidentiality order in a federal proceeding, as that question is covered both by statutory law and principles of federalism and comity. *See* 28 U.S.C. §1738 (providing that state judicial proceedings "shall have the same full faith and credit in every court within the United States . . . as they have by law or usage in the courts of such State . . . from which they are taken"). *See also Tucker v. Ohtsu Tire & Rubber Co.*, 191 F.R.D. 495, 499 (D.Md. 2000) (noting that a federal court considering the enforceability of a state confidentiality order is "constrained by principles of comity, courtesy, and . . . federalism"). Thus, a state court order finding no waiver in connection with a disclosure made in a state court proceeding is enforceable under existing law in subsequent federal proceedings.

*Subdivision (d)*. Confidentiality orders are becoming increasingly important in limiting the costs of privilege review and retention, especially in cases involving electronic discovery. But the utility of a confidentiality order in reducing discovery costs is substantially diminished if it provides no protection outside the particular litigation in

which the order is entered. Parties are unlikely to be able to reduce the costs of pre-production review for privilege and work product if the consequence of disclosure is that the communications or information could be used by non-parties to the litigation.

There is some dispute on whether a confidentiality order entered in one case is enforceable in other proceedings. *See generally Hopson v. City of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), for a discussion of this case law. The rule provides that when a confidentiality order governing the consequences of disclosure in that case is entered in a federal proceeding, its terms are enforceable against non-parties in any federal or state proceeding. For example, the court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party; the rule contemplates enforcement of "claw-back" and "quick peek" arrangements as a way to avoid the excessive costs of pre-production review for privilege and work product. *See Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (noting that parties may enter into "so-called 'claw-back' agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privilege documents"). The rule provides a party with a predictable protection from a court order—predictability that is needed to allow the party to plan in advance to limit the prohibitive costs of privilege and work product review and retention.

Under the rule, a confidentiality order is enforceable whether or not it memorializes an agreement among the parties to the litigation. Party agreement should not be a condition of enforceability of a federal court's order.

Under subdivision (d), a federal court may order that disclosure of privileged or protected information "in connection with" a federal proceeding does not result in waiver. But subdivision (d) does not allow the federal court to enter an order determining the waiver effects of a separate disclosure of the same information in other proceedings, state or federal. If a disclosure has been made in a state proceeding (and is not the subject of a state-court order on waiver), then subdivision (d) is inapplicable. Subdivision (c) would govern the federal court's determination whether the state-court disclosure waived the privilege or protection in the federal proceeding.

*Subdivision (e)*. Subdivision (e) codifies the well-established proposition that parties can enter an agreement to limit the effect of waiver by disclosure between or among them. Of course such an agreement can bind only the parties to the agreement. The rule makes clear that if parties want protection against non-parties from a finding of waiver by disclosure, the agreement must be made part of a court order.

*Subdivision (f)*. The protections against waiver provided by Rule 502 must be applicable when protected communications or information disclosed in federal proceedings are subsequently offered in state proceedings. Otherwise the holders of protected communications and information, and their lawyers, could not rely on the protections provided by the Rule, and the goal of limiting costs in discovery would be substantially undermined. Rule 502(f) is intended to resolve any potential tension between the provisions of Rule 502 that apply to state proceedings and the possible limitations on the applicability of the Federal Rules of Evidence otherwise provided by Rules 101 and 1101.

The rule is intended to apply in all federal court proceedings, including court-annexed and court-ordered arbitrations, without regard to any possible limitations of Rules 101 and 1101. This provision is not intended to raise an inference about the applicability of any other rule of evidence in arbitration proceedings more generally.

The costs of discovery can be equally high for state and federal causes of action, and the rule seeks to limit those costs in all federal proceedings, regardless of whether the claim arises under state or federal law. Accordingly, the rule applies to state law causes of action brought in federal court.

*Subdivision (g)*. The rule's coverage is limited to attorney-client privilege and work product. The operation of waiver by disclosure, as applied to other evidentiary privileges, remains a question of federal common law. Nor does the rule purport to apply to the Fifth Amendment privilege against compelled self-incrimination.

The definition of work product "materials" is intended to include both tangible and intangible information. *See In re Cendant Corp. Sec. Litig.*, 343 F.3d 658, 662 (3d Cir. 2003) ("work product protection extends to both tangible and intangible work product").

[During the legislative process by which Congress enacted legislation adopting Rule 502 (Pub. L. 110–322, Sept. 19, 2008, 122 Stat. 3537), the Judicial Conference agreed to augment its note to the new rule with an addendum that contained a "Statement of Congressional Intent Regarding Rule 502 of the Federal Rules of Evidence." The Congressional statement can be found on pages H7818–H7819 of the Congressional Record, vol. 154 (September 8, 2008).]

### References in Text

The Federal Rules of Civil Procedure, referred to in subd. (b)(3), are set out in this Appendix.

### Effective Date

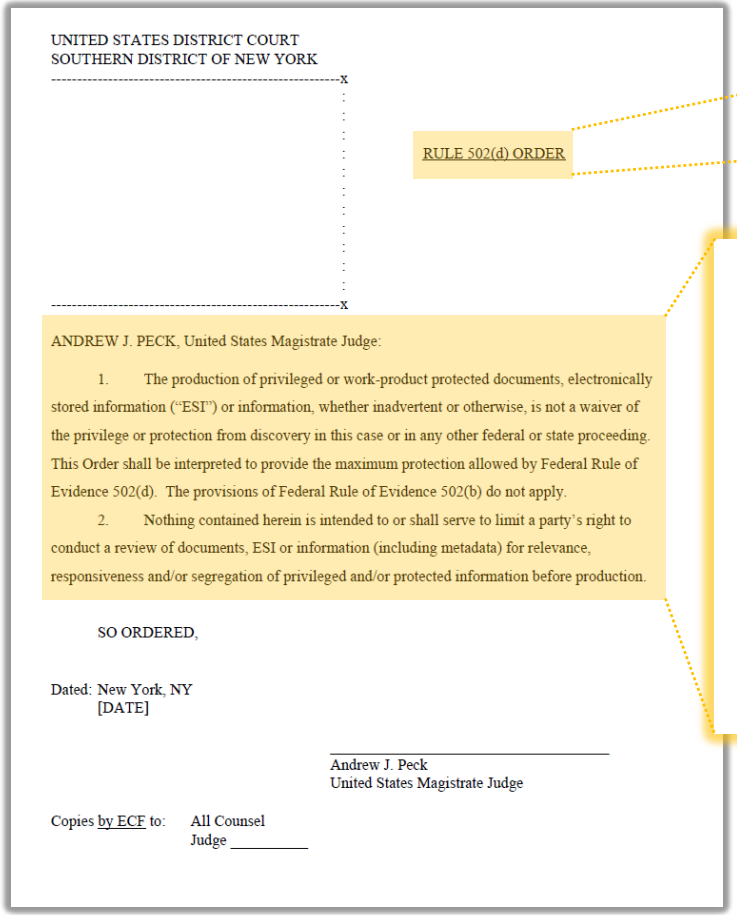
Pub. L. 110–322, §1(c), Sept. 19, 2008, 122 Stat. 3538, provided that: "The amendments made by this Act [enacting this rule] shall apply in all proceedings commenced after the date of enactment of this Act [Sept. 19, 2008] and, insofar as is just and practicable, in all proceedings pending on such date of enactment."

### Committee Notes on Rules—2011 Amendment

Rule 502 has been amended by changing the initial letter of a few words from uppercase to lowercase as part of the restyling of the Evidence Rules to make style and terminology consistent throughout the rules. There is no intent to change any result in any ruling on evidence admissibility.

‹ Rule 501. Privilege in General up ARTICLE VI. WITNESSES ›

# RULE 502(d) ORDER GOVERNING ESI



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

RULE 502(d) ORDER

----------x

ANDREW J. PECK, United States Magistrate Judge:

1. The production of privileged or work-product protected documents, electronically stored information ("ESI") or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). The provisions of Federal Rule of Evidence 502(b) do not apply.

2. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

SO ORDERED,

Dated: New York, NY
[DATE]

Andrew J. Peck
United States Magistrate Judge

Copies by ECF to: All Counsel
Judge _____

RULE 502(d) ORDER

ANDREW J. PECK, United States Magistrate Judge:

1. The production of privileged or work-product protected documents, electronically stored information ("ESI") or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). The provisions of Federal Rule of Evidence 502(b) do not apply.

2. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

DLA PIPER

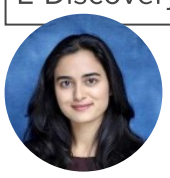
ANALYSIS

# The E-Discovery 502(d)ilemma: Attorneys Continue to Neglect an 'Amazing Level of Protection'

A lack of knowledge about FRE 502(d)—the easiest and most fool-proof of safety nets—has kept attorneys and judges from utilizing the valuable claw back provision. But Judges Andrew Peck and Paul Grimm warn that, with increasing digital evidence, such ignorance is tantamount to malpractice.

February 24, 2023 at 05:46 PM

E-Discovery



**Isha Marathe**
Legal Tech Reporter

Accidents happen—even to the most careful lawyers.

An attachment gets unintentionally tacked on to an email. A Slack message gets copied and pasted by an associate. In rarer, more notorious cases, an entire Dropbox file full of privileged goodies falls through the cracks and into the laps of opposing counsel.

Still, there are clawback or “snap-back” provisions in place for just such an occasion, allowing parties to recover the mistakenly shared information without having to waive attorney-client privilege. They consist of a handful of state rules and opportunities for counsel to set up their own discovery plans that include contingencies in case of a mistake.

But the easiest and most foolproof of safety nets has remained grossly underused for the 15 years it’s been available, federal judges told Legaltech News. And as the risk of inadvertent disclosures rises in tandem with digital collaboration and data review, it’s time for attorneys to examine the valuable rule collecting dust in their ESI toolboxes: Federal Rule of Evidence 502(d), which permits a federal court to enter an order that allows an attorney to claw back an inadvertent production regardless of their e-discovery practices, essentially, no questions asked.

## An Unopened Gift

Former U.S. District Judge Paul W. Grimm of the District of Maryland, now head of the Bolch Judicial Institute at Duke Law, and an architect of Rule 502(d), called the rule "a gift that has remained unopened."

"If you look at the advisory note under [Rule] 502, it is designed to do two things—have a national rule governing inadvertent disclosures. And No. 2, keep costs down in big data cases," Grimm said. "But 502(d) has just never really got the kind of publicity and acceptance within the bar that it really deserved."

Six provisions exist under Rule 502—a, b, c, d, e and f. Before Rule 502, courts relied on Rule 26 of the Federal Rules of Civil Procedure, which "was designed to allow parties in the kind of litigation that we have now, with large amounts of electronic information where the deadlines for completing discovery are tight, and you're dealing with large datasets … there are chances of something slipping through the cracks," Grimm noted. However, the caveat was that a nonwaiver agreement under Rule 26 remained true only between the two parties it was agreed by, making it vulnerable to a potential privilege waiver between other parties who don't share an agreement.

That's what makes 502(d) so unique in its scope, Grimm noted. On federal court order, it allows for clawback irrespective of how a disclosure happened, or why, and issues a complete nonwaiver of privilege. As digital evidence in legal proceedings was growing in the mid-2000s, courts were attempting to create better rules to prevent privilege waivers in case of such disclosures.

To be sure, before  FRE 502 and FRCP Rule 26, an inadvertent disclosure could be "like a death sentence to any lawyer that had that happen," Grimm added.

## Bad PR

So why has this "Get Out of Jail Free" card been relegated to what Grimm calls "Sedona nerds" and niche "e-discovery bubbles"? There is more than one answer, depending on who you ask.

For example, Craig Ball, a Texas attorney and forensic expert, said that it largely amounts to "ignorance, complacency and fear" among attorneys. "Many lawyers have no idea what you're talking about when you propose the rule," he said, "and those who do reason they've done just fine without one … whatever 502 does."

Meanwhile, former U.S. Magistrate Judge Andrew J. Peck, a 502(d) evangelist for nearly a decade and now senior counsel at DLA Piper, said some attorneys in asymmetric cases are "hoping" that a defense attorney without a 502(d) order is likely "to do something careless and you might be able to play 'gotcha.'"

On the other hand, it could simply result in a hassle and a lengthy discovery process if opposing counsel sends over a document under the protection of 502(d), but periodically keeps requesting the return of certain portions after they have been processed, Peck said.

Of course, the majority of lawyers, "nearly 40% to 50% have no clue what 502(d) is and why it's useful," he noted. A relatively small percentage of federal cases even go to trial, putting attorneys in the habit of waiting on reading the Federal Rules of Civil Procedure until they go to trial.

Not to mention, Rule 502 itself isn't part of the Federal Rules of Civil Procedure, often putting the onus on a judge to issue the order themselves to raise awareness, or rely on an attorney who is well-versed in changing e-discovery developments.

For Grimm, the problem lies beyond attorneys, and also with judges who tend to be unaware of 502(d). In fact, many district judges don't tend to deal with e-discovery in the same way that magistrate judges do, making them oblivious to the need of federal disclosure agreements, he told Legaltech News.

"When I was a district judge, I would talk to my colleagues and ask how many times have you had a real electronic discovery issue pop up? And they were like 'Once every few years.' Then you talk to the magistrate judges, you get a different story, because they're doing a lot more discovery," Grimm said. "Other judges don't really have that sort of muscle memory of civil procedure. They don't get that training consistently, and complicated discovery issues seem to be like a bunch of whining."

## Ignoring 502(d) 'Akin to Malpractice'

Over the last few months, Legaltech News has reported on several high-profile cases of inadvertent disclosures, from Alex Jones to Supreme Court Judge Clarence Thomas. David Cohen, practice group leader of records and e-discovery at Reed Smith, had told Legaltech News that accidental leaks are likely to grow.

"In the old days, you couldn't mistakenly turn over 10,000 documents because they were [in] hardcopy, so you could see 10,000 documents there," Cohen said. "Now, in the electronic days, you could have one little disk that you could send in a FedEx envelope that could literally have millions of pages of documents. [So] you might think you are turning over three documents, but you're turning over a million pages."

In spite of the many reasons why 502(d) has often remained out of touch, Peck stressed that the failure of attorneys and judges to "at least consider a 502(d) order is akin to malpractice."

Both Grimm and Peck said they rarely missed the opportunity to ask attorneys if they wanted to issue a 502(d) order, sometimes even taking the liberty to insert the order themselves. While some attorneys offered blank expressions signaling they had no idea what it was, others were hesitant to go through the trouble of using the provision when they didn't think there was enough ESI in a case to merit it.

"The higher the volume of digital evidence, the more likely it is that something is going to slip through, no matter how good the screening process for the privilege is," Peck said. "And as lawyers are dealing with new technology, a lawyer who is being cautious should want that extra protection of 502(d). Of course, if they don't know it exists, then no volume of evidence is going to make them ask."