

eDISCOVERY EXPERIENCE AND CAPABILITIES

2022 eDiscovery Case Law Year in Review

SIGNIFICANT DECISIONS TOUCHING ON ISSUES RELATED
TO THE PRACTICE OF ELECTRONIC DISCOVERY

EDITORS

John J. Rosenthal \ \ Editor in Chief

Jason D. Moore \ \ Lead Editor

CONTRIBUTING EDITORS

Bobby Malhotra

Matthew Poplawski

Tushar Vaidya

Karen Wagshul

CONTRIBUTORS

Shiza Arshad

Isabella L. Caito

Salah Muhiddin

Adam B. Shniderman

WINSTON
& STRAWN
LLP

eDISCOVERY
& INFORMATION
GOVERNANCE

Table of Contents

INTRODUCTION	5
PREDICTIONS FOR 2023	6
REGULATORY FOCUS ON COLLABORATION PLATFORMS, SHORT MESSAGE FORMATS, AND EPHEMERAL MESSAGING	9
SEC and CFTC Settlements.....	9
DOJ Indicates An Even More Expansive Stance On Unapproved Messaging Apps.....	10
PRESERVATION, SPOILATION, AND SANCTIONS	12
Calhoun v. Google LLC	12
Carty v. Steem Monsters Corp. (Discord)	12
Drips Holdings, LLC v. Teledrip LLC (Slack).....	13
Fast v. GoDaddy.com LLC (Facebook and Telegram).....	14
Gina Centner v TMG Utility Advisory Services (Preservation Letters Rejected)	16
In re Gold King Mine Release in San Juan County, Colorado	16
Henderson v. Waxspot Grp., LLC (Text Messages).....	17
Hollis v. CEVA Logistics U.S., Inc.....	18
Jones v. Riot Hospitality Grp. LLC (Text Messages).....	19
Meta Platforms, Inc. v BrandTotal, Ltd.	20
Red Wolf Energy Trading LLC v. Bia Capital Management LLC (Slack).....	21
Resolute Forest Products v. Greenpeace International (Skype, Text Messages).....	23
Schnatter v. 247 Group, LLC (Text Messages)	24
Twitter v. Musk (Signal)	26
TECHNOLOGY ASSISTED REVIEW	28
In Re Allergan Biocell Textured Breast Implant Products Liability Litigation.....	28
In re Diisocyanates Antitrust Litigation.....	29
Quirurgil v. Hologic, Inc.	31
SCOPE OF DISCOVERY/PROPORTIONALITY	33
In re 3M Combat Arms Earplug Products Liability Litigation	33
American Atheists, Inc. v. Rapert.....	33
Edwards v. McDermott International, Inc.....	34

Jim Hawk Truck-Trails of Sioux Falls, Inc. v. Crossroads Trailer Sales & Service, Inc.....	35
Mobile Equity Corp. v. Walmart, Inc. (Slack).....	36
Ravikant v. Rohde.....	37
Saint Clair County Employees’ Retirement System v. Acadia Healthcare	37
POSSESSION, CUSTODY, OR CONTROL.....	39
In re Pork Antitrust Litigation (Text Messages)	39
R & R Packaging, Inc. v. Evenflo Co., Inc.	40
Signify Holding B.V. v. TP-Link Research America Corp.....	40
Stafford v. Bojangles’ Restaurants Inc. (Text Messages)	41
SEARCH AND PRODUCTION.....	42
Benanav v. Healthy Paws Pet Insurance, LLC	42
Boyd v. Lazer Spot.....	42
Carl Zeiss Meditect, Inc. v. Topcon Medical Systems, Inc.	43
Equal Employment Opportunity Commission v. Qualtool, Inc.	43
Famulare v. Gannett Co., Inc.	44
Martley v. City of Basehor.....	44
Raine Group LLC v. Reign Capital.....	45
Robinson v. De Niro.....	45
Simon and Simon PC v. Align Technology, Inc.....	46
In re Telescopes Antitrust Litigation.....	46
Terpin v. AT&T Inc.	47
FORENSIC EXAMINATIONS.....	48
Aminov v. Berkshire Hathaway Guard Insurance Companies.....	48
Jordan Khan Music Co., LLC v. Taglioli	48
Juul Labs, Inc. v. Chou	49
TK Elevator Corp. v Abels & Schumacher Elevator Co.....	49
Stevens v. Sullum	50
RULE 34	52
D.M. v. County of Merced.....	52
Metro Service Group, Inc. v. Waste Connections Bayou, Inc.	53
Weatherspoon v. 739 Iberville, LLC.....	54
ESI PROTOCOLS	55

In re Actos Antitrust Litigation.....	55
DR Distributors, LLC v. 21 Century Smoking, Inc.	56
Equal Employment Opportunity Commission v. Scottsdale Healthcare Hospitals.....	56
In re Google RTB Consumer Privacy Litigation.....	57
In re Keurig Antitrust Litigation.....	57
Rekor Systems, Inc. v. Loughlin	59
Sure Fit Home Products, LLC v. Maytex Mills Inc.	59
Vasoli v. Yards Brewing Co.,	60
CROSS-BORDER DISCOVERY.....	61
Cadence Design Systems, Inc. v. Syntronic AB.....	61
Kashef v. BNP Paribas S.A.....	62
Philips Medical Systems (Cleveland), Inc. v. Buan.....	62
U.S. Moves toward new E.U.-U.S. Data Privacy Framework	63

Introduction

Winston & Strawn LLP's eDiscovery & Information Governance Group is pleased to present the following year in review of important decisions and developments concerning a wide variety of electronic discovery and cross-border discovery issues.

The past year has continued a multi-year trend—hastened by the COVID-19 pandemic—toward the dramatic expansion of collaboration and short message formats in discovery. In practice and in the case law, we observe that parties, courts, government agencies, and practitioners are all increasingly familiar—and struggling—with collaboration messaging platforms like Slack, Microsoft Teams, and Discord, and with app-based messaging ecosystems such as WhatsApp and Signal. These platforms are in common in many organizations, and consequently, in litigation, and each presents new challenges in terms of its preservation, collection, unitization, and production. The decisions in **Drips Holdings LLC v. Teledrip LLC**, **Red Wolf Energy Trading LLC v. Bia Capital Management LLC**, and **Mobile Equity Corp. v. Walmart Inc.** illustrate courts' recent focus on the preservation and production issues related to Slack, in particular. We anticipate continued focus on and disputes about the appropriate form of production for messaging platforms (i.e., individual message, 24-hour digest, or other unitization) to move to the forefront.

This year also saw a continuation of a troubling trend in the context of motions brought under Rule 37(e) over loss of ESI. While we perceive an uptick in the number of sanctions motions being brought, generally, we also note the increasing frequency with which judges and other discovery referees recommend or award “curative measures” under Rule 37(e)(1) that include evidentiary instructions to

the jury short of mandatory or permissive adverse inference instructions, including missing evidence instructions, and the opportunity to allow evidence about the loss to be placed before the jury. The instruction awarded in **Fast v. GoDaddy.com LLC** is illustrative of this trend. We are concerned that jurists are increasingly willing to entertain the prospect of messy, distracting, and potentially misleading “mini-trials” about ESI loss—something the framers of the 2015 amendment to Rule 37(e) were acutely attuned to and wanted to avoid.

On the topic of the 2015 amendments, we continue to observe that courts are struggling with how to apply the abstract notion of proportionality in practice. In part, this appears to stem from a continued failure of practitioners to properly support their arguments addressing the proportionality factors of Rule 26(b)(1)(B) with sufficient facts and evidence, leaving problem-solver jurists with little to go on but a meager record and intuition.

Finally, we witnessed a dramatic slowdown in the number of opinions on TAR, while observing TAR is becoming commonplace in document review – at least for prioritization and quality control. To that end, we still observe some decisions and regulators that are placing undue and unwarranted obligations regarding “transparency” or limitations of the use of TAR in conjunction with search terms.

Predictions for 2023

At the outset of the year, we wanted to take this opportunity to identify some trends that we anticipate in 2023 and beyond.

COLLABORATION PLATFORMS

We anticipate that we will continue to a great deal of focus on the discovery of collaboration platforms, including MS Teams and Slack. We believe that the discovery of such platforms will expand with additional decisions indicating that such ESI should be considered part of the discovery process. We also see the software providers in the space continuing to offer enhancements in the tools available to identify, collect, review and produce such collaboration-generated ESI. We do not, however, see a single set of case law developing around production format and anticipate that we will continue to see a wide variety of decisions regarding the appropriate unitization of messages for production (e.g., X-messages before and after; 24-hour segments; entire message chain, etc.)

PORTABLE /PRE-BUILT CLASSIFIERS

The days of a single TAR classifier designed for relevancy determinations are coming to a close. Customers are demanding that their analytics and review software be delivered with pre-built and portable classifiers that can be run simultaneously over the same data set to address not just relevancy, but also significance, confidentiality, privilege and key issue identifiers. Certain service providers, such as Reveal, have made great advances in this area in recent updates. It remains to be seen if the largest software provider (Relativity) will focus on this capability.

THIRD-GENERATION AI HITS ITS STRIDE

Over the last decade, artificial intelligence engines have largely been used by lawyers in the area of e-discovery, with more advanced neural network AI engines remaining empty promises in terms of realistic deliverables beyond search and production. A wide variety of 3rd generation AI engines are now ready for prime time for use in a wide variety of legal tasks to include legal research, basic legal document drafting, document analysis, and contract management. The maturity of these engines is quite disparate, but we are likely to see numerous offerings in the legal industry this year and coming years. Adoption of these AI engines within the legal industry is very low at this point, but likely to gain speed rapidly through the year. Winston & Strawn has already contracted with a leading provider with hopes to integrate their advanced AI engine into a wide variety of workstreams. More to come!

INFORMATION GOVERNANCE COMEBACK

Information Governance has largely remained elusive for many organizations beyond those key documents relating to organization governance, accounting, and human relations. The primary reason why is quite simple: information governance requires classification of records in order to manage them through their lifecycle. To date, AI engines have not been able reliably to solve the classification problem, although we are optimistic third-generation AI engines will deliver in this area. With this said, Microsoft's information governance tools built into its MS Office 365 have finally

reached a point of maturity where they can support automated (or semi-automated) classification and management of custodial based documents at a lower price-point. With additional pressures from cyber security and privacy to limit the amount and time period of records held (more on that below), we anticipate this new functionality within MS Office 365 has as now enabling organizations to revisit their approach to information governance.

LEGACY DATA RETIREMENT

Relatedly, with data privacy breaches and cyber security attacks on the rise, it is not surprising that organizations are making their prevention an operational imperative and that an increasing number are focusing on the retirement of legacy applications and their data. Legacy systems that have exceeded their “end of life” dates, with their often-outdated technology and large volumes of data – including data subject to privacy and consumer protection regulations – often are particularly vulnerable to attacks from cyber criminals. With the average cost of a single data breach more than \$4.3 million, it makes sense that organizations are focusing their efforts on removing these vulnerabilities from the equation. Data that you don’t have can’t be stolen.

With more jurisdictions implementing CCPA-like data privacy laws, we expect to see increased focus in this area in 2023 and beyond. Of course, legacy retirement is not without its challenges, particularly where an organization must balance the needs of complying with internal or regulatory records retention requirements and also the preservation of records under a continuing duty to preserve for active or reasonably foreseeable litigation. To help ensure legacy retirement is performed defensibly, we believe more and more organizations increasingly engaging will expand the trend of engaging cross-functional teams, including, without limitation, IT, legal e-discovery, technical e-discovery, records management/information governance, privacy,

security, and regulatory compliance. Adopting such a multidisciplinary approach gives an organization the greatest chance of developing, documenting, and executing defensible legacy retirement plans while minimizing vulnerabilities to breach and cybercrimes, reducing legal and regulatory risks, reducing costs, and ensuring continued compliance with preservation obligations.

MOVE TO THE CLOUD

The transition from on-premise and private clouds to public / vendor-based clouds will continue at a rapid pace, and this transition will continue to raise a host of e-discovery issues, including preservation by cloud-providers, defensible migration, and third-party discovery. Here, issues of possession, custody, and control will continue to be important for organizations, and we believe results will be increasingly dependent upon whether the data sits within a “practical ability” or a “legal right to obtain” jurisdiction. International data issues may also be implicated depending upon whether the underlying ESI resides and/or is accessed.

FORENSICS TO REMOTE COLLECTION

The need to conduct formal forensics in the context of e-discovery continues to be on the decline, with noted exceptions for mobile devices. The ability to conduct remote collections within MS Office 365 and Google Vault continues to be on the rise. Organization should have in place processes and procedures for the collection and transfer of data from these platforms.

CONTINUED RISE OF NON-CUSTODIAL DISCOVERY

Several commentators in the industry have asked whether custodial-based discovery is dead. Our answer, based on both our experience and our read of information trends: far from it. With this said, we are seeing a rise in non-custodial discovery particularly in the space of asymmetrical litigation.

Class action and MDL plaintiffs' firms are engaging in more discovery focused on non-custodial sources and sources that stretch the notion of a "custodian" to the breaking point (e.g., Jira, Quip, Sharepoint). We recommend that producing organizations should be prepared for such discovery, including a plan for how to preserve, collect, and produce from such sources.

YET MORE CONFUSION ON INTERNATIONAL CROSS-BORDER TRANSFERS

The third version of a transfer mechanism between the EU and the US now announced – the E.U.-U.S. Data Privacy Framework mechanism is likely to receive an adequacy decision sometime next summer. With this said, it is only a matter of time before the new Framework is subject to attack by activists such as Max Schrems. Organizations should be very cautious about adopting this mechanism as a means for data transfers until it has had a chance be judicially reviewed. As a result, standard contractual clauses will continue to reign supreme as the primary method of data transfers, now further complicated by unclear guidance from the EU regarding the relatively new requirement for Data Transfer Impact Assessments. To further muddy the water on international data transfers, France appears to be serious about putting some teeth behind its newly revised blocking statute, requiring regulatory notice prior to transfers and insisting upon discovery via the Hague Convention. We are also likely to see further guidance from the Peoples Republic of China regarding how they intend to interpret and enforce their web of various privacy, cyber, and security laws that appear to be intended to preclude the transfer of data outside of its borders.

AUTOMATED LEGAL HOLD PRESERVATION TOOLS

In the past, the mention of "automated legal hold tools" brought to mind technology for creating, issuing, tracking, and managing legal hold notices. Such technology solved the challenges associated with all the manual work attendant thereto. Recent years, however, have seen the arrival of new legal hold automation tools to automate the process for preserving ESI. These tools are being heralded for, among other things, addressing the risks and challenges attendant to such current preservation practices as suspending automated ESI deletion policies and custodial self-preservation. They allow IT administrators to automate the preservation of custodial ESI generated by, or stored within, a given application by preventing users (most likely the custodians) from deleting or modifying the ESI (including its related metadata) or, alternatively, maintaining a copy of the original version of ESI in a secure location of the application, even if the custodians delete or modify the original version. Examples include, without limitation, MS Office 365, which makes available the ability to implement custodial preservation across Outlook e-mail, Teams Chats, and OneDrive content; and Google Suite, which has similar functionality within its Google Vault feature; and a growing number of third-party tools that can "reach into" cloud provider platforms like Office 365, Google, and Salesforce to initiate preservation-in-place. Over the next several years, we anticipate continued development of, and increased functionalities in these tools, along with increased adoption by organizations. We also anticipate, eventually, decisional case law on evaluating preservation questions around the use of these tools. For now, we caution organizations to think carefully about their policies, practices, and related documentation around the implementation of automated ESI preservation tools.

Regulatory Focus on Collaboration Platforms, Short Message Formats, and Ephemeral Messaging

A recent wave of enforcement actions against leading regulated financial institutions related to the use of unapproved messaging applications provides an important message from the Securities and Exchange Commission (“SEC”) and the Commodity Futures Trading Commission (“CFTC”). Moreover, the Department of Justice (“DOJ”) recently issued a memorandum indicating that (among other things) the use of such applications by any companies—not just regulated institutions—could be problematic in the context of criminal investigations.

Collectively, the SEC and CFTC’s enforcement actions levied \$1.8 billion of civil monetary penalties against 16 financial institutions for not prohibiting, and in some cases knowingly allowing, the use of messaging applications for business purposes that did not comply with the recordkeeping obligations applicable to those institutions. All companies—whether regulated or not—should therefore ensure that they are able to preserve communications and records that are required by applicable laws and consider addressing the use of various messaging applications for business-related communications in their policies and procedures.

SEC AND CFTC SETTLEMENTS

On September 27, 2022, the SEC issued and published settlement orders against 11 leading financial institutions and their affiliates (including 15 broker-dealers and one investment adviser) for violating certain recordkeeping requirements and for failures to supervise, imposing civil monetary penalties that collectively exceed \$1.1 billion. On the same day, the CFTC ordered 11 swap dealers and

futures commission merchants (“FCMs”) to pay a total of \$710 million dollars in fines for similar violations.

These enforcement actions relate to alleged violations of recordkeeping requirements of Rule 17a-4(b)(4) under the Securities Exchange Act of 1934 (the “Exchange Act”), Rule 204-2(a)(7) under the Investment Advisers Act of 1940 (the “Advisers Act”), and Rules 1.35, 23.201, and 23.202 under the Commodity Exchange Act (the “CEA”). These regulations generally require the regulated entities to preserve communications and other documents related to their regulated businesses. However, according to the SEC and CFTC, employees across all levels of seniority frequently used unapproved methods of communication for business purposes, including WhatsApp, personal email, and text messages, which were generally not monitored, subject to review, or archived.

Additionally, certain applications used by employees at the financial institutions, including Signal, WhatsApp, and Telegram, possess self-deleting functionalities, making it impossible for the companies to produce records to the government in response to a request for documents or subpoena. Furthermore, in one instance, the CFTC found that heads of trading desks explicitly requested that their subordinates delete business communications taking place on personal devices through unapproved applications. As a result, the SEC and CFTC found that the financial institutions failed to maintain thousands of business-related communications, including communications related to investment strategy, client meetings, and market activity.

The SEC and CFTC also found that the widespread use of unapproved communication methods violated the regulated entities' internal policies and procedures, which generally prohibited business-related communication taking place via unapproved methods.

Separately, the SEC and CFTC found that the financial institutions failed to adequately supervise their regulated businesses due to the widespread nature of these recordkeeping violations. Indeed, in certain instances, the SEC and CFTC found that the supervisors responsible for implementing and enforcing policies and procedures related to recordkeeping requirements were themselves using unapproved methods of communication and/or personal devices for business purposes.

As part of the settlements and in addition to the civil monetary penalties described above, the SEC required each respondent to hire a compliance consultant, who must review each institution's recordkeeping-related compliance programs and submit a report to SEC staff. The compliance consultant must also conduct a follow-up evaluation one year after the initial report is submitted to the SEC and issue a second report detailing the institution's progress toward improving its recordkeeping compliance program. Each institution must also conduct an internal audit into the same issues and submit a report to SEC staff. Additionally, for two years, each institution must notify SEC staff of any disciplinary measures imposed on employees related to recordkeeping issues.

The CFTC required each institution to conduct a similar review of its recordkeeping compliance program, but required the respondents themselves to conduct this review rather than an independent consultant. Additionally, similar to the SEC, the CFTC required each institution to conduct a one-year evaluation and assessment of its recordkeeping compliance programs, and to notify


CFTC staff of any disciplinary measures taken against employees related to recordkeeping issues.

DOJ INDICATES AN EVEN MORE EXPANSIVE STANCE ON UNAPPROVED MESSAGING APPS

While the SEC and CFTC enforcement actions targeted registered entities subject to onerous recordkeeping obligations, the DOJ indicated in a memorandum on Corporate Criminal Enforcement Policies, dated September 15, 2022, that it may hold all corporate entities to a similar standard. Specifically, the DOJ stated that, moving forward, "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." Furthermore, the enforcement of existing policies and training will be taken into account when considering whether to grant cooperation credits to a corporation being investigated by the DOJ.

The DOJ's memorandum does not create explicit legal obligations for companies to prevent employees from using unapproved means of communications for business purposes. Rather, the DOJ indicated that, in evaluating whether a company maintained an adequate compliance program (which could warrant a more preferential resolution), prosecutors should consider whether the company took measures to ensure that it would be able to collect and provide to the government all non-privileged responsive documents relevant to an investigation.

Subsequently, on December 1, 2022, in prepared remarks, Acting Principal Deputy Assistant Attorney General Nicole Argentieri announced that DOJ Criminal Division is examining whether additional



guidance is necessary regarding the use of personal devices, third party messaging applications, and ephemeral messaging.

In her remarks, DAAG Argentieri acknowledged that these applications have legitimate uses such as security and reliability, but that they also present corporations with substantial challenges in implementing compliance programs and when needing to access such communications when necessary. Currently, the DOJ considers whether companies that permit the use of ephemeral messaging platforms are continually updating their policies in compliance with their legal and retention obligations. However, given the rapid evolution of technology and messaging applications, varying retention requirements across industries, and privacy implications in jurisdictions, ensuring corporate compliance has been a challenge.

DAAG Argentieri noted that the DOJ is striving for transparency while developing this new guidance which will account for rapidly evolving technology, disparate retention periods, and varying jurisdictional privacy implications. In the interim, companies should have clear policies on the use and enforcement of mobile devices, third party messaging applications and ephemeral messaging applications. However, those policies need to be constantly reviewed, updated, and enforced.

EDITOR'S NOTE

These enforcement actions and advisories make clear that regulators are focusing heavily on the use of unapproved apps and messaging systems. As a result, all companies—and securities and derivatives market participants in particular—should ensure that they are able to maintain all business communications consistent with their legal obligations and compliance policies and procedures.

[†] Special thanks to Jonathan T. Ammons, Baseil Godellas, Beth Kramer, and Aida Liman-Tinguiri for portions of this analysis.

Preservation, Spoliation, and Sanctions

The 2015 Amendments to Rule 37(e) were intended to enhance uniformity and predictability around the preservation burdens faced by parties to litigation, as well as to the types of actions that might lead to onerous sanctions. Some rule-makers and practitioners also believed they would have the effect of decreasing the frequency with which severe sanctions, now reserved for acts of intentional spoliation, would be doled out. As courts have become more familiar and confident in applying the framework of amended Rule 37(e), we increasingly see courts focused on and wrestling with, first, the kinds of conduct that rise to the level of reflecting “intent to deprive,” and, second, the nature and severity of “curative measures” short of sanctions where intent to deprive has not been shown. To that end, we have seen what we believe to be an inappropriate expansion of the use of evidentiary remedies in the context of Rule 37(e)(1) curative measures that appears to stand in contrast with the intent and purpose beyond the 2015 amendments. The following cases address these and other issues relating to the imposition or denial of sanctions.

CALHOUN v. GOOGLE LLC

In *Calhoun v. Google LLC*, 2022 WL 1987864 (N.D. Cal. June 6, 2022), Magistrate Judge Susan Van Keulen received a response from the defendant regarding the court’s order to compel and order to show cause as to why the defendant should not be sanctioned for interfering with the production of third-party documents, as ordered by the court. The third-party is the defendant’s auditor and plaintiff subpoenaed the auditor for documents relating to the valuation of certain user information. Defendant argued that its review and culling of the auditor’s production were substantially justified because the auditor’s search efforts mostly produced irrelevant documents. Defendant argues that only irrelevant documents were removed from the auditor’s

production and the “no harm, no foul” rule should apply. Magistrate Judge Van Keulen disagreed and stated that the defendant appeared blind to the gravity “of the errors of its interference with a court order.” Judge Van Keulen ordered the defendant to pay plaintiffs’ fees and costs accrued in filing the motion to compel.

CARTY v. STEEM MONSTERS CORP. (DISCORD)

In *Carty v. Steem Monsters Corp.*, 2022 WL 17083645 (E.D. Pa. Nov. 18, 2022), United States Magistrate Judge Elizabeth T. Hey denied plaintiff’s second motion for sanctions against the defendant for spoliation of Discord messages. The plaintiff sued the defendants for breach of contract, fraud, and other claims arising from the defendants’ operation of a digital card game called *Splinterlands*. Before serving the complaint, the plaintiff sent the defendants a Notice to Preserve, instructing on the preservation of both paper and ESI records. During discovery, testimony from the deposition of one of the co-founder defendants gave the plaintiff reason to believe that defendants had removed data from a relevant Discord channel, in violation of the Notice to Preserve. Plaintiff moved for sanctions and/or an adverse inference against the defendants for spoliation of evidence, and also requested additional time to conduct discovery on the question of spoliation. Judge Hey granted the motion for the limited purpose of allowing the plaintiff additional time to depose another defendant on the issue of spoliation; she denied the motion in all other respects, but without prejudice to the plaintiff renewing the motion for sanctions, if warranted, after the deposition.

The plaintiff deposed the second co-founder defendant, who confirmed that data had, in fact, been deleted from their *Splinterlands* Discord channel. However, the defendant explained that the

deletion followed three hacking incidents that were likely scamming attempts. The defendant testified that at some point after the hacks, the data was deleted by either a moderator, who was hoping to prevent an attempted scam, or by the hackers, who were hoping to avoid detection. The defendant asserted that it was not their practice to randomly delete data; that, to the contrary, their policy is to allow for the free flow of content, an exception being malicious content such as hacking and scams; and that they provide their moderators with guidance on data deletion. The defendant also confirmed that they had been complying with the Notice to Preserve since its receipt and, moreover, noted that prior to the hacking, they had produced more than 17,000 pages of Discord messages from the relevant period of time. Finally, the defendant also testified that the data had been permanently deleted and could not be restored, but opined on the possibility that Discord (the company) may have retained the data on their end.

After this additional deposition, the plaintiff filed the instant second Rule 37(e) motion. Judge Hey denied the motion, holding that the plaintiff had failed to demonstrate that spoliation had occurred and, as such, further holding that sanctions were not warranted. On the first point, Judge Hey focused on (i) whether the defendants had a duty to preserve ESI; (ii) whether the defendants failed to take reasonable steps to preserve the ESI; (iii) whether ESI was lost because of said failure; and (iv) whether the lost material could not be restored or replaced. Judge Hey determined that the evidence demonstrated that the defendants had a duty to preserve pursuant to the Preservation Notice, had taken reasonable steps to comply with same, and, moreover, had produced more than 17,000 pages of Discord data for the relevant period of time. Judge Hey also observed that while the data had been deleted, there was no evidence that it had been lost and could not be replaced. Indeed, the defendants had identified Discord as

another potential source for the deleted data, but the plaintiff failed to take any steps to request data from that source. Finally, Judge Hey noted that even if relevant ESI had been lost, the record did not support a finding that any such loss was intentionally caused by the defendants. To the contrary, Judge Hey noted that the record clearly supported a finding that the data deletion was the direct result of a hacking event. In light of these findings, Judge Hey concluded that plaintiff had failed to demonstrate that spoliation had occurred – let alone spoliation that was intentional or motivated by bad faith – and that, consequently, no sanctions of any kind were appropriate.

DRIPS HOLDINGS, LLC v. TELED RIP LLC (SLACK)

In **Drips Holdings, LLC v. Teledrip LLC**, 2022 WL 3282676 (N.D. Ohio Apr. 5, 2022), *report and recommendation adopted in part, rejected in part sub nom.* 2022 WL 4545233 (N.D. Ohio Sept. 29, 2022), United States District Judge John R. Adams imposed a mandatory adverse inference instruction on defendants. The underlying case involved a trademark claim by Drips against Teledrip, and the motion for sanctions involved Teledrip's failure to retain Slack messages until ten months after litigation commenced. Magistrate Judge Carmen E. Henderson found the threshold requirements for spoliation under Rule 37 were met and found that defendants intentionally destroyed ESI with the intent to deprive plaintiffs of the documents, allowing the more severe sanctions under Rule 37(e)(2). Magistrate Judge Henderson concluded that a mandatory adverse inference instruction is allowed but recommended a permissive adverse inference instruction. Judge Adams accepted Magistrate Henderson's findings in the R&R that defendants intentionally destroyed ESI but determined the appropriate sanction to be a mandatory adverse inference, rather than a permissive adverse inference instruction.

Magistrate Judge Henderson first found that the threshold requirements under Rule 37(e) were met. She found that the duty to preserve documents existed since at least August 2019, when a screenshot revealed that defendants acknowledged “the possibility of a trademark dispute” during a trade show. Magistrate Judge Henderson then found that Teledrip intended to destroy ESI by changing its Slack retention policies from indefinite to seven days in October 2019 and not changing it back until September 2020, 10 months after being served and receiving a litigation hold letter in November 2019. Teledrip argued that it changed its retention policies to ensure compliance with ISO standards and the California Consumer Privacy Act and to mitigate risk of liability from retaining information about their consumers. Magistrate Judge Henderson found that “[a]lthough the Defendants’ explanation for changing Teledrip’s Slack retention policy in October 2019 is doubtful, it is plausible. Nonetheless, Defendants’ failure to change the retention policy [for ten months] upon receipt of the litigation hold letter and notice of the lawsuit is ‘inexcusable.’” Magistrate Judge Henderson also found that the destroyed ESI was relevant to the litigation, pointing to evidence that showed that Slack was the “primary mode of communication used by Teledrip” employees and to testimony that “there were several Slack channels on which Teledrip employees internally discussed competing with Drips.” Judge Adams accepted Magistrate Judge Henderson’s analysis finding the threshold requirements were met.

Magistrate Judge Henderson then concluded that the defendants “knowingly spoliated the Slack data with the intent to deprive Drips from discovering its content,” thus allowing the more severe sanctions under Rule 37(e)(2). In coming to this conclusion, Magistrate Judge Henderson noted that “Defendants’ refusal to abide by the litigation hold letter, or seek clarification from their attorney, strongly suggests that the earlier change in policy was not an innocent change of policy to comply

with ISO or CCPA requirements.” For all these reasons, Magistrate Judge Henderson determined that it was “certainly permissible” but “not required” to impose a mandatory adverse-inference sanction. She ultimately recommended a permissive adverse inference, noting that defendants’ excuse “is plausible, albeit convenient,” that “this Court does not believe that Drips is so severely prejudiced by the lack of the Slack data that its case is ‘severely compromised’ without it,” and that “Drips has not argued that absent this evidence it cannot prove its claims.” Upon review, District Judge Adams determined that. “[r]egardless of plausibility,” Teledrip’s excuse was “not credible.” Judge Adams thus accepted Magistrate Judge Henderson’s recommendation to find that Teledrip “knowingly spoliated the Slack data with the intent to deprive Drips from discovering its content” but concluded that the appropriate remedy for this was a mandatory adverse-inference instruction.

EDITOR’S NOTE

This case is noteworthy for the court’s willingness to impose Rule 37(e)(2) sanctions in the absence of direct evidence of intent to destroy the records, but rather inferred from the circumstantial evidence and the court’s rejection of Teledrip’s explanation for the change in the retention setting. A lesson learned about documenting the rationale around changes in retention practices in the midst of litigation and ensuring changes in retention practices are consistent with legal hold practices.

FAST v. GODADDY.COM LLC (FACEBOOK AND TELEGRAM)

In **Fast v. GoDaddy.com LLC**, 2022 WL 325708 (D. Ariz. Feb. 3, 2022), the defendants brought a motion for sanctions on five different counts under Federal Rule of Civil Procedure 37(e) for spoliation of ESI, and on three different counts under FRCP 37(c)(1) for failure to produce relevant information. Judge David G. Campbell granted the motion for three of the five claims under 37(e), and for all three of the claims under 37(c)(1). The plaintiff was a former employee of the defendants, and sued for sex and disability discrimination, as well as Family

Medical Leave Act retaliation. The defendants claimed the plaintiff knowingly deleted relevant information from her devices and accounts and failed to produce other relevant information.

Rule 37(e) authorizes a court to sanction a party for losing or destroying ESI if three prerequisites are met: (1) the ESI in question should have been preserved in anticipation or conduct of litigation; (2) it is lost through a failure to take reasonable steps to preserve it; and (3) it cannot be restored or replaced through additional discovery. If these are met, sanctions are authorized, and even greater sanctions are permitted if the court finds the party acted intentionally to deprive the other of the information's use. Judge Campbell went through each of the defendants' claims. He found sanctions were authorized for the plaintiff's deleted Facebook posts, one "unsent" Facebook message, and deleted messages on the Telegram app. In each of these instances, the court found by a preponderance of the evidence that the plaintiff consciously deleted and "unsent" the content with the intent of depriving the defendants of its use. The plaintiff deleted the Facebook posts despite evidence that she knew how to archive posts; she "unsent" the message five days before the recipient's deposition and the context of the conversation strongly implied the message contained summarized evidence; and the Telegram app being cloud-based implied she had to manually delete the messages off of her and her coworker's devices. The plaintiff was not sanctioned for content on a stolen iPhone that was not backed up or for emails lost via her deactivation of an old email account, since Judge Campbell could not find that she intentionally did not back up her phone or discontinued her email service in order to deprive the defendants of information.

Rule 37(c)(1) authorizes a court to sanction a party for failing to produce information required by Rule 26(a) or (e). Rule 26(e), which was the only relevant subsection here, allows for sanctions if a party

provides "incomplete, misleading, or false discovery responses and does not complete or correct them by supplement," and a party in violation of this Rule may not use the information at trial unless the failure was substantially justified or harmless. The defendants moved for sanctions in connection with the plaintiff's failure to produce 487 Facebook messages, her failure to produce four audio recordings on her phone, and her failure to produce her email communications with her podiatrist. Judge Campbell found her failure to produce this information was not substantially justified or harmless in any instance, and her "last-minute tender" of some of this information did not cure the prejudice. He especially emphasized the "disturbing" nature of her failing to produce her communications with her doctor, as she failed to disclose emails showing she "ghostwrote one of the key medical conclusions in the case." For these reasons, Judge Campbell imposed sanctions on all three of these claims.

The defendants wanted dismissal of the plaintiff's suit, but Judge Campbell noted that dismissal is "the ultimate sanction for spoliation," and was not warranted unless the resulting prejudice essentially denied a party the "ability to adequately defend its case," which he did not feel was the case here, as all the evidence related to damages, not the defense of the case. The sanctions Judge Campbell imposed were: allowing an adverse-inference jury instruction based on the 37(e) sanctions; permitting the defendants to inform the jury of the plaintiff's "redactions" (deletions) of the Facebook posts; requiring the plaintiff to pay some, and perhaps all, of the defendants' attorneys' fees in connection with this motion; allowing the defendants to conduct a forensic review of the plaintiff's electronic devices if they so chose; and allowing the defendants to issue up to four additional third-party subpoenas.

EDITOR'S NOTE

This case provides a textbook example of how the former Chief Judge and Chair of the Advisory Committee methodically applied the elements of Rule 37(e) as well as a balanced approach to the remedy granted, even in light of clear evidence of an intent to deprive.

GINA CENTNER v. TMG UTILITY ADVISORY SERVICES (PRESERVATION LETTERS REJECTED)

In **Gina Centner v. TMG Utility Advisory Services**, 2022 WL 3040884 (D. Ariz. Aug. 2, 2022), the defendant filed a motion for an order precluding plaintiffs from sending “preservation letters” to third parties. Former employees of the defendants brought the case to advance claims of promissory estoppel, fraudulent inducement, and wrongful termination against the defendants. In connection with bringing the suit, the plaintiffs sent copies of the complaint to at least 13 of the defendants’ “investors, auditors, business partners, and clients,” along with letters directing those third parties to “place a litigation hold on all documents and [ESI] (including . . . text messages) that may be potentially relevant to this action.” Plaintiffs claimed that they must file preservation letters with the third parties to preserve their right to obtain sanctions against any third parties should they destroy evidence. However, Chief United States District Judge Murray Snow observed, the plaintiffs provided “no suggestion that they have or ever will have any claims arising against the third parties that will make them defendants in this action.” Judge Snow continued that plaintiffs also “make no claim that their belief that Defendants were violating the law or public policy was founded on any particular document or documents that would likely be in the possession of third parties and that are not already in the parties’ possession.” Finally, Judge Snow added that the lack of specificity in the litigation hold letter and its expansive scope could place a significant burden on the third-party recipients of the letter. Judge Snow explained that “even should

there be no direct rule of civil procedure that addresses such potential abuse to third parties . . . there is substantial likelihood that such conduct is prohibited by the Rule of Professional Conduct ER 4.4(a).” Judge Snow granted the motion to preclude plaintiffs from sending “preservation letters” to third parties in part by prohibiting plaintiffs from serving “further litigation hold letters on third parties without an articulable and good-faith belief that there is a sufficiently specific, relevant, and proportional basis for doing so.”

EDITOR'S NOTE

This case highlights the unwarranted practice of sending prophylactic preservation letters (often just copied wholesale from the internet) without legitimate justification in the hopes of using such letters to support a later spoliation motion. Here, the court rightly found the practice was not supported. It highlights that parties should discuss preservation in the context of Rule 26(f) conferences (as required) and not resort to such gamesmanship letters.

IN RE GOLD KING MINE RELEASE IN SAN JUAN COUNTY, COLORADO

In **In re Gold King Mine Release in San Juan County, Colorado**, 2022 WL 2230759 (D. N.M. June 21, 2022), Chief United States District Judge William P. Johnson granted plaintiff State of Utah’s Motion for Sanctions Due to defendant Harrison Western Construction Corporation’s Spoliation of Evidence in part. The underlying case involved the State of Utah suing Harrison Western regarding a mine blowout that Harrison Western was alleged to be involved with as a contractor for the EPA. Utah moved for sanctions when Harrison Western failed to produce the “documents related to the work Harrison performed or planned to perform at the Gold King Mine in 2014 and 2015.” Judge Johnson noted that “[t]he only pre-blowout emails Harrison produced were those that pertained to its being awarded the subcontract work at the mine and related funding issues and the only post-blowout documents were emails and an employee’s journal, and no other types of documents.” Harrison argued

that it took reasonable precautions to preserve the information, and that the data was lost in a “catastrophic event” during a server migration in circumstances that were beyond its control.

Judge Johnson first found that the threshold requirements for sanctions in Rule 37(e) were met. Judge Johnson found that Harrison had a duty to preserve the data, as there was “no dispute that Harrison knew, or should have known, that litigation was imminent.” He also found that Harrison did not take reasonable steps to preserve the data. While Harrison argued that it took reasonable steps by implementing a litigation hold, Judge Johnson found that it was not enough to implement a hold but not take steps to follow it through. Judge Johnson noted that “Harrison does not identify any other steps it took to preserve its ESI such as taking affirmative steps to monitor compliance” or “having a back-up storage system in place to ensure that the relevant ESI would be preserved.” Judge Johnson further found that the spoliation of the ESI prejudiced Utah, as Utah was left unable to access documents pertaining to key issues in the case. Finally, Judge Johnson stated that he was not convinced “that none of the documents can be replaced,” but seemed to believe that most of the documents were probably irreplaceable. Having found the threshold requirements, Judge Johnson concluded that “some spoliation sanctions are proper.”

After finding the threshold requirements were met, Judge Johnson turned his attention to remedies. He began by granting Utah the right to introduce evidence regarding the spoliation during trial. Judge Johnson then denied Utah’s request to preclude Harrison’s evidence that it was not invited to the mine during the day of the incident, stating that “precluding Harrison from putting on such evidence while allowing Utah to introduce evidence of Harrison’s spoliation at trial would undermine the Court’s interest in promoting accurate fact finding by the jury.” The court also

denied Utah’s request for an adverse instruction, stating that Utah failed to prove bad faith. The court noted that “Harrison’s spoliation appears to be the result of one ‘catastrophic’ server event” and that “Utah did not appear at or attend the depositions of . . . witnesses who may have been able to address Utah’s concerns about the implausibility of Harrison’s explanation regarding the loss of the ESI.” Finally, the court awarded Utah reasonable expenses and fees, stating that such costs would not have been incurred by Utah but for the spoliation.

HENDERSON v. WAXXPOT GRP., LLC (TEXT MESSAGES)

In **Henderson v. Waxxpot Group, LLC**, 2022 WL 2980531 (S.D. Ohio July 28, 2022), plaintiff brought a disability discrimination and retaliation suit against her former employer. Plaintiff sought spoliation sanctions under FRCP 37(e)(2), alleging defendant’s former employee, who was responsible for terminating plaintiff, destroyed relevant text messages and documents. Defendant claimed that the text messages were printed and put into a file relating to plaintiff’s termination, and that the text messages were read aloud to other employees. However, the printed copies of the text messages were not found, and the former employee who had the texts did not have them after leaving the defendant’s employment. Defendant still sought to testify as to the content of the text messages, claiming they contained the reasoning for the termination of plaintiff.

United States District Judge Edmund A. Sargus held that spoliation sanctions were not warranted under Rule 37 because “[t]he record [was] insufficient to establish spoliation.” Judge Sargus did not perform a full analysis of the issues under Rule 37(e)(2), and instead focused on whether the defendant engaged in “the intentional destruction of evidence,” finding that there was no showing of such intent. However, Judge Sargus held that that the defendant could not testify as to the actual text

messages' text, as it should be excluded under FRE 801, 403, and 1002 as it is inadmissible hearsay, highly prejudicial to plaintiff, potentially cumulative, and subject to the Best Evidence Rule. The judge noted that witnesses would be allowed to testify about their own recollections of meeting with plaintiff and direct conversations during those meetings.

HOLLIS v. CEVA LOGISTICS U.S., INC.

In *Hollis v. CEVA Logistics U.S., Inc.*, 2022 WL 1591731 (N.D. Ill. May 19, 2022), District Judge Iain D. Johnston ordered a missing-evidence jury instruction for plaintiff as a curative measure under Rule 37(e)(1). The underlying dispute was an employment discrimination case in which plaintiff alleged that defendant unlawfully terminated him due to race. The defendant asserted that it terminated plaintiff for putting his hands on a coworker. The incident involved conflicting testimony, as three white witnesses alleged that the plaintiff placed his hands on a coworker, but black witnesses asserted that he did not. Two days after the incident, plaintiff notified the defendant of his intent to sue and asked his supervisor to obtain the recording, maintaining that he would be vindicated by the recording. Plaintiff's supervisor failed to retrieve security footage of the incident during the 30-to-90-day window when security footage is preserved, even though obtaining the footage involved merely submitting a request to security, something that the same supervisor had done regarding another incident only a few months prior.

Judge Johnston began his analysis with the threshold requirements for spoliation of ESI under Rule 37(e), finding that each of them were met. Judge Johnston first found that the recordings were ESI. Judge Johnston rejected the defendant's argument that "Plaintiff must first prove that a video camera recorded Plaintiff's encounter with [the coworker]," saying that "[u]nder [Defendant]'s theory, as a practical matter, the spoliation itself

prevents a claim of spoliation." In doing so, Judge Johnston interpreted Seventh Circuit precedent to hold that the burden of proof was on the defendant to show that the video did not exist because plaintiff alerted them of the footage and it was solely within their control to determine whether the footage existed (although he noted that plaintiff would have satisfied his burden to prove the video existed if that burden fell on him). Judge Johnston then found that the employer had a duty to preserve recordings, as "[Plaintiffs]'s letter to [Defendant] on December 5, 2018 alerted [Defendant] of the video and triggered an obligation to preserve it as [Defendant] should have then reasonably anticipated litigation." Judge Johnston next found that the ESI was relevant to the former employee's claim, rejecting a favorableness requirement for the relevance analysis and noting that it is reasonable to infer the footage is favorable to plaintiff anyway. Judge Johnston then found that the defendant failed to take reasonable steps to preserve the ESI and that the ESI was lost and unable to be replaced. Judge Johnston rejected the notion that conflicting witness testimony serves as a replacement for the ESI under Rule 37 and stated that "[t]he question is whether the electronically stored information can be restored or replaced." Finally, Judge Johnston found that the loss of the ESI prejudiced plaintiff. He noted that prejudice "includes the thwarting of a party's ability to obtain the evidence it needs for its case" and found that plaintiff was prejudiced under this definition.

After finding that the threshold requirements were met, Judge Johnston concluded that a curative measure in the form of a jury instruction was the proper remedy. He concluded that a reasonable inference could be drawn that the defendant intended to lose the evidence. This being said, Judge Johnston chose to leave the question of intent to the jury, stating that the defendant's actions could also be explained by incompetence. ("Humans are just as likely to be dimwitted as they

are dastardly.”) Judge Johnston provided a finding of facts to the jury followed by the following instruction: “If you decide that [Defendant] intentionally failed to preserve the video recording of November 28, 2018, to prevent [Plaintiff] from using the video recording in this case, you may—but are not required to—presume that the video recording was unfavorable to [Defendant]. You may then consider your decision regarding the video recording, along with all the other evidence, to decide whether [Defendant] terminated [Plaintiff] because of his race.”

EDITOR’S NOTE

This case highlights the use of Rule 37(e)(1) to allow evidentiary instructions to a jury and allow the jury to make the ultimate factual findings regarding the loss of evidence. While such instructions are technically permissible under the Rule, this expanded practice raises serious questions as to whether it stands in contrast to the intention and purpose of the 2015 Amendments, which was to divorce evidentiary remedies (which are likely to have a severe impact on the outcome of cases) in all but those matters where intent to deprive is demonstrated.

JONES v. RIOT HOSPITALITY GRP. LLC (TEXT MESSAGES)

In **Jones v. Riot Hospitality Group LLC**, 2022 WL 3682031 (D. Ariz. Aug. 24, 2022), Chief Judge G. Murrow Snow granted defendant’s Rule 37 motion for sanctions, dismissing plaintiff’s suit against the defendant with prejudice. The underlying case involved a claim by the plaintiff against her employer alleging sexual harassment by a supervisor.

After deposing three of plaintiff’s witnesses, the defendant learned that each witness had exchanged text messages with the plaintiff regarding the harassment claim after the litigation commenced. Plaintiff only produced unresponsive screenshots of these messages, so “the Court ordered the parties to jointly retain a third-party forensic search specialist and ordered Plaintiff and her witnesses to submit their devices to that

specialist for imaging.” After another court order, plaintiff and two witnesses produced their phones; the witness who did not was excluded from testifying. A jointly retained forensic expert sent the extracted data to counsel for the plaintiff in September 2020, but counsel failed to turn over the messages to the defendants despite two court orders. On March 2, 2021, Judge Snow ordered the expert to produce the messages to defendants directly. Defendants subsequently retained the expert separately to conduct a spoliation analysis. Defendants filed a motion for spoliation sanctions based on his conclusion “that whenever the text message logs between Plaintiff and her witnesses show asymmetric communication, it is highly likely that additional messages sent around the time of the apparent asymmetries were also deleted by both parties.” The expert explained that this was because “when two custodians collaborate to delete specific text messages and in particular, a large number of text messages, they often delete in unison the most egregious messages, but messages of no or minor importance are not as diligently deleted.”

The court began by analyzing the threshold requirements for ESI spoliation sanctions under Rule 37(e). Judge Snow first found that plaintiff had a duty to preserve the ESI, noting that the messages at issue were all “sent after the litigation commenced” and that plaintiff “was aware that she had potential claims against defendants” at least from the time she completed an EEOC intake questionnaire. Judge Snow then found that plaintiff not only failed to take reasonable steps to preserve the ESI but actively and intentionally deleted it from her own phone and coordinated with her witnesses so they would delete it from their phones as well. Judge Snow then found that the ESI could not be restored or replaced through additional discovery as “any attempt at obtaining these messages would likely be prohibitively expensive at this point.” Judge Snow noted that “costly forensic techniques

would likely be required” for recovery and that the techniques “are not guaranteed to recover all deleted messages” anyway.

Having found the threshold requirements met, Judge Snow turned to intent, finding “by a preponderance of the evidence that [Plaintiff] deleted the text messages with her witnesses intending to deprive Defendants of their use in the litigation.” Judge Snow noted that “Plaintiff does not argue that the text messages were inadvertently deleted, nor could she, as it is clear that she affirmatively selected certain text messages for deletion while otherwise preserving text messages sent around the same time. Nor does she offer any explanation, let alone a credible one, for why she deleted messages notwithstanding her duty to preserve. A finding that she intentionally deleted messages is therefore justified.”

Applying the Ninth Circuit *Leon* factors, Judge Snow concluded that dismissal was warranted in this case, as no lesser sanctions were available. Judge Snow noted that lesser sanctions were already tried: the monetary sanctions imposed were not paid and other sanctions imposed were not effective. Judge Snow concluded that the plaintiff had “willfully violated the Court’s orders for over two years, thwarting the discovery process and undermining the fairness of any trial on the merits” and “that the only effective sanction that will appropriately punish her behavior and deter potential discovery misconduct in other cases is to dismiss Plaintiff’s Fourth and Final Amended Complaint with prejudice.”

META PLATFORMS, INC. v. BRANDTOTAL, LTD.

In **Meta Platforms, Inc. v BrandTotal, Ltd.**, 2022 WL 1990225 (N.D. Cal. July 6, 2022), Chief United States Magistrate Judge Joseph C. Spero granted in part, and denied in part, Plaintiff’s sanctions motion for spoliation of evidence, while at the same time, ruling on both parties’ motions for summary

judgment. The Defendant provides its corporate clients consulting services regarding how digital advertisements are presented to social media users, including on Plaintiff’s Facebook and Instagram social networks. For approximately four months, Defendant’s products automatically collected user access and demographic information about Facebook and Instagram users. Plaintiff’s sanctions motion related to debugging log data that was allowed to be deleted on a regular thirty-day schedule after Defendants had learned that the data was relevant as it showed that Plaintiff user data had been sent to Defendants, as well as inaccurate deposition testimony regarding the data deletion.

Plaintiff specifically requested an adverse presumption to the fact-finder at trial against Defendants that (1) Defendants were obligated to preserve the lost debugging log data, but intentionally failed to do so because the data was unfavorable to defendants; (2) the deleted data would have shown misappropriated user credentials from Plaintiffs’ users moved to Defendant’s servers; and (3) the deleted data would have shown that Defendants continuously used created or purchased accounts to gain access to Facebook and Instagram, pose as legitimate users, and scrape data from Plaintiff’s computers. Plaintiff also sought to preclude Defendants from relying on the inaccurate testimony regarding data deletion, as well as for fees and costs in bringing its motion. In response, Defendants argued that it did not intentionally or even affirmatively delete data, but rather, the data was lost in the ordinary course of business, that Plaintiff was not prejudiced because other evidence shows the conduct at issue, and because the relief Plaintiff seeks is excessive.

Judge Spero found that the lost debugging logs included information relevant to the case, that Defendant knew that the logs contained relevant information, and should have taken steps to preserve it once litigation was contemplated,

despite not doing so until one year later. Judge Spero specifically noted that the absence of a real-time log at the time of collection prejudices Plaintiff's ability to understand the scope and nature of the scraping conduct. Despite finding that the information was spoliated, Judge Spero declined to award Plaintiff the relief it requested. First, because Plaintiff has also filed a pending summary judgement motion asking the Court to treat certain fact as established, while also seeking an instruction at trial that the jury may presume such facts to be true, its requested relief is inconsistent and unsupported. Second, Judge Spero also found that Plaintiff did not meet Rule 37(e)(2)'s requirement that Defendant acted with the intent to deprive Plaintiff of the information in the lost logs. Defendant argued that it was merely negligent in failing to take steps to prevent the automatic deletion. Judge Spero found that while Defendants should have known to preserve those records, they did take steps to preserve more obvious sources of information such as email accounts and databases. Judge Spero did allow for the possibility that Defendant's failure to preserve the logs was intentional, he ultimately concluded that Plaintiff failed to meet its burden of showing that Defendant's intentional actions were the most likely explanation for the ongoing automatic deletion of those logs. Finally, Judge Spero denied Plaintiff's request to impose an adverse inference instruction under the Court's inherent authority because the relief Plaintiff requested was "too far removed from the evidence that *is* in the record." Specifically, Plaintiff requested the Court to provide an instruction that the deleted logs would have shown a year-long practice of exfiltrating user access credentials to scrape data, without offering any other evidence besides the absence of the missing logs. Ultimately, Judge Spero's relief was limited to a jury instruction that Defendant had a duty to preserve the logs between October 2020 and October 2021, but failed to do so and that jurors "may consider whether one party intentionally concealed or destroyed evidence, or *intentionally*

allowed evidence to be lost. If you decide that a party did so, you may decide that the evidence would have been unfavorable to that party."

RED WOLF ENERGY TRADING LLC v. BIA CAPITAL MANAGEMENT LLC (SLACK)

In **Red Wolf Energy Trading LLC v. Bia Capital Management LLC**, 2022 WL 4112081 (D. Mass. Sep. 8, 2022), United States District Judge Mark L. Wolf sanctioned defendants under Rule 37(b) and entered default judgement for plaintiffs on all claims. The underlying case involved claims for misappropriation of trade secrets and unfair trade practices, with Red Wolf alleging that its competitor, Bia Capital, promoted its business by obtaining trade secrets from a Red Wolf employee. Judge Wolf noted that "this case has generated more meritorious motions to compel and for sanctions against defendants for failure to produce documents than any other case in which this court has presided in more than 37 years."

In determining sanctions, Judge Wolf stated that courts must analyze the "totality of circumstances" and balance all relevant factors. Judge Wolf noted that default judgements are "disfavored," "drastic," and only to be used in "extreme situations," but also noted that "a party's disregard of a court order is a paradigmatic example of extreme misconduct" (quoting the First Circuit). Judge Wolf found that "[i]n this case, despite repeated orders to review, and supplement if necessary, their production of documents, and repeated warnings that severe sanctions could be imposed if they failed to do so, [defendant's principals] violated the April 1, 2021 and August 31, 2021 discovery orders."

On April 1, 2021, the court issued its first order following a motion to compel from Red Wolf. The Order directed Bia to review the Google Suite docs and any other responses to discovery requests and produce anything necessary under Rule 26(e). Moeller filed a sworn affidavit on April 14, 2021

asserting compliance with the order. Bia subsequently deposed defendants in May 2021. These depositions revealed that Bia failed to produce all pertinent Slack communications. After another motion to compel production, the court issued a second order on August 31, 2021, instructing Bia to supplement production as necessary under Rule 26 and to file an affidavit addressing compliance with the order. On September 7, 2021, Moeller filed another sworn affidavit stating that no further supplementation was required.

On March 22, 2022, Judge Wolf found that the defendants violated the two orders by failing to produce 47 Google Suite documents, including a PowerPoint that contained “meaningful evidence that [the former employee] and [defendant’s principals] misappropriated Red Wolf’s trade secrets and engaged in deceptive trade practices.” Judge Wolf also ordered production of all Slack communications between the former employee and the defendants from January 1, 2015 to January 31, 2019. Judge Wolf stated that it was reasonable to infer that the defendants intentionally violated the court orders but that he was extending the “benefit of great doubt.” He allowed Red Wolf to retake depositions of three defendants because Red Wolf lacked these documents during the initial depositions. Judge Wolf repeatedly and sternly admonished defendants to comply, even raising the prospects of criminal contempt for noncompliance. Following the March hearing, defendants produced certain Slack messages and Red Wolf retook the depositions. One witness testified that the failure to produce Slack messages was “due to a mistake made by Abramyan, the independent contractor in Kazakhstan, who wrote a program to search and produce Bia’s Slack messages.” After the repeated depositions, “defendants made two additional productions containing Slack messages with Search Terms that had not been previously produced.” Plaintiffs then filed the motion for sanctions being discussed here.

Judge Wolf found that defendants’ actions constituted “extreme misconduct.” He noted that the “[d]efendants seek to excuse their repeated failures to produce potentially important documents by blaming people they employed for purportedly inadvertent errors. First, they blame Brown for inexplicably not searching the entire Google Vault when he searched Google Suite which includes it, and for failing to produce 47 documents including the PowerPoint presentation. Second, they blame Abramyan for devising from scratch a flawed program to search Slack, which he had never done before.” Regarding intent, Judge Wolf noted that “there is evidence that indicates that Bia and Moeller may have deliberately failed to produce some Slack messages,” given that there are 87 Slack channels that contain no data. This being said, Judge Wolf determined that “litigating whether [the deletion of messages] was deliberate would be time-consuming for the court and expensive for Red Wolf” and “defendants’ misconduct was extreme” even if not deliberate. Judge Wolf stated “[t]hat misconduct is exacerbated because defendants continued their misconduct despite multiple, increasingly severe warnings that any further failure to supplement their incomplete production of documents would be severely sanctioned.”

Judge Wolf found that the “misconduct significantly prejudiced Red Wolf,” as it deprived Red Wolf of the documents during the second depositions; it “deprived Red Wolf of the opportunity to file a fully informed motion for summary judgment that may have been meritorious and ended this case long ago,” and it meant that “defendants have prolonged their opportunity to profit from the misappropriation of Red Wolf’s trade secrets and other unfair practices that Red Wolf alleges.” Judge Wolf also found that “Defendants’ misconduct has also severely injured the court’s ability to manage this case and the many other cases,” as the court “has never in more than 37 years had a civil case with more discovery disputes and motions for

sanctions than this one.” Judge Wolf concluded by entering judgement for plaintiff and granting plaintiff’s reasonable expenses and fees incurred for their second sanctions motion.

RESOLUTE FOREST PRODUCTS v. GREENPEACE INTERNATIONAL (SKYPE, TEXT MESSAGES)

In **Resolute Forest Products v. Greenpeace International**, 2022 WL 16637990 (N.D. Cal. Nov. 2, 2022), United States Magistrate Judge Kandis A. Westmore granted in part, and denied in part, both parties’ motions for sanctions stemming from loss of multiple categories of documents.

The case involves claims for defamation brought by a collective of companies in the forest products industry against the defendant environmental preservation activist organization and its representatives. The plaintiffs sent an initial cease and desist notice in June 2015, in response to which the defendants issued a legal hold. Plaintiff subsequently sued in May 2016.

As part of its production, the defendants produced over 9,600 Skype messages from the time period of December 2016 through December 21, 2017, but few messages from the period May to December 2016. As the court explained, Skype messages from April 20, 2017 onward were available to the defendants in the cloud, while messages prior to that date were not thanks to a service migration, so that messages prior to that date could only be retrieved directly from custodian phones and laptops. The defendants cooperated with the plaintiffs to collect available messages, including having custodians complete consent forms so that the plaintiffs could subpoena the data from Microsoft, which produced some Skype messages for the date range. Nevertheless, despite the legal hold notices and all of the parties’ attempts at collection, some Skype messages for some custodians during the relevant time period were not

preserved or produced. Additionally, around December 2017, more than 2.5 years after the duty to preserve attached, a defendant custodian recognized that his Skype message retention was set to something other than "forever" during a critical portion of the discovery period.

The defendants, in turn, alleged that the plaintiffs failed to adequately preserve and search for evidence, resulting in spoliation and the tardy production of over 14,000 (out of 25,000) documents. The defendants further allege that the plaintiffs failed to institute a litigation hold specific to the claims in this case. The defendants served initial discovery requests to the plaintiffs in September 2019. Plaintiffs attempted to meet and confer with Defendants to discuss search terms and custodians, but Defendants did not respond. The plaintiffs subsequently identified five relevant custodians and produced 10,564 documents (about half of which did not include hash value metadata and another 700 of which did not include date metadata). Through deposition testimony, the defendant also identified several categories of hard copy documents, electronic documents, emails, and text messages that the plaintiffs had not produced. In response, the plaintiffs supplemented their productions (often, the defendant complained, just a few days before scheduled depositions).

Judge Westmore individually ruled on each source of allegedly spoliated information. With respect to the defendants’ missing Skype messages, Judge Westmore found that there was no dispute that the lost messages were relevant. However, she ruled that the plaintiffs had not demonstrated that the defendants failed to take reasonable steps to preserve those messages because they did issue a litigation hold notice. Moreover, outside of one custodian failing to turn off his auto-delete function on Skype messages, the plaintiffs did not offer any evidence showing that the defendants actively deleted or caused Skype messages to be lost. Judge Westmore determined that the defendants

reasonably believed that the Skype messages were being saved, making sanctions under Rule 37(e) inapplicable because the data was lost despite reasonable efforts to preserve them. Judge Westmore also dismissed the plaintiff's allegation that the defendants intentionally deleted the Skype messages, noting that plaintiff's speculation was not supported by the record. However, Judge Westmore found that messages lost due to the failure to turn off the auto-delete setting in Skype were lost due to a failure to take reasonable steps to preserve and that the plaintiff was prejudiced as a result. As a curative measure, Judge Westmore recommended that the jury be instructed that certain Skype messages should have been preserved, but were not because the witness failed to turn off the auto-delete setting.

With respect to the plaintiffs, Judge Westmore found that they spoliated potentially relevant text messages. Specifically, Judge Westmore noted that the plaintiffs failed to take any reasonable steps to produce or preserve text messages as they did not conduct any searches for text messages, nor did they suggest any alternative means to search for potentially relevant text messages. Judge Westmore declined to find that emails sent between a Plaintiff employee's personal and work email addresses were lost because those emails from the custodian's personal email account would have been preserved via her business email address. As to the defendant's claims that the plaintiffs failed to institute a legal hold specific to the claims in this case, Judge Westmore highlighted the plaintiff's extensive preservation efforts in connection with a separate, earlier in time and similar litigation with the defendants. Specifically, in April 2014, the plaintiffs issued a litigation hold notice requiring the preservation of records from 2009 onward relating to the defendant's allegedly false and defamatory statements about the plaintiffs. This hold notice was distributed to 56 employees, was updated quarterly, custodian interviews were conducted, email data was

backed-up annually and custodians were given additional storage space. Also, witnesses testified to understanding that their preservation obligation extended to all Defendant statements, including the ones at issue in this litigation. Given their extensive preservation efforts under the related hold, Judge Westmore declined to find that the plaintiffs' failure to issue a litigation hold specific to this matter was a failure to take reasonable steps to preserve.

Judge Westmore also declined to find that documents missing metadata were spoliated because the defendants did not demonstrate how the missing metadata prejudiced them, nor did it show that the plaintiffs intentionally deleted the metadata. The defendants also requested monetary sanctions under court's inherent power for the plaintiff's "belated and ad hoc production". The plaintiffs argued that any delay was due to defendant's failure to meet and confer regarding custodians and search terms. Judge Westmore noted that the plaintiffs provided no authority that the defendants were required to assist plaintiffs in crafting searches to identify relevant documents. However, the defendants argued, without dispute, that the plaintiffs would routinely produce documents just prior to depositions, resulting in the adjournment or delay of those depositions. Judge Westmore found that this pattern of behavior demonstrated bad faith and improper gamesmanship and ordered plaintiffs, under the Court's inherent authority, to pay for the defendant's costs to reschedule depositions and to review the belatedly produced documents.

SCHNATTER v. 247 GROUP, LLC (TEXT MESSAGES)

In **Schnatter v. 247 Group, LLC**, 2022 WL 2402658 (W.D. Ky. Mar. 14, 2022), defendants sought sanctions against plaintiff for his alleged spoliation of text messages. As background, in May 2018, plaintiff, the founder of Papa John's, "made controversial comments about racial issues and uttered a racial slur" during a conference call with

defendants. Unbeknown to plaintiff, that call was recorded and leaked to *Forbes*, which published a story, resulting in plaintiff voluntarily resigning from his position and the company terminating his Founder Agreement. Plaintiff filed suit against his former company in July 2018, relating to his termination. In December 2019, plaintiff filed suit against defendants, relating to the leak to *Forbes* and the *Forbes* story.

During the course of discovery, defendants identified certain text messages produced by non-parties that the plaintiff failed to produce from his own collection. Plaintiff eventually disclosed that he had used six phones since January 2017. The first he used between January 2017 and February 2018 and discarded around March 2018, before the initial suit was filed. The second he used between February 2018 and January 2019. This phone was imaged in July 2018 in anticipation of litigation, but plaintiff discarded it in February 2020 without imaging any messages since July 2018. The third phone was imaged early in the December 2019 litigation. The fourth phone was his current phone and was not yet imaged. The fifth and sixth phones were secondary phones that he used between December 2019 and June 2020 and that he discarded in August and December 2020 without imaging. Defendants sought sanctions for spoliation of text messages. Plaintiff argued that deleting messages in this way has been his practice since 2014 and that he did this to protect his privacy as a public figure.

Magistrate Judge Colin H. Lindsay recommended that the jury be allowed to hear evidence and arguments related to lost text messages and ordered the plaintiff to pay reasonable costs and attorneys' fees stemming from defendants' motion.

The court conducted a detailed analysis under Rule 37(e), finding there was a duty to preserve text messages arising from the separate July 2018 litigation and those messages were lost. The court

noted that a July 25, 2018 litigation-hold notice put plaintiff on notice that his cell phone messages were potentially relevant ESI. The court then found that plaintiff "not only took no steps to preserve his text messages, he deliberately deleted every text message he sent and received since his preservation duty was triggered." The court rejected plaintiff's justification "that it was his routine practice since 2014 due to privacy concerns" and stated that "[r]egardless of the reason for his routine practice before he anticipated potential litigation, such practices must be suspended once the duty to preserve is triggered." Finally, the court found that the ESI was not replaceable, as "Defendants should not be required to expend unlimited resources turning over every stone that [plaintiff] points to, especially when [plaintiff] has been unwilling to put forth any meaningful effort to recover any lost ESI."

Although Rule 37(e)'s threshold requirements had been met, Magistrate Lindsay found that "it is difficult to conclude that [plaintiff's] spoliation was anything less than grossly negligent," and as such, the court was "unable to conclude that [plaintiff] acted with the specific intent of depriving Defendants of the use of the evidence in litigation." In arriving at this conclusion, the court noted that "[plaintiff] has put forth evidence that he routinely deleted all text messages beginning in 2014 and often uses multiple cell phones due to privacy concerns as a public figure" and that "no evidence has been presented that [plaintiff] knew the significance of the missing evidence at the time the evidence was lost." The court thus determined that it may not impose the more severe sanctions permitted under Rule 37(e)(2). The court nonetheless found that defendants were prejudiced by the lost ESI and concluded that lesser sanctions were warranted under Rule 37(e)(1). The court recommended that both parties be allowed to present evidence related to the missing ESI and make arguments to the jury regarding whether to make an adverse inference. The court

further recommended that plaintiff pay defendants' reasonable costs and attorneys' fees related to prosecuting the motion for sanctions.

EDITOR'S NOTE

Another case of concern where the court used evidentiary instructions to a jury and allowed the jury to make the ultimate factual findings regarding the loss of evidence under Rule 37(e)(1), creating the probability that the outcome of the litigation could be impacted by the loss of ESI, even in the absence of intent to deprive.

TWITTER v. MUSK (SIGNAL)


In **Twitter v. Musk**, No. 2022-0613-KSJM (Del. Ch. Oct. 5, 2022), Chancellor Kathaleen St. Jude McCormick found that messages that Elon Musk sent via Signal were likely "irretrievably lost" and that sanctions would be appropriate "[i]f Defendants deleted documents after they were under a duty to preserve." Twitter sought "to compel production of all of Musk's messages from January 1, 2022 to July 8, 2022, and request[ed] an adverse inference that Defendants recklessly or intentionally deleted or withheld damaging messages." Chancellor McCormick stated that she has not yet decided what the appropriate remedy would be and reserved ruling on sanctions pending post-trial briefing.

Chancellor McCormick first found that Musk's alleged failure to produce SMS messages does not warrant sanction. Twitter argued that "Musk unreasonably frustrated Twitter's attempts to verify adequacy of production" by failing to produce certain SMS messages, but Chancellor McCormick found that these issues were mostly mooted. Twitter also argued that certain SMS messages to and from Musk appeared in third-party productions or Musk's phone logs, but not in Musk's productions. In addressing this, Chancellor McCormick first ordered Musk to log or produce responsive messages between Musk and his attorney. Chancellor McCormick then found that Musk should have produced four texts with investor

Larry Ellison from hours before the "temporarily on hold" tweet earlier, but Musk produced those messages in his brief. Chancellor McCormick finally found that 58 messages between Musk's business manager, Jared Birchall, and Morgan Stanley produced by Morgan Stanley but not produced by Musk were largely not substantive. Taken together, Chancellor McCormick concluded that these missing productions did not warrant sanction.

Chancellor McCormick then ordered Musk to produce all such messages that are responsive. Chancellor McCormick noted that the fact that Musk produced no responsive messages during critical periods between May 24 and May 30 and June 1 and June 7 "raises the possibility that Musk communicated through other informal channels not captured by text records, such as iMessage or Signal." That Musk traveled internationally during the end of May made it even more likely that he used internet-based messaging services. Chancellor McCormick also noted that Musk has stated publicly that he uses "iMessage and Signal," and Birchall testified in deposition that he and Musk used Signal to communicate about "personal financial matters." Taken together, Chancellor McCormick concluded that "it seems possible (even likely) that Musk used informal channels of communications other than text message during the relevant gaps" and ordered production of any such responsive messages.

Chancellor McCormick then determined that Musk likely used Signal's auto delete feature and that messages he sent via Signal were likely "irretrievably lost." A screenshot from third-party discovery revealed that Musk used Signal to message another potential investor, Marc Andreessen, about potentially joining the Twitter deal as an equity partner. Musk filed an affidavit stating that he does not recall using Signal at any other point to discuss the Twitter deal, but discovery revealed another instance of Musk using Signal to discuss the deal, this time to message



Birchall. Chancellor McCormick noted that: “Musk initiated the Birchall Signal Exchange, and it concerned routine scheduling matters. It seems unlikely, therefore, that the Birchall Signal Exchange and the Andreessen Signal Exchange were the only times Musk chose to use Signal to communicate regarding the Twitter transaction.” Chancellor McCormick also noted that “[i]t is reasonable to infer from Defendants’ representations and the apparent lack of any Signal messages in their production thus far that Musk used Signal’s automatic deletion feature.” Finding that Musk likely communicated via Signal regarding the deal and that those communications are unlikely to be retrievable, Chancellor McCormick concluded that some remedy would be appropriate if the “deletions occurred when Defendants were under a duty to preserve documents.” She reserved judgement on sanctions, stating that she had not yet determined what the proper sanctions would be.

Technology Assisted Review

2022 has been a relative slow year regarding judicial decisions on the use of Technology Assisted Review (“TAR”), perhaps reflecting that in practice TAR (especially Continuous Active Learning (“CAL”)) has become a relatively commonplace part of the document review process and, therefore, required less judicial review regarding its adoption and use. That said, we have observed a broadening unwillingness of parties to spend time and effort to negotiate and/or litigate extensive TAR protocols, instead opting to use CAL for prioritization and quality control rather than the determination of relevancy. Nevertheless, whether negotiated and agreed or not, parties continue to generate disputes around the use of TAR/CAL—including, such as in the Allergan case described below, whether that use would be appropriate under the circumstances.

IN RE ALLERGAN BIOCELL TEXTURED BREAST IMPLANT PRODUCTS LIABILITY LITIGATION

The issue of whether a party can use search terms prior to TAR was before the two special masters in **In re Allergan Biocell Textured Breast Implant Products Liability Litigation**, 2022 WL 16630821 (D.N.J. Oct. 25, 2022). Defendant filed an application with the court to allow it to proceed with its search protocol, which included using key word searches to cull a 9.371 terabyte document set before TAR. Plaintiffs objected to the proposed search protocol, arguing that the defendant should first apply TAR to the full data set, and then apply search terms after. Defendant stated plaintiffs’ proposal was not reasonable, as defendant would be required to re-collect the 9.371 terabytes of data, and the search terms were broad. The plaintiffs stated that if defendant did not agree to their proposal, then defendant should only proceed using search terms and full human review.

Special Masters Judge Joseph A. Dickson, U.S.M.J. (Ret.) and Judge Rachelle L. Harz, J.S.C., issued a Special Masters Case Management Order denying defendant’s application, and ordered defendant to proceed with search terms and full human review. In reaching this conclusion, the Special Masters rejected defendant’s argument that the use of search terms prior to TAR was “consistent with the majority of courts,” which defendant supported by citing to *In re Biomet M2a Magnum Hip Implant Products Liability Litigation*, *Livingston v. City of Chicago*, *Huntsman v. Southwest Airlines Co.*, and *Bridgestone Ams., Inc.* Instead, the Special Masters found that “[t]here is no such general principle espoused by the courts or the commentators. . . . The courts find solutions to the problems confronting them, but do not settle the question of which method is better.” Here, the Special Masters relied on several factors to reach their conclusion: (i) they doubted that the defendant would have to recollect all 9.371 terabytes of data; (ii) defendant did not provide specific burden and cost information for plaintiffs’ proposal as compared to its own proposal; (iii) the use of search terms with TAR could open the door for additional discovery disputes related to the accuracy of the review; and (iv) their belief that the agreed-upon ESI protocol suggested there would be party agreement on this issue. On this last note, the Special Masters observed that “the parties have not agreed to the application of TAR.” They noted that the ESI protocol agreed to by the parties required them “to work in a cooperative and collaborative manner to maximize the efficiency and success of the application of the methodologies proposed at identifying potentially relevant ESI,” and that “if either Party believes that revisions to agreed-upon search-term or advanced-technology procedures are necessary to enhance or improve the identification of potentially responsive ESI, the Parties shall promptly meet and confer regarding

the proposed revisions prior to implementation. No such revisions shall be permitted absent agreement of the Parties, or order of the Court.” Accordingly, the Special Masters found that, because the parties “did not bargain for” the ability to unilaterally implement “advanced-technology procedures,” it would be inappropriate to allow the defendant to do so at this stage.

IN RE DIISOCYANATES ANTITRUST LITIGATION

In *In re Diisocyanates Antitrust Litigation*, 2:18-mc-01001-WSH, Dkt. 798 (W.D. Pa. Oct. 19, 2022), Special Master James C. Francis IV (Ret.) issued a Report and Recommendation recommending that the court grant the plaintiffs’ motion to compel to require three defendants to resume their TAR review and continue until the last two batches reviewed contained no more than 10% responsive documents.

The case involves allegations by purchasers that manufacturers of certain precursor chemicals used in polyurethane manufactory colluded to restrict supply and increase prices. In March 2021, the plaintiffs moved for an order compelling the defendants to use certain search terms and TAR methodologies for their review and production. The defendants cross-moved for a protective order permitting them to proceed with the search terms and TAR protocols they had proposed. In August 2021, Judge Francis recommended that both motions be denied; the defendant’s motion because, among other reasons, Judge Francis did not view defendant’s proposal for the use of TAR to be reasonable, “first because the validation procedure tested recall only for the search conducted by TAR, ignoring the documents eliminated by search terms, and, second because it failed to take advantage of the capability of the defendants’ continuous active learning (“CAL”) tools to analyze the marginal value of conducting

additional search iterations beyond a putative stopping point” (i.e., stopping only after a minimum threshold of relevance has been detected in newly batched documents).

The defendants subsequently modified their TAR protocol to address the flaws identified by Judge Francis, and also proposed that, if the parties were not able to agree on search terms, they would apply their preferred terms subject to a validation analysis. They also agreed to disclose the number and content of responsive documents identified during the last two batches of documents promoted for review by the TAR software. Upon review of these, the defendants proposed that the plaintiffs would then be able to petition the court to review the process if plaintiffs disagreed with the defendants’ assertion that the search was reasonably complete.

The plaintiffs previously had objected to the August Report and Recommendation and asked the district court to either order defendants to use the plaintiffs’ proposed search terms and TAR protocol or order the defendants to produce all non-privileged documents in their collections that hit on the plaintiffs’ search terms, subject only to a privilege review. The district judge overruled the objection and ordered the defendants to “proceed, forthwith, as they have outlined in their submissions.” (In January 2022 the plaintiffs again moved to compel use of their preferred search terms, and Judge Francis recommended this motion be denied as foreclosed by the district court’s prior order, and the court agreed.) The defendants thereafter proceeded with their search terms and TAR approach. Each defendant disclosed that its review reached an estimated recall of between 74% and 89%, along with the results of an elusion test. However, three of the five defendants stopped their CAL reviews at a time when batches still were returning responsiveness rates above 10% (19%, 18%, and 15%).

In the most recent motion before Judge Francis, the plaintiffs challenged the defendants' conclusions that their productions were reasonably complete. First, they argued that the defendants' search terms were too narrow, and they should have been required to use the more-expansive search terms plaintiffs proposed but that were rejected by the special master and district court. Plaintiffs argued that the disputed terms they sought to compel would have returned documents "central to the case," and provided examples of such documents that "were not identified by the defendants' search terms." They also argued that the defendants' estimates of a high level of recall, despite the narrower terms applied, were "overly rosy" and unreliable because "they were not calculated using blind, stratified samples."

Second, the plaintiffs challenged the adequacy of the review completed by the three defendants who ceased their TAR review procedures while still encountering a high level of responsiveness, having previously proposed that review should continue until "the last two batches of documents identified by TAR and reviewed by humans contains no more than five to ten percent (5%–10%) responsive documents, and none of the responsive documents is novel and/or more than marginally relevant"—which neither Judge Francis nor the district court adopted.

Judge Francis disagreed with the plaintiffs' assertion that substantial responsive documents necessarily had been missed because of defendants' narrower terms. Instead, he reasoned, "[t]he better conclusion is that the defendants' search terms were robust enough to capture many of the same documents that the disputed terms would have, without bringing in volumes of additional non-responsive documents." He rejected a standard calling for something close to perfection, however, observing that this "does not mean that the defendants' search terms are perfect; they are not. But the parties agreed that the

defendants could use search terms to narrow the population of documents to be presented to the TAR tools. . . . and the search terms utilized by the defendants have not been demonstrated to be unreasonable. The evidence shows that the documents that they missed were probably not of high value, and the search terms adequately captured the critical issues that the plaintiffs have identified." He therefore recommended the motion be denied to the extent it sought to compel the defendants to redo their review using plaintiffs' preferred terms.

With respect to the objection that three of the defendants stopped their TAR review too soon, Judge Francis sided with the plaintiffs. He noted that "because large swaths of documents had already been excluded by search terms, it is particularly important not to stop the review of the remaining documents prematurely." Judge Francis noted that both the quantity and the quality of the documents found in later batches led him to believe additional review was needed. Having reviewed the responsive documents from the three defendants' final review batches, he concluded that qualitatively they were "not entirely novel and would not justify implementing a new set of search terms, [but] they are sufficiently important to require [the defendants] to continue their review of documents already identified as potentially responsive based on their own search terms." Importantly, he observed, "the fact that these documents were identified at this point in the TAR process suggests that other similar documents, some of which may be unique, remain in the unreviewed TAR population."

In resisting this aspect of plaintiffs' motion, the three subject defendants argued that the relief plaintiffs sought "would impose a disproportionate burden on them"; however, Judge Francis noted that most of the costs described by two of the defendants included costs associated with applying broader search terms and then re-running their TAR review,

and did not carve out costs solely associated with continuing the prematurely terminated review. One defendant did appropriately tailored burden estimates, including review costs of between \$50,000 and \$100,000 per week.

Judge Francis evaluated these concerns using the proportionality factors in FRCP 26(b)(1)(B), finding “[o]n balance . . . the proportionality factors favor requiring [the defendants] to continue their TAR review.” Judge Francis found it significant that “the additional discovery sought from these defendants does not consist of information that is likely to differ in kind from what the plaintiffs already possess, [but] it is potentially important in allowing them to build their case, and the benefit therefore outweighs the burden.” Judge Francis recommended “that each review may presumptively be terminated when the last two batches reviewed contain no more than 10% responsive documents,” in order to reduce “the probability of further dispute and to provide the parties with a benchmark.”

EDITOR’S NOTE


This case provides a rare analysis of what is an appropriate level of recall and elusion. It is notable that Judge Francis focused not merely on the numeric metrics the parties provided concerning the level of recall and elusion achieved, but also on the “quality” or unique content of the documents identified in later batches. It may be tempting for future litigants to cite this Report & Recommendation for the general prospect that “greater than 10% responsiveness rate in CAL review batches” means review should continue, but Judge Francis’s conclusion is grounded in the fact that the later-identified records suggested that distinctly relevant categories of documents were being identified by the models late in the review. This R&R therefore should be read narrowly and does not contradict the general guidance set out in other cases: that review can be concluded once a suitably high level of recall, supported by a corroborating elusion test, has been achieved. Otherwise, a CAL review that develops a very high level of precision (a metric not discussed in Judge Francis’s R&R) could be burdened to continue well past achieving the targeted level of recall as the model continues to successfully scrape the bottom of the null-set barrel. The case also highlights whether and to

what extent courts should be engaged at this level in managing a TAR process, including validation. Here, plaintiffs seem to be litigating to a standard of perfection—not reasonableness. The case highlights why many litigants have simply decided to use TAR for prioritization to avoid lengthy negotiation and litigation over the use of TAR for relevancy determination.

QUIRURGIL v. HOLOGIC, INC.

In *Quirurgil v. Hologic, Inc.*, 2022 WL 2719528 (D. Mass. Jan. 7, 2022), the plaintiff asked United States District Judge Indira Talwani to grant its motion to compel against the defendant. The plaintiff had brought a breach-of-contract claim against the defendant, who then counterclaimed for breach of contract and payments under the contract. In this action, the plaintiff wanted the defendant to supplement its production in response to seven Requests for Production (“RFP”), its response to one interrogatory, and its response to one Request for Admission (“RFA”). Judge Talwani granted the motion to compel with respect to the RFA, but otherwise denied it.

With respect to the RFPs, the plaintiff raised three main issues: (1) that the defendant should have produced documents from a third party, (2) that its deletion of former employees’ files was equivalent to spoliation, and (3) that its use of TAR meant that they failed to comply with FRCP 34(b)(2)(C)’s requirement to “state whether any responsive materials are being withheld on the basis of an objection.” Judge Talwani dismissed the first two arguments because the plaintiff could not show a principal-agent relationship between the defendant and the third party, and because there was no dispute that the defendant did not have the responsive former-employee documents, respectively. As to the TAR argument, the defendant countered that plaintiff’s logic was flawed, since there were no discovery requests they could point to that limit or even address the use of TAR, and thus nothing for the court to compel. Judge Talwani agreed, noting that the plaintiff served no discovery request seeking



document review methodology. However, she did not agree with the defendant's assertions that TAR is widely accepted by courts for document review and that plaintiff was incorrect in claiming it resulted in inadequate document review. Rather, she explicitly stated that she was not determining the appropriateness or sufficiency of the use of TAR, and said that if the defendant only produced responsive documents it identified through TAR, it should amend its responses and make clear any limitations.

Scope of Discovery/Proportionality

Discovery is limited to that which is both relevant to the claims and defenses in the litigation and proportional to the needs of the case. Defining precisely where the boundary markers lie that separate the “in scope” from the “out of scope” can be a challenging prospect, as the factors listed in Rule 26(b)(1)(B) are not amenable to bright-line rules. Courts are taking their responsibility to analyze those factors seriously, and the case law increasingly supports the proposition that counsel must present sufficient facts on each element if they want to move a court to adopt their view of the dispute. With that said, and despite various efforts, judicial decisions as well as the e-discovery think tanks have been unable to come forward since the 2015 Amendments with an analytical framework for the application of proportionality in practice. Much work remains to be done in this area.

IN RE 3M COMBAT ARMS EARPLUG PRODUCTS LIABILITY LITIGATION

In **In re 3M Combat Arms Earplug Products Liability Litigation**, 2022 WL 4448917 (N.D. Fla. Sept. 23, 2022), Magistrate Judge Gary Jones denied the defendants’ motion to compel the plaintiffs to produce noise-exposure data recorded by the operating systems for Plaintiffs’ smartphones and smartwatches. “According to Defendants, Plaintiffs’ noise exposure data stored on their smart devices are highly relevant to Plaintiffs’ hearing injury claims and can be collected with only a minimal burden on Plaintiffs.” The plaintiffs objected to the request on substantive and procedural grounds. “Substantively, Plaintiffs argue that Defendants have not shown Plaintiffs used or possessed any post-2019 iOS devices where such data might be stored. Further, Plaintiffs say that the discovery sought is not proportional to the needs of the cases, is overly burdensome, and the burden of producing it outweighs any minimal benefit

achieved by its production.” And “[p]rocedurally, Plaintiffs argue that the motion was not timely made, that Defendants failed to conduct pre-motion conferences, and that if the motion is granted, additional case-specific motion practice will be required as the Defendants’ omnibus motion as to all Wave 2 Plaintiffs fails to account for facts specific to each Plaintiff.” The court discussed iOS devices’ capabilities with respect to recording ambient sound levels, concluding there are significant limitations to the data.

Ultimately, Magistrate Judge Jones concluded that “while there are legitimate concerns about the timing of the motion to compel, timeliness as an independent ground is not a sufficient reason to deny the motion. Instead, because Defendants failed to establish that the noise exposure data would be important to resolving the issues in this case and the burden and expense of collecting and reviewing the hearing data outweighs the likely benefit, the motion to compel fails on proportionality grounds.” Ultimately, “[a]gainst the minimal benefit of the data the burden and expense of producing the data far outweighs any likely benefit.” Magistrate Judge Jones therefore denied the motion.

AMERICAN ATHEISTS, INC. v. RAPERT

In **American Atheists, Inc. v. Rapert**, 2022 WL 2959908 (E.D. Ark. July 26, 2022), District Judge Kristine G. Baker granted the plaintiffs’ motion to compel discovery on every count and held that they could submit a petition for attorneys’ fees should they choose to do so. The plaintiffs filed suit against the defendant, a state senator, in his official and individual capacities. They asserted various constitutional and state claims, including viewpoint discrimination, violation of their right to free exercise of religion, and equal protection violations.

In their first RFP, the plaintiffs requested information and documents relevant to the defendant's non-privileged communication regarding this litigation, information pertaining to his social media presence, and information pertaining to his use of information technology. They served the defendant in March 2021 and went back and forth with his attorneys in a good-faith effort to secure his compliance until September 2021, when they thereafter filed this motion to compel. Judge Baker first analyzed whether the plaintiffs made a good-faith effort to confer with the defendant, and concluded that they did, based on their attachment of several correspondences in which they reached out to the defendant's individual and official-capacity counsel on multiple occasions, with no success in securing compliance with discovery.

Judge Baker then went through each of the plaintiffs' requests for compelled discovery. The requests were that the defendant: (1) respond to Interrogatory Nos. 12 and 13 in the plaintiffs' official-capacity requests; (2) supplement his responses to Interrogatory Nos. 4, 5, 6, 8, and 17 in the plaintiffs' official-capacity requests, and Interrogatory Nos. 1 and 2 in the plaintiffs' individual-capacity requests; (3) produce documents responsive to RFP Nos. 4, 6, and 7 in the plaintiffs' official-capacity requests, and RFP Nos. 1, 2, 3, and 4 in the plaintiffs' individual-capacity requests; (4) supplement his responses to RFP Nos. 2, 3, and 9 in the plaintiffs' official-capacity requests; and (5) pay the plaintiffs' reasonable costs and attorneys' fees incurred as a result of the plaintiffs' filing this motion to compel. The Interrogatories and RFPs asked the defendant to identify and produce documents pertaining to: Arkansas state government employees and contractors; every social media account under his control since May 18, 2014, as well as every instance in which he restricted or considered restricting a person's ability to interact with one of the accounts, and all changes made to every account since October 2, 2018; all correspondence of his, including social media, that contained certain

key words; all correspondence he received that claimed to have reported content on his social media accounts; and all internet service providers and mobile data providers he contracted with on or after May 18, 2014, as well as all devices used to access social media.

The defendant provided boilerplate objections to every motion to compel, broadly arguing that the information the plaintiffs sought was either publicly available or available through third-party sources, that much of the requested information was protected by attorney work-product and/or attorney-client privilege, and that the information sought was "unduly burdensome, fail[ed] to identify the documents sought with reasonable particularity," and "disproportionate to the needs of the case." Judge Baker disagreed in each instance, repeatedly noting that an opposing party's ability to obtain the information through a third party is irrelevant, and that if a defendant has responsive information or documents, they still have to provide them. She also concluded that the information was sufficiently relevant and ordered the defendant to either produce the documents or a privilege log for each withheld document. Judge Baker also held that the defendant's privacy concerns were not a sufficient basis on which to refuse to comply with discovery, as he could have applied for a protective order. Finally, Judge Baker held the plaintiffs could file a petition for attorneys' fees, since the defendant did not respond to any of the plaintiffs' requests to get him to comply with discovery, and because he doubled down on his boilerplate objections without requesting a protective order or submitting a privilege log.

EDWARDS v. MCDERMOTT INTERNATIONAL, INC.

In **Edwards v. McDermott International, Inc.**, 2022 WL 1568279 (S.D. Tex. May 18, 2022), Magistrate Judge Andrew M. Edison was asked by the parties to decide the appropriate scope of discovery. A decision in favor of the plaintiffs' proposed search

terms would have required the defendant to review close to 1.3 million documents. Thus, the proportionality of the proposed search was at issue in this case, and Magistrate Judge Edison ran through each of the six proportionality factors individually in coming to his conclusion.

The first and second factors, the importance of the issues at stake and the amount in controversy, weighed in favor of the plaintiffs, as this was an important suit with over \$1 billion claimed in damages. The third factor, the parties' relative access to relevant information, also weighed in favor of the plaintiffs, as the information at stake was emails and other electronic communications maintained by the defendants. The fourth factor, the parties' resources, was neutral, as Magistrate Judge Edison was unaware of the parties' resources and neither side offered evidence. The fifth factor, the importance of discovery in resolving the issues, weighed in favor of the plaintiffs, as did the sixth factor, the importance of the discovery in resolving the issues. Magistrate Judge Edison said "what ultimately sway[ed]" him was that another judge had denied the defendants' motion to dismiss the claims, which meant the door for discovery had "swung open." He again emphasized the large amount of damages at stake, and ordered the defendants to apply the plaintiffs' proposed search terms.

JIM HAWK TRUCK-TRAILS OF SIOUX FALLS, INC. v. CROSSROADS TRAILER SALES & SERVICE, INC.

In **Jim Hawk Truck-Trails of Sioux Falls, Inc. v. Crossroads Trailer Sales & Service, Inc.**, 2022 WL 3010143 (D.S.D. July 29, 2022), District Judge Karen E. Schreier granted in part and denied in part the plaintiff's motion to compel discovery. The plaintiff sued the defendant for multiple claims, including misappropriation of trade secrets, breach of the duty of loyalty, and unfair competition. The parties exchanged correspondence and met and

conferred extensively after the plaintiff served its first discovery requests, but were unable to resolve several issues, which eventually led to this motion to compel discovery.

The plaintiff moved on multiple requests for production and interrogatories. Notably, the plaintiff sought an order compelling the defendant to run additional search terms to which the defendant had not agreed. The defendant had already conducted searches using 92 terms and/or strings, but the plaintiff wanted them to run seven more. The defendant objected, claiming this would be unduly burdensome. Judge Schreier observed that discovery may be limited if the party resisting discovery can establish that the source is "not reasonably accessible because of undue burden or cost" pursuant to FRCP 26(b)(2)(B). Here, Judge Schreier found that the ESI subject to plaintiffs' terms was not reasonably accessible. First, Judge Schreier found the marginal burden of the additional terms would be substantial, based on the defendant's showing that the additional searches would require roughly \$3,150 to \$4,275 in processing costs, and roughly \$114,000 in lawyer's fees. However, Judge Schreier noted that discovery can nevertheless be ordered despite not being reasonably accessible, so long as the requesting party shows good cause. She therefore analyzed the plaintiffs' request according to seven factors outlined in the Advisory Committee notes to Rule 26 to help courts consider whether good cause has been shown: "(1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties'

resources.” Judge Schreier stated that the first factor weighed in favor of plaintiff because the request was sufficiently specific, while the second factor weighed in favor of the defendant because there had been “extensive discovery in this case” and defendant had “already produced ESI responsive to 92 search terms of 13 employees’ data” from which a “vast quantity of information is already accessible.”

Most notably, Judge Schreier found that the fourth and fifth factors favored defendant because the responsiveness rate of these search terms would be “incredibly low.” She observed that the defendant’s review to date had revealed an overall relevance rate of only seven percent among the documents searched. While the plaintiff argued that there still could be relevant documents among those returned by the new terms, and that those terms corresponded with facts from the case, Judge Schreier concluded the newly searched ESI was unlikely to contain important information based on the low rate of relevance to date.

Judge Schreier explained that the good-cause factors were not a checklist, but rather “should be weighed by importance.” She found that here, the “low likelihood of finding relevant, responsive information is the most important ‘good cause’ factor.” In light of this, she held that the low probability of the search terms yielding new and relevant information did not justify the substantial burden and expense required by the discovery sought. She denied the motion.

EDITOR’S NOTE

We typically expect that federal courts will analyze questions of expanding the scope of discovery from existing sources under FRCP 26(b)(1) by questioning whether the additional discovery is both relevant to the claims and defenses in the case and also proportional to the needs of the case. Here, Judge Schreier relied on Rule 26(b)(2)(B), which focuses on whether discovery should be sought from sources that are not reasonably accessible due to undue burden or cost—somewhat unusual since the search terms

the plaintiff sought to compel were to be run against a corpus of documents that the defendant had already accessed, collected, and searched. Nevertheless, Judge Schreier essentially conducted a relevance and proportionality analysis to assess whether the marginal utility of the discovery would outweigh the marginal cost to conduct it, and although the balancing factors under 26(b)(2)(B) are different than the proportionality factors under 26(b)(1), we expect she would have reached the same conclusion under the latter.

MOBILE EQUITY CORP. v. WALMART, INC. (SLACK)

In **Mobile Equity Corp. v. Walmart, Inc.**, 2022 WL 36170 (E.D. Tex. Jan. 4, 2022), United States Magistrate Judge Ron Payne heard a series of cross-motions to compel filed by the plaintiff and the defendant. One of the plaintiff’s motions involved a Motion to Reopen Hearing on its first motion to compel, which required the defendant to produce additional source code information, Slack channels, and Jira documentation.

The case involves allegations that the defendant infringed on certain software patents held by the plaintiff. Magistrate Judge Payne granted the plaintiff’s Motion to Reopen Hearing on its first motion to compel. He opined that he was “gravely concerned about the continuing resistance—and perhaps defiance—[Defendant] has shown with respect to the full production of its source code and accompanying documentation.” He noted, for example, that he had previously ordered the defendant “to produce any source code contained in [the ‘Store Services’] module,” but that the defendant had not done so. Magistrate Judge Payne stated that he believed “plaintiff has demonstrated there is additional source code in the ‘Store Services’ module that [Defendant] failed to produce, despite this Court’s order.” He therefore ordered the defendant to export all code in its GitHub directory for “Store Services,” to produce in native format all “Jira documents” described in the plaintiff’s briefing, and to produce Slack channels relevant to the “Store Services” topic. Magistrate


Judge Payne noted, however, that the plaintiff had identified as potentially relevant “roughly forty” Slack channels. He did not order production of all 40 because “the Court is sensitive to the burden that [Defendant] would incur if all forty channels are ordered to be produced.” Consequently, he ordered the parties “to meet and confer and narrow the list of forty channels. The Court is hesitant to place a limit on the number of channels that are to be produced but will resolve any dispute remaining after the parties’ efforts.”

RAVIKANT v. ROHDE

In **Ravikant v. Rohde**, 2022 WL 1177342 (S.D.N.Y. Mar. 18, 2022), Magistrate Judge Ona Wang denied the plaintiff’s motion to compel and granted the defendant’s motion for a protective order. “In August 2021, Defendants provided Plaintiffs with Dr. Alukal and Nurse Rovano’s treatment records. After 5pm on Friday, February 18, 2022, Plaintiff served Defendant NYPH with a Notice of Deposition pursuant to FRCP 30(b)(6). The deposition was set to occur . . . 4 business days later.” The court noted that “Plaintiff’s Notice did not provide reasonable notice of the deposition. Rule 30(b)(6) requires that a party who wants to depose a person by oral questions must give ‘reasonable written notice to every other party.’ Fed. R. Civ. P. 30(b)(1). Particularly where there is no stated urgency, or well-articulated need for this information, this notice is unreasonable.” Moreover, “[t]he Court ha[d] previously voiced concerns ‘about proportionality and unnecessary motions practice,’ as it relates to the Plaintiff’s demands for additional records from NYPH (among other things).” Magistrate Judge Wang summarized her view of this dispute: “Plaintiff seeks—on an unreasonable timetable—depositions and documents that are substantively duplicative of what he already has. Plaintiff does this without any explanation of how or why the metadata sought would be at all helpful or even relevant in proving his claims.” Magistrate Judge Wang denied the motion.

SAINT CLAIR COUNTY EMPLOYEES’ RETIREMENT SYSTEM v. ACADIA HEALTHCARE

In **Saint Clair County Employees’ Retirement System v. Acadia Healthcare**, 2022 WL 4095387 (M.D. Tenn. Sept. 7, 2022), Magistrate Judge Alistair Newbern granted the plaintiffs’ request for production. In this class action, Plaintiffs filed a “motion to compel [that] identifies eleven requests for production that address Acadia’s relationship to Priory, Acadia’s U.K. operations, and the retention of documents related to this action by Acadia and Priory.” In response, “Defendants . . . produced discovery responsive to Plaintiffs’ requests for production collected from Acadia custodians located in the United States. Plaintiffs now move to compel Defendants to collect and produce discovery responsive to these requests from the following sources located in the U.K.” And Acadia objected to the request, asserting that it would be burdensome to collect the information from outside the U.S. and in compliance with foreign law. The court reminded that “the scope of discovery is within the sound discretion of the trial court[.]” And “[t]he party moving to compel discovery bears the initial burden of proving the relevance of the information sought.” Having met that burden, “Rule 26 requires generally that discovery be ‘proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.’” “[T]he party resisting discovery bears the burden of demonstrating why the request is unduly burdensome or otherwise not discoverable under the Federal Rules.” Having gone through these factors, Magistrate Judge Newbern concluded that the information requested was relevant, and it was unavailable from other sources. “However, having reviewed the proposed



search terms to be applied to the Priory Custodians and the shared noncustodial drives, the Court finds that they can and should be narrowed to avoid cumulative production. Given the additional costs Defendants cite of reviewing the production to comply with the U.K.'s data protection laws, the search terms should be specifically tailored to avoid production of ESI that already been identified and produced from U.S. custodians.”

Possession, Custody, or Control

The changing nature of the workplace and the ways that employees and agents access, manipulate, and share documents and communications, mean that questions about who owns, controls, or has the right or ability to collect, preserve, and produce ESI can require careful analysis of complex, highly contextual facts. These cases highlight whether the traditional notions of possession, custody, and control—as well as the existing legal framework around this important issue—are sufficient to account for the manner in which ESI is being generated, stored, transferred, and communicated.

IN RE PORK ANTITRUST LITIGATION (TEXT MESSAGES)

In *In re Pork Antitrust Litigation*, 2022 WL 972401 (D. Minn. Mar. 31, 2022), plaintiffs allege “that Defendants, among America’s largest port producers and integrators, conspired to limit the supply of pork and thereby fix prices in violation of federal and state antitrust law.” Plaintiffs allege defendants were able to carry out the conspiracy in two ways: by exchanging detailed, competitively sensitive, and closely guarded nonpublic 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 by signaling the need to cut production through public statements aimed at one another. Plaintiffs sought communications and meetings between the defendants or related to the lawsuit’s subject matter, and information regarding supply, demand, and price of pork products. Plaintiffs and defendants were unable to reach an agreement regarding custodians and text message imaging.

Plaintiffs sought an order before Magistrate Judge Hildy Bowbeer compelling one defendant to produce text messages from currently employed custodians, declaring the defendant had an obligation to image text messages from all of its custodians’ personal phones and cloud backups, and enforcing subpoenas against defendant’s custodians. Plaintiffs argued that Defendant had “control” of the custodians’ personal text messages because its “bring your own device” (BYOD) policy required employees to use their cell phones to conduct business.

Magistrate Judge Bowbeer disagreed with plaintiffs and denied the motion to compel. Judge Bowbeer found that the defendant did not have the legal right to obtain the text messages on personally owned cell phones, and that plaintiffs misconstrued the defendant’s BYOD policy because there was nothing in the policy that required any employee to use a personally owned phone to conduct work. The court also rejected plaintiffs’ argument that because the defendant may have “a practical ability to demand” the employees turn over their personal devices, that defendant had “control” over the devices.

Judge Bowbeer did find that plaintiffs’ subpoenas to the non-party custodians should be enforced, as the subpoenas were not ambiguous and vague, they would likely lead to responsive information, and there was no burden argument made to support the custodians’ position.

EDITOR’S NOTE

This decision exemplifies the current minefield and confusion surrounding an employer’s possession, custody, and control over its employees’ personal devices, data, or even corporate information stored on such devices. Employers have legitimate concerns of violating state and federal privacy laws by engaging in authorized access to employee personal devices and data. At the same time, the

corporate data stored on such devices is the property of the employer—not the employee. That may not mean, however, the employer has either the legal right or practical ability to preserve, collect, or produce that information. We recommend that employers continue to update their BYOD and Device Use policies to be consistent with applicable laws and regulations in this important area.

R & R PACKAGING, INC. v. EVENFLO CO., INC.


In **R & R Packaging, Inc. v. Evenflo Co., Inc.**, 2022 WL 1086206 (W.D. Ark. Apr. 11, 2022), plaintiff filed a motion to compel discovery and for sanctions. The case revolved around “a patent dispute over technology that alerts users when a child may have been forgotten in a car seat.” Plaintiff claimed that defendant obtained sensitive information from the plaintiff during licensing or purchasing negotiation. Plaintiff added that after disclosing this information to defendant, the defendant broke contact and released a product of its own. Defendant argued that materials plaintiff sought were not within the defendant’s control. Defendant also argued that plaintiff’s requests placed an undue burden on it and were not proportional to the needs of the case. District Judge P.K. Holmes found that the defendant did retain control over the materials. Judge Holmes stated that to whatever extent the defendant does not understand the material sufficiently to discern which portions are relevant to the plaintiff’s claim, it is the defendant’s obligation to acquire sufficient understanding. Judge Holmes added that “the Court also cannot overlook that it had to spend far more time working to resolve the issues raised in this motion than is typically necessary on discovery motions, and that on every single issue.” Judge Holmes found that the defendant’s arguments concerning undue burden and proportionality were conclusory and lacked evidence regarding time or expense. The court granted the plaintiff’s motion to compel discovery and for sanctions.

SIGNIFY HOLDING B.V. v. TP-LINK RESEARCH AMERICA CORP.

In **Signify Holding B.V. v. TP-Link Rsch. Am. Corp.**, 2022 WL 3656315 (S.D.N.Y. Aug. 25, 2022), plaintiff and defendants disputed whether defendants’ non-party affiliate in Hong Kong must pay royalties to plaintiff under a patent-licensing agreement. During settlement discussions, defendants and their non-party affiliate used the same legal counsel in negotiations. The non-party affiliate produced certain files to plaintiff. The settlement negotiations did not bear fruit, and plaintiff was ordered to destroy the documents it obtained during settlement and to proceed with discovery against the defendants. During discovery, the defendants refused to produce files that the non-party affiliate produced in settlement negotiations, arguing they were not in their possession, custody or control. Plaintiffs moved to compel defendants, or defendants’ counsel, to produce the files.

United States Magistrate Judge Katherine Parker denied the motion to compel. First, Magistrate Judge Parker rejected compelling defendants’ legal counsel to produce the documents, noting that “it is not correct that a client has control over its attorneys’ other clients’ documents also possessed by the attorneys. Such a rule would turn client confidentiality on its head and ride roughshod over attorney ethical obligations to their clients.”

Magistrate Judge Parker next turned to the question of whether the defendants either directly possess the documents, or whether they have the practical ability to obtain the documents, which is the Second Circuit’s standard for determining possession, custody, or control. Regarding the latter, Magistrate Judge Parker found that the plaintiffs did not meet their burden, as the fact that (i) the non-party affiliate voluntarily stepped into joint negotiations with defendants to resolve the



royalties dispute, (ii) the non-party affiliate supplied products to defendants, and (iii) the defendants and the non-party affiliate are under the same corporate umbrella and share counsel were insufficient to show the defendants had the practical ability to obtain the documents. However, Magistrate Judge Parker ordered defendants to state whether they possessed the documents themselves, and if so, to produce them.

STAFFORD v. BOJANGLES’ RESTAURANTS INC. (TEXT MESSAGES)

In **Stafford v. Bojangles’ Restaurants Inc.**, 2022 WL 2680040 (W.D.N.C. July 11, 2022), United States Magistrate Judge David Cayer was asked to consider the plaintiffs’ motion to compel discovery responses. The matter involved wage-hour claims by employees of the defendant’s restaurants. Plaintiffs sought to compel defendant “to fully and completely respond to their second set of requests for production of documents,” to include production of “emails and text messages [between] Unit Directors and Area Directors” and the plaintiffs. Defendant asserted that it has produced all documents in its “possession, custody, or control” that are responsive to plaintiffs’ requests. Magistrate Judge Cayer granted the plaintiffs’ motion in part, ordering production of emails and texts, but refusing to order production of texts from the personally owned phones of the targeted Unit and Area Directors. Magistrate Judge Cayer cited several cases for the proposition that “a company does not possess or control the text messages from the personal phones of its employees and may not be compelled to disclose text messages from employees’ personal phones.”

Search and Production

As the type, amount, and location of ESI generated and stored by organizations continues to grow dramatically, the issue of when, whether, and how to search for those materials is experiencing growth as an area of discovery motions practice. The cases highlight the need to implement and document reasonable procedures and processes around the identification, search, and collection of custodian and non-custodial sources.

BENANAV v. HEALTHY PAWS PET INSURANCE, LLC

In **Benanav v. Healthy Paws Pet Insurance, LLC**, 2022 WL 3587982 (Aug. 22, 2022), United States District Judge Lauren King found that “Plaintiffs’ unilateral ‘self-search’ is inconsistent with Plaintiffs’ commitment, undertaken in the ESI Protocol, to ‘work in good faith to agree on the use of reasonable search terms ... along with any other relevant search parameters,’” and ordered the parties “to meet and confer in good faith to negotiate search terms that are designed to capture documents that are responsive to Healthy Paws’ discovery request.”

The defendant questioned the steps the plaintiffs took to search for and produce responsive ESI. It objected to the plaintiffs’ self-searching, their continued refusal to produce load files or metadata, and to deficiencies in their production, including missing attachments in response to the defendant’s production requests. The court noted that, “self-collections by document custodians tend to give rise to ‘questions regarding the accuracy and completeness of collections if directions and oversight by legal counsel or forensics experts are poor or non-existent.’” Judge King remarked that plaintiffs “provide[d] only a vague explanation of how counsel supervised and directed each Plaintiff in searching for and identifying responsive documents” and did not provide the defendant with

additional explanation it requested of the search criteria used by each of the plaintiffs. The court wrote that “[t]he[] defects in Plaintiffs’ manual self-search are sufficient to highlight the risks of such self-search processes: ‘parties and counsel that embark on self-collection can soon encounter multiple pitfalls that can sidetrack the litigation and lead to motions to compel, spoliated evidence, and even sanctions.’ The pitfalls include the client’s failure (1) ‘to identify all sources of responsive information,’ (2) ‘to preserve evidence,’ (3) to ‘find or provide to counsel all responsive documents and ESI,’ or (4) to ‘fully document how they conducted their searches.’”

BOYD v. LAZER SPOT

In **Boyd v. Lazer Spot**, 2022 WL 2865881 (N.D. Ill. July 6, 2022), United States Magistrate Judge Maria Valdez granted the plaintiff’s motion in part, denied in part. The defendant claimed that it has already produced “all free standing electronic documents that it could find with a reasonable search – including electronically stored documents in a folder.” In adjudicating ESI issues for purposes of the plaintiff’s motion to compel, the Court said it “[wa]s hamstrung by the fact that Defendant has not provided any fulsome explanation of the ESI methodologies it has already employed. Given Defendant’s lack of any real explanation in that regard, the Court is not now in a position to rule on the sufficiency of Defendant’s ESI searches.” The court concluded that granting the plaintiff’s request that the defendant be compelled to “produce all responsive ESI” would be meaningless since it remains unclear what ESI search efforts the defendant has already undertaken and whether it is holding back any documents. The Court determined that the best solution was to require the parties to meet and confer on the topic of ESI. Magistrate Judge Valdez ordered the defendant to “falsomely explain its ESI search methodologies.”

To the extent he intends to remain lead counsel for the defendant, Eric Samore is directed to inform himself of the defendant's search methodologies and to personally participate in the ESI conferrals with Plaintiff's counsel. Consistent with the rulings above, to the extent the parties' conferrals lead the defendant to run additional ESI searches, the defendant shall promptly produce any newly found documents responsive to Plaintiff's Requests for Production Nos. 14 and 15.

CARL ZEISS MEDITECT, INC. v. TOPCON MEDICAL SYSTEMS, INC.

In **Carl Zeiss Meditect, Inc. v. Topcon Medical Systems, Inc.**, 2022 WL 2394815 (N.D. Cal. July 1, 2022), United States Magistrate Judge Laurel Beeler granted Zeiss's motion to compel Topcon's discovery contractor's search protocols. Zeiss filed a motion to compel Topcon to disclose the custodians being searched and the search parameters and protocols challenged. "Zeiss wants a collaborative process to make sure that the Kroll audit accomplishes the audit's goals. To that end, (1) it wants disclosure of the custodians being searched and the search parameters and protocols, and (2) it defines the appropriate custodians (in sum) as Topcon employees who acquired, sent, received, or accessed Zeiss files or who worked on products that competed with Zeiss products (specifically the Harmony product, including its 'decoder' feature and its plug-ins, and including the Glaucoma Module and the now-discontinued Retina Module)." Zeiss challenged Topcon's search on the ground that it is inappropriately narrow because Topcon's trade-secrets misappropriation is broader than the search terms Topcon employed. The court ordered Topcon to produce the discovery contractor's search protocols within 30 days.

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION v. QUALTOOL, INC.

In **Equal Employment Opportunity Commission v. Qualtool, Inc.**, 2022 WL 16963829 (M.D. Fla. Nov. 16, 2022), United States Magistrate Judge Phillip R. Lammens granted in part, and denied in part, Plaintiff's motion to compel. Plaintiff originally filed a motion to compel Defendant to (1) produce documents in a usable format and in a manner requested by the Plaintiff; (2) provide an affidavit listing ESI repositories; and (3) cease unsupervised ESI self-collection and conduct supervised searches. Judge Lammens denied Plaintiff's initial motion to compel, finding that Defendant "made a good faith effort to comply with all of Plaintiff's requests and has even offered to allow Plaintiff to search the computers and give additional search terms." Plaintiff filed this subsequent motion to, among other demands, compel Defendant to re-run searches using specific terms, custodians and agreed-upon software, and to produce its email search history to disclose how it ran the agreed-upon searches.

Plaintiff specifically requested Defendant run six search terms on six email accounts and five computers using Outlook and Windows File Explorer computer software. After conferring with Defendant, Plaintiff sent Defendant an email noting that "Qualtool agreed to search the entirety of all ESI documents using those terms." Defendants responded to Plaintiff's email with a list of ten email addresses that may be repositories for the searches and stated "please let me know what other search terms you propose beyond those I provided to you a few months ago." After several subsequent meet and confers, Defendant stated that it would run only five of the Plaintiff's proposed searches against only two computers and two email addresses, and that none of these contained any responsive documents. Defendant did not indicate how it ran the searches it agreed to run.

Judge Lammens granted Plaintiff's motion with respect to search terms, sources, and method of search, relying upon the parties extensive conferrals. Notably, while he observed that "the Sedona Principles caution that the parties must cooperate to craft search terms that will effectively capture all relevant information without being too burdensome," he cautioned that "this cooperation must be in good faith, consistent with the local rules." He also took note of case law supporting the proposition that "[w]hen a party has limited the search terms following conferral according to the opposing party's input, that has been found sufficient to compel the opposing [sic] party to run the search." Judge Lammens therefore ordered the Defendant to run all of the search terms proposed by the Plaintiffs, and also to run those searches using Outlook and Windows File Explorer, exactly as Plaintiff had requested. Judge Lammens denied, however, Plaintiff's request for Defendant's Outlook search history to determine if the searches were run correctly. Judge Lammens noted that Defendant's counsel represented that the searches were properly executed, making this request unnecessarily burdensome without a specific allegation of misconduct.

FAMULARE v. GANNETT CO., INC.

In **Famulare v. Gannett Co., Inc.**, 2022 WL 815818 (D.N.J. Mar. 17, 2022), United States District Judge William Martini upheld Magistrate Judge Hammer's discovery order. "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." Magistrate Judge Hammer held a telephonic hearing. 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."

Judge Hammer concluded that a Rule 30(b)(6) deposition of an appropriate representative was "clearly going to have to happen" to allow the plaintiff to investigate why "all they can get in response to the document production request is the Excel spreadsheet." Judge Hammer also informed the defendants that "to the extent they "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." The defendants challenged Magistrate Judge Hammer's order. Judge Martini concluded: "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."

MARTLEY v. CITY OF BASEHOR

In **Martley v. City of Basehor**, 2022 WL 1302820 (D. Kan. May 2, 2022), United States Magistrate Judge Gwynne Birzer ordered subpoenas of the City's former IT service provider, NetStandard, be quashed. The city "object[ed] to the subpoena pursuant to Federal Rules 26(c), 34, and 45(a)(4)." Specifically, they argued that the subpoena was issued in violation of Fed. R. Civ. P. 45(a)(4) because Defendants were not provided notice of the subpoena before it was served upon NetStandard. Additionally, Defendants argued that the plaintiff attempted to use a subpoena to avoid compliance with Federal Rules 26 and 34. They argued that the plaintiff sought to obtain documents via subpoena after failing to obtain them when he served his Sixth

Request for Production too late for the response to occur prior to the close of discovery.” The Court did “not believe a third-party subpoena to NetStandard is the appropriate vehicle to get the information Plaintiff seeks.” However, Magistrate Judge Birzer was “trouble[d] . . . that documents continue[d] to come to light [that] are presumably responsive to requests for production Plaintiff . . . served” The Court determined that Martley had provided adequate notice to the City, but the Court was “uncomfortable with Plaintiff’s tactic of going around Defendants to their former IT vendor to conduct searches on any of the City’s email data it may still have in its possession after its services were terminated.” Moreover, the Court “question[ed] whether the documents are in the control of NetStandard and questions whether it should be burdened with the production.” Ultimately, the Court concluded that the City had control of any documents still in NetStandard’s possession and quashed the subpoena.

RAINE GROUP LLC v. REIGN CAPITAL

In **Raine Group LLC v. Reign Capital, LLC**, 2022 WL 538336 (S.D.N.Y. Feb. 22, 2022), United States Magistrate Judge Katharine Parker was asked to resolve disputes between parties their respective search obligations. The court founds that the Defendant’s proposed language was unnecessary. Specifically, the requested language requiring parties to search “all company files” or “all files from all employees” was overbroad. The court analyzed each of the proposed search terms to determine whether they were relevant and could produce responsive ESI. The court ruled that the term “real estate” was too broad, even with modifiers. The term “lawsuit” did not have to include the plaintiff’s name because it could return documents pertaining to other lawsuits that are irrelevant to the current matter. The court allowed the usage of the terms “sophisticated” and “trademark” because the terms were focused on

issues relevant to the case. Judge Parker required the parties to submit a revised ESI protocol consistent with these rulings.

ROBINSON v. DE NIRO

In **Robinson v. De Niro**, 2022 WL 229593 (S.D.N.Y. Jan. 26, 2022), United States Magistrate Judge Katharine Parker denied Canal Productions, Inc. and Robert De Niro’s motion to compel the plaintiff to produce documents from one of her former email accounts and for their costs associated with having to file this motion. The plaintiff opposed the motion because the email account at issue is old and inaccessible, contains little relevant information, and any relevant information it does contain can be or has been provided from a more readily accessible source. The parties negotiated an ESI protocol pursuant to which they would search for electronically stored information. As part of the protocol, each party identified sources of relevant information. The plaintiff identified two personal email accounts which she agreed to search. On the last day of document production, the plaintiff delivered several boxes of hard copy documents and other tangible items to defense counsel. In the course of reviewing the documents, defense counsel discovered another personal AOL email address that Plaintiff utilized during the time she was employed by Canal, but that had not been identified by Plaintiff during the negotiation of the ESI protocol. The email address was revealed on certain Caviar receipts. The court noted that “[w]hen served with a document demand pursuant to Rule 34, a party has a duty to conduct a reasonable inquiry for responsive documents.” However, a party is only required to produce documents in that party’s “possession, custody or control.” The Court noted that “[d]ifficulty accessing an account is not the same as not having possession, custody and control.” Because the plaintiff had already produced the requested documents from another source, the Court concluded that the plaintiff did not need to obtain

access to the AOL account. The Court reminded the parties that the federal rules do not require production of redundant information.

SIMON AND SIMON PC v. ALIGN TECHNOLOGY, INC.

In **Simon and Simon PC v. Align Technology, Inc.**, 2022 WL 2387729 (N.D. Cal. July 1, 2022), United States Magistrate Judge Thomas Hixson granted the plaintiffs' motion to compel and ordered the defendant to re-run the search strings without geographic limiters. The plaintiffs sued the defendant under the Sherman Act for allegedly anticompetitive conduct that took place in the United States. Judge Hixson noted that since the defendant was "an international business, it [had] a legitimate reason to limit document review to documents that are likely to be evidence of conduct in the United States. The most common way of doing this is by choosing custodians whose work involves the U.S. market" For most of the search strings it agreed to run, the defendant included geographic limiters in the string, such as "U.S." or "American." The plaintiffs said that they agreed to the use of geographic limiters, reserving their right to challenge them later, because the defendant represented that its employee email signatures typically contain one or more of the geographic limiters at issue. In their motion to compel, the plaintiffs now assert that the defendant's employee emails "almost always have either no signature at all or signatures without geographic limiters." The court ultimately found the defendant's arguments for limiting its search using geographic limiters unpersuasive. The defendant could make no representation as to how many employees used email signatures with geographic limiters in them, and Judge Hixson noted that it was illogical to expect that American employees would explicitly reference America every time they communicated. Therefore, Judge Hixson concluded, a lot of relevant communications were likely excluded from the search. Due to this, Judge Hixson found restraining the search via these

geographic limiters to be an arbitrary and irrational limitation on discovery, and ordered the defendant to re-run the searches without them.

IN RE TELESCOPES ANTITRUST LITIGATION

In **In re Telescopes Antitrust Litigation**, 5:20-cv-03642-EJD, Dkt. 255 (N.D. Cal. Aug. 22, 2022), United States Magistrate Judge Virginia Demarchi denied the Direct Purchaser Plaintiffs' ("DPPs") motion to compel. The DPPs asked "the Court to order Defendants to (1) certify that they have now substantially completed their document production and are not withholding any other potentially responsive documents pending further review for undisclosed purposes; (2) disclose to the DPPs the criteria Defendants used to identify the collection of 51,500 documents as sensitive or potentially privileged and how they made their determinations that some of these documents are non-responsive; and (3) show cause why they should not be sanctioned for violating the Court's scheduling order setting deadlines for the substantial completion of document production and the production of privilege logs." The defendants did not challenge that they failed to comply with the court's scheduling order regarding this production. DPPs contend the delay was intentional "so that they could conduct a supplementary review of these documents, without informing Plaintiffs of what they were doing and how they were doing it . . ." DPPs suggest in their briefing that the defendants were required to produce all documents that hit on a court-ordered search term and prohibited from using any criteria or methods to cull documents from review without first disclosing those criteria or methods to the plaintiffs in advance. The court disagreed. Moreover, Magistrate Judge Demarchi concluded that the DPPs had obtained substantial all the relief that had requested before she had ruled. The court, therefore, denied the DPPs motion to compel and for sanctions.

TERPIN v. AT&T INC.

In **Terpin v. AT&T Inc.**, 2022 WL 3013153 (C.D. Cal. June 13, 2022), the plaintiffs asked Magistrate Judge Karen L. Stevenson to grant a motion to compel discovery. They wanted the defendants to expand the document production date range by a year and produce the search terms used in their ESI searches. The plaintiff had sued the defendant for a variety of claims, including negligence and breach of contract, after the plaintiff was the victim of a “SIM swap” in which hackers disabled their phone and transferred their account data, resulting in the theft of \$24 million in cryptocurrency from their wallets. They wished to expand the document production date range so that it would begin on January 1, 2015, as opposed to January 1, 2016, because they claimed an internal document from September 2015 referred to “identified unauthorized SIM swapping . . . as a ‘Hot Fraud Issue’” would help prove the foreseeability of the theft. The defendant argued this expansion was unnecessary both because the current range already fully showed the state of their knowledge leading to the swap, and because the document in question related to fraud against the defendant, not fraud against consumers. The plaintiff also wished to compel the defendant to disclose its ESI search terms so the completeness of discovery could be measured, which it referred to as a “customary and standard litigation practice.” The defendant argued this was not a “fundamental requirement” under the Federal Rules of Civil Procedure, and noted that where courts had allowed discovery into search terms after document production had occurred, it was because the court had already determined a party’s investigation and witness preparation for a deposition were inadequate.

Magistrate Judge Stevenson denied the motion to compel discovery on both grounds. She denied the motion to expand the date range primarily because she found the article in question to be of little relevance. She noted that the document was dated

just a few months prior to the January 1, 2016, discovery date, which did not justify expanding the search all the way back to January 2015. Magistrate Judge Stevenson then went through each Rule 26(b)(1) proportionality factor and concluded that even if the document was arguably relevant, expanding the search would certainly not be proportionate to the needs of the case. She also denied the motion to compel the defendant to provide their ESI search terms, agreeing with the defendant that this was not a “fundamental discovery requirement,” even if parties regularly agree to it. She also agreed that the plaintiff had not alleged any deficiencies in searches or disclosures, and stated that the plaintiff’s “speculation about possible deficiencies in Defendant’s search procedures do not support an order compelling AT&T to produce discovery.”

Forensic Examinations

Today, forensic examination of an opponent's electronic devices is the exception rather than the rule, reserved for situations where the opponent has manifestly failed to meet its discovery obligations or where the litigation revolves around a trade secret issue (e.g., who had access to data, whether that data was accessed, what devices that data sat upon). Even in those situations, however, that solution must be proportional to the needs of the case and in service of discovery into matters relevant to the claims and defenses. Courts increasingly analyze requests to compel the surrender and forensic examination of devices through the lens of the proportionality factors of Rule 26(b)(1)(B). The following cases demonstrate that a movant seeking such an order faces a high bar to show its necessity and fairness.

AMINOV v. BERKSHIRE HATHAWAY GUARD INSURANCE COMPANIES

In **Aminov v. Berkshire Hathaway Guard Insurance Cos.**, 21-CV-479-DG-SJB, 2022 WL 818944 (E.D.N.Y. Mar. 3, 2022), Magistrate Judge Sanket J. Bulsara denied the defendant's motion to compel the plaintiff to produce the cell phone that recorded videos produced by the plaintiff for forensic examination. He noted that "forensic examinations of computers and cell phones are generally considered a drastic discovery measure because of their intrusive nature," and held that there was no justification for ordering it in this case. Magistrate Judge Bulsara found that the motion itself was based on "misplaced and unsupported speculation." The defendant alleged that there was reason to believe the video's metadata was altered, but this determination came from a free online metadata tool whose reliability was never asserted. Further, the metadata tool's website only said the data "could have been altered," which was a blanket statement that appeared automatically for

every file uploaded on the website as a means of liability protection. Judge Bulsara observed, "This is hardly the kind of analysis or support that provides a reasonable basis to conclude that there was an alteration of metadata or to warrant forensic examinations." The two experts the defendant consulted also did not provide this basis, as one never claimed the plaintiff's files had missing or altered metadata, and the other was not a computer expert and only made an unsupported assertion. For this reason, and because there was "no evidence of spoliation or alteration," the motion was denied.

JORDAN KHAN MUSIC CO., LLC v. TAGLIOLI

In **Jordan Khan Music Co., LLC v. Taglioli**, 2022 WL 1511319 (E.D. Tex. May 12, 2022), the plaintiffs brought suit against the defendants alleging violations of the Lanham Act, common law trademark infringement, common law unfair competition, unjust enrichment, tortious interference, civil RICO, and fraud. The plaintiffs alleged that "Defendants have and will continue to willfully use and distribute unlicensed, pirated versions of copyrighted software to create, use, and sell audio backing tracks." The defendants counterclaimed, "asserting breach of non-competition contract, tortious interference with business relations, conversion, and license termination." United States District Judge Amos Mazzant was asked to rule on the plaintiffs' motion to compel forensic examination of the defendants' devices. The plaintiffs sought evidence of the defendants' unlicensed use of the plaintiffs' software. The plaintiffs claimed this was crucial to their RICO claims. The defendants responded that the discovery request was far too invasive and would provide information beyond the scope of any claims in the case. Judge Mazzant stated that although the plaintiffs "may very well find such

evidence through examinations,” the request was “massively disproportionate to the issues.” The plaintiffs will have access to information “far beyond the scope of the audio software,” including the employees’ personal hospital health portal applications, banking applications, dating applications, and other personal sites. Judge Mazzant was persuaded that the plaintiffs could engage in the discovery process in a less invasive manner and denied the motion to compel.

JUUL LABS, INC. v. CHOU

In **Juul Labs, Inc. v. Chou**, 2022 WL 2161062 (C.D. Cal. Apr. 19, 2022), United States Magistrate Judge Patricia Donahue was asked to consider the plaintiff’s motion to compel inspection of the defendants’ electronic devices. The court previously issued an order requiring defendants to provide information about its prior WeChat Enterprise Software System and a sworn declaration identifying individuals who conducted searches. The order also required that the defendants describe how the searches were conducted. The defendants proceeded to cut and paste WeChat messages into Word documents, thereby omitting the original messages’ metadata. The plaintiff described this “as a particularly egregious example of insufficient production.” The defendants were required to produce Skype messages. The plaintiff argued that the defendants’ production of messages was in an inaccessible format and did not contain metadata. To remedy these issues, the plaintiffs asked the court to allow a forensic examination of 13 of the defendants’ devices. Magistrate Judge Donahue was not persuaded that this “extraordinary remedy” was warranted because the plaintiff failed to show that the defendants intentionally destroyed or concealed relevant ESI. Magistrate Judge Donahue added that the plaintiff failed to argue the specific relevance of each individual device it sought to forensically examine. There was also a high

disruption to the defendants’ business which could not be remedied by overnight shipping. Judge Donahue denied the motion to compel.

TK ELEVATOR CORP. v. ABELS & SCHUMACHER ELEVATOR CO.

In **TK Elevator Corp. v Abels and Schumacher Elevator Co.**, 2022 WL 17551765 (D. Neb. Dec. 9, 2022), United States Magistrate Cheryl R. Zwart granted the plaintiff’s motion to compel a forensic examination of the defendants’ devices, but limited the scope to a “connectivity analysis,” as opposed to allowing full forensic imaging. The plaintiff sued its former employee and the former employee’s new company for, among other things, breach of employment agreement and misappropriation of trade secrets. In its original Request for Production, the plaintiff included a request for forensic exam of the defendants’ devices. The defendants objected, asserting that the request was unreasonably intrusive, overly broad and burdensome, disproportionate to the needs of the case, sought documents and information irrelevant to the claims and defenses asserted in the case, and was cumulative as responsive documents and information had been or would be produced. This motion to compel followed.

The plaintiff’s main argument in favor of the inspection was that while the former employee defendant was still employed by the plaintiff, he may have used a USB drive to access and store confidential information that belonged to the plaintiff, and later used that same USB drive to transfer the information to the defendant company’s devices and/or systems, for use while employed by the defendant company. To support this allegation, the plaintiff relied, in significant part, on the results a forensic exam of the computer that it had issued to the former employee defendant. That exam revealed that a USB drive had been inserted into the subject computer months before the former

employee defendant resigned, and that the device contained at least one of the highly sensitive documents that is the same as, or similar to, one of the trade secret documents at issue. The plaintiff, therefore, argued that “[w]hat exists on the devices and systems, when and what documents were reviewed, saved, modified, or downloaded, and what may have once existed but has since been deleted, is critical to the claims and defenses at issue in this case.” The exam results notwithstanding, the former employee defendant claimed that he never had or used a USB drive, and the defendant company asserted that it had already conducted a thorough search of its relevant devices and had produced responsive documents.

Judge Zwart recognized that forensic inspections of an opposing party’s devices or systems can be highly intrusive and that, therefore, granting such an exam pursuant to Rule 34 is the exception, and not the rule, for discovery of ESI. Even so, Judge Zwart ultimately determined that consideration of the relevant factors weighed in favor of allowing the inspection. Specifically, Judge Zwart concluded that (i) there were inconsistencies in the facts presented regarding, among other things, the former employee defendant’s use of a USB Drive; and (ii) the devices at issue, and the possible discovery – via forensic examination – of electronic data about their use, would likely yield information that would either prove or disprove the parties’ respective positions as to the former employee defendant’s alleged use of the plaintiff’s information. Importantly, however, despite allowing the inspection to proceed, Judge Zwart determined that a full forensic exam, which would include full imaging of the subject devices, was too intrusive, and instead limited the scope of the inspection to a USB connectivity analysis. This type of analysis would use the serial number of the of the USB drive at issue to determine whether it had been used to transfer plaintiff’s confidential data to the defendants’ devices. Judge Zwart held that the connectivity analysis was a more narrowly tailored,

less intrusive approach that would still provide the information regarding the use of the USB drive that the plaintiff sought. Judge Zwart ordered that the analysis be conducted promptly, and that the parties should promptly notify the court if the analysis indicated that further inspection of devices was warranted.

STEVENS v. SULLUM

In **Stevens v. Sullum**, 2022 WL 4122195 (M.D. Pa. Sept. 9, 2022), Chief Magistrate Judge Karoline Mehalchick granted the defendant’s motion for a protective order regarding a deposition question and granted the plaintiff’s request for an independent forensic analysis regarding missing ESI. The underlying case was a civil rights complaint under 42 U.S.C. § 1983. This specific ruling involved a discovery dispute where the plaintiff claimed that the defendants’ witness failed to answer a deposition question and sought to compel a second deposition of the witness. The plaintiff also sought an adverse inference, arguing that they were prejudiced by the witness not answering the question and the witness will now have time to prepare an answer with counsel. The defendants, in turn, sought a protective order precluding that deposition question, arguing their witness repeatedly answered the question. This case also addressed the plaintiff’s separate request for an independent forensic examination of the defendants’ server.

Magistrate Judge Mehalchick first denied the plaintiff’s requests to depose the defendant’s witness a second time and for an adverse inference. The plaintiff claimed that the witness did not answer “which of [the plaintiff’s] allegations set forth in the affidavit of probable cause were inaccurate and incredible.” The defendants claimed that their witness “was instructed not to answer one (1) question because Plaintiff’s counsel repeatedly asked Attorney Riccardo the same question over and over after it had been answered as to harass the deponent.” The Court noted that under Rule

30(d)(3), “a party may move to terminate or limit [a deposition] on the ground that it is being conducted in bad faith or in a manner that unreasonably annoys, embarrasses, or oppresses the deponent or party.” The Court excerpted numerous instances from the deposition transcript where the plaintiff asked this question to the witness and concluded that “Defendant counsel properly instructed witness not to answer question under Fed. R. Civ. P. 30(d)(3) as the Court found that the question was asked and answered repeatedly.” The Court also found that “the discovery sought by Stevens, at the end of the day, appears to be cumulative and/or duplicative.”

Magistrate Judge Mehalchick next granted the defendant’s motion for a protective order “as to the narrow issue of precluding the re-deposition of Attorney Riccardo regarding the question: ‘tell me which of the underlying allegations are not accurate?’” The Court noted that under FRCP 26(c), a “court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.” Referencing its prior findings, the Court concluded that “Defendants appear to have acted in good faith in instructing Attorney Riccardo not to answer upon the belief that Stevens’ questions has been ‘asked and answered’ or in a manner that annoyed the dependent,” that “counsel properly instructed Attorney Riccardo not to answer the questions presented by Attorney Guzzardo,” and that “the discovery sought by Stevens, at the end of the day, appears to be cumulative and/or duplicative.”

Finally, Magistrate Judge Mehalchick granted “Stevens’ request to obtain an independent forensic computer expert to conduct a search of Defendants’ server to search and produce emails from all accounts used in connection with Stevens’ case.” Magistrate Judge Mehalchick stated that “[a] forensic investigation of a litigant’s computer is a n-

routine intrusion that may be ordered as a sanction after a litigant has failed to preserve evidence, equivocally responded to discovery or otherwise resisted discovery” Magistrate Judge Mehalchick noted that “Courts have ordered forensic investigations to be performed to determine whether electronically stored information was deleted or withheld.” Here, she granted plaintiff’s request for the forensic analysis, noting that “additional emails were acquired pertaining to Stevens’ prior electronic discovery requests only after [a third party’s] emails were subpoenaed.” The Court nonetheless determined that “Stevens must limit the temporal and term scope of the independent expert’s search to maintain privacy and confidentiality” and that the plaintiff “is responsible for payment of the fees and costs charged by the independent computer forensics expert.”

Rule 34

Rule 34 governs the requests for and production of documents and tangible things. Rule 34(b)(2)(E) requires that documents be produced as they are kept in the ordinary course, or that the producing party organize the documents to identify the requests to which each is responsive. As a general matter, courts have held that documents produced with Tiff+ productions satisfy Rule 34(b)(2)(E). Sixteen years after the production format rule was adopted, production format battles continue, as is evidenced by **D.M. v. County of Merced** and **Metro Service Group, Inc. v. Waste Connections Bayou, Inc.**, described below. Likewise, Rule 34(b)(2)(B) & (C) permit a party who has received a request for production to object to that request, but require the objection to set out “with specificity” the grounds and reasons for the objection, and to state “whether any responsive materials are being withheld on the basis of the objection.” These requirements are intended to bring an end to the practice of interposing “boilerplate” or “general” objections to discovery requests, so that the parties can focus their energy and attention on the genuine crux of a dispute. **Weatherspoon v. 739 Iberville, LLC**, demonstrates both that some practitioners continue to interpose disfavored general objections, and also the perils they risk encountering by doing so.

D.M. v. COUNTY OF MERCED

In **D.M. v. County of Merced**, 2022 WL 705621 (E.D. Cal. Mar. 9, 2022), Magistrate Judge Stanley A. Boone granted the plaintiffs’ motion to compel production, and imposed sanctions in the form of attorneys’ fees. The case dealt with a death by suicide in the Merced County Jail. The plaintiffs alleged the defendants knew or recklessly disregarded the fact that the decedent was at a significantly increased risk of suicide and failed to adequately monitor or screen her. There were difficulties in procuring discovery, and the court

granted the plaintiffs’ first motion in July 2021, ordering the defendants to provide further responses and responsive documents to the plaintiffs’ Requests for Production (“RFPs”) numbers 20 and 21. Following seven months of efforts to get the defendants to comply with production, the plaintiffs filed this instant motion to compel in February 2022. They asked for either compulsion with monetary sanctions, or evidentiary sanctions in the form of adverse inference instructions.

Magistrate Judge Boone granted the motion to compel and motion for sanctions in the form of attorneys’ fees, but denied their motion for adverse inference instructions. He focused particularly on Federal Rule of Civil Procedure 34’s requirement that a responding party produce documents “as they are kept in the usual course of business, or organize and label them to correspond to the categories in the request” or “in a reasonably usable form” if the request is not specific. Here, however, the documents the defendants produced through ESI searches were separated into four productions, each bearing a different person’s name. The plaintiffs did not know who the individuals were or why their emails were selected for search and production, and they believed the scope of the production was unclear since it contained many non-email documents, there was no sufficient load file or apparent organization, and there were clearly missing documents. The court granted the plaintiffs’ motion to compel the defendants to redo the production to resolve these problems, as well as attorneys’ fees for all the time and money the plaintiffs had spent attempting to procure the production. It denied the motion for an adverse inference instruction because “there [did] not appear to be indications of intentionally withholding or destroying relevant evidence,” but Magistrate Judge Boone noted this may change based on what the defendants ultimately produced.

METRO SERVICE GROUP, INC. v. WASTE CONNECTIONS BAYOU, INC.

In **Metro Service Group, Inc. v. Waste Connections Bayou, Inc.**, 2022 WL 2255203 (E.D. La. May 31, 2022), United States Magistrate Judge Dana M. Douglas found that the defendant waived privilege by failing to produce a privilege log. The underlying case was a breach of contract claim brought by a subcontractor against a general contractor alleging “defective and delayed performance, nonperformance, and failure to pay.” The plaintiff brought a motion to compel, arguing that that defendants made email productions “much more difficult and burdensome for Metro to use efficiently in the litigation” by converting the original files into PDF files. The plaintiff also asked the Court to compel defendants to produce 534 pages of placeholder files “in their native digital format,” sought the production of files withheld under claim of privilege, and sought costs related to their motion to compel. The Court granted the plaintiff’s claim regarding privilege and denied all other claims.

Magistrate Judge Douglas first rejected the plaintiff’s request that defendants reproduce emails in their original form, finding that the PDF production by defendants was a “reasonably usable form.” Magistrate Judge Douglas noted that the defendant was required under Rule 34(b)(2)(D) “to inform Plaintiff of the form it intended to use where none was stipulated” and that the defendant violated this rule by not informing the plaintiff that it will produce the documents as PDFs. Magistrate Judge Douglas nonetheless stated that under Rule 26(b)(2)(B), “[i]f the producing party shows that an undue burden or cost would be required to produce the information as requested, the requesting party must show ‘good cause’ for the production of the requested information in an alternative format.” Here, Magistrate Judge Douglas found good cause, noting that “Defendant has made a strong showing that producing the

documents in the manner now requested would have created the undue burden of waiving certain privileges, and that the shift to PDF documents was intended to make it possible to review and redact privileged information from the 14,000 emails and twenty-four gigabytes of data without inadvertently waiving those privileges.” Magistrate Judge Douglas also found that “the PDF documents, while certainly not ideal, did constitute a reasonably usable format,” noting that they were still searchable to an extent and that the plaintiff utilized them to build a chronology. “Thus, the Court finds the PDF production is reasonably usable, and will not order the documents be reproduced in another form.”

Magistrate Judge Douglas then rejected the plaintiff’s request to compel defendants to produce placeholders “in their native format.” The plaintiff sought production of native files because the “native format allows Plaintiff to digitally search the documents and contains metadata that will reflect when the files were changed and by whom.” In denying the request, Magistrate Judge Douglas noted that “Plaintiff failed to originally request production in native format, and Defendant has shown that production in native format would be unduly burdensome.” Regarding the plaintiff’s timing, the Court stated that “[o]rdinarily, courts will not compel the production of metadata when a party did not make that a part of its request.” Regarding the burden on the defendant, the Court noted that “to review 103,000 pages for privilege—particularly at this juncture—without a clear showing by Plaintiff that the production is relevant and proportional to the needs of the case is unwarranted at this late stage in the proceeding.” The Court stated that “[h]ad Plaintiff raised this issue prior to production, when it received the production in October 2021, or when counsel personally determined the files were not included in January, there would have been ample time to do so.” The Court also noted that “Plaintiff did not specify a form until four months after Defendant

responded to the requests” and that “Plaintiff filed its motion to compel roughly two weeks before the discovery deadline and set it for submission after that date had passed.” Finally, the Court also noted that “Defendant states that it will produce the native format of any emails Plaintiff specifically asks for, and notes that Plaintiff is capable of identifying those emails because the emails themselves are included in PDF format, just the attachments are omitted.”

Finally, Magistrate Judge Douglas compelled defendants to produce a series of documents it had redacted under claim of privilege but for which it failed to provide a privilege log. The defendant claimed that “in lieu of a privilege log, it provided all emails, utilizing PDF format to redact the substantive information within the emails, but leaving the header including who sent the email to whom, when, and about what.” Magistrate Judge Douglas noted that Fed. R. Civ. P. 26(b)(5) requires a party withholding information under a claim of privilege “must” keep a privilege log meeting specific requirements. Magistrate Douglas concluded that “[t]he use of the word ‘must’ indicates that production of a privilege log, including the detail specified by Rule 26(b)(5)(A)(i) and (ii), is mandatory. The rules do not allow for an “in lieu” production of a privilege log. Indeed, the “privilege log’s description of each document and its contents must provide sufficient information to permit courts and other parties to ‘test[] the merits of’ the privilege claim.” Because the defendant failed to provide a privilege log, the Court concluded that “to the extent the [defendant] sought to assert vague and blanket privileges, the objections are waived because of its failure to comply with the Federal Rule 26. Thus, unredacted copies of MSG-WCB002401, the series of communications between Clay Richardson of Waste Connections and Katherine Constanza of Jefferson Parish must be produced.”

WEATHERSPOON v. 739 IBERVILLE, LLC

In **Weatherspoon v. 739 Iberville, LLC**, 2022 WL 824618 (E.D. La. Mar. 18, 2022), Magistrate Judge Karen Wells Roby was asked to compel the defendant to provide full and adequate responses to requests for production. Magistrate Judge Roby granted the request in part, finding that pursuant to Federal Rule of Civil Procedure 34(a), the defendant’s boilerplate and vague objections were insufficient. She noted that “[b]oilerplate and general objections . . . ‘are taglines, completely devoid of any individualized factual analysis.’” These objections “fall ‘woefully short of the burden that must be borne by a party making an objection to an interrogatory or document request.’” Judge Roby explained that the rule requires specificity to allow the parties to discuss any alleged defects in a discovery request or response, in the hopes of fixing those defects. Thus, she observed, boilerplate objections make it impossible to meet and confer and avoid the need to file a motion to compel. Magistrate Judge Roby struck many of the defendant’s objections and ordered the defendant to produce documents relating to these requests for production.

ESI Protocols

Parties often enter ESI Protocols to provide a degree of certainty in terms of custodians, search terms, production format, and other matters that can give rise to disputes. However, despite their best efforts, the parties cannot always anticipate all the turns a particular case may take or every dispute that might arise. When disputes about discovery do arise, courts are often asked to interpret the parties' actions and positions through the lens of the ESI protocol they agreed to (and, in many cases, the Court gave binding effect by entering it as an agreed order). The following cases illustrate how some jurists have approached such disputes and raise a question as to whether we have reached a point whether ESI protocols have outlived their useful life.

IN RE ACTOS ANTITRUST LITIGATION

In *In re Actos Antitrust Litigation*, 112 Fed. R. Serv. 3d 793 (S.D.N.Y. 2022), United States Magistrate Judge Stewart Aaron ruled on the plaintiff's motion to compel the defendants to produce all nonprivileged, responsive emails and provide privilege log entries for emails that are part of redacted email threads or have been withheld for privilege. The case is a long-running antitrust class action alleging the defendants conspired to prevent competitors from marketing a generic drug. Early on, the parties agreed to an ESI discovery protocol that permitted deduplication of ESI but that did not explicitly permit email threading. In making its production, the defendant against whom the motion was directed used a process email threading, "by which a party reviews and produces the most-inclusive email in a thread." The plaintiffs objected to the defendant's use of email threading and sought to compel the defendant to produce "earlier-in-time emails and any metadata associated with those emails."

Magistrate Judge Aaron observed that ESI protocols are a tool commonly used "to avoid downstream misunderstandings or disputes" (quoting *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 Sedona Conf. J. 1, Comment 3.c. (2018)). He also noted that it is not uncommon for ESI protocols to address the use of email threading in document production. Nevertheless, here the parties' agreed protocol did not address threading, leading Magistrate Judge Aaron to consider the question of whether a producing party's unilateral decision to implement email threading in a production deprives the requesting party of important information.

Here, Magistrate Judge Aaron found that the defendant's use of email threading resulted "in the exclusion of the metadata associated with earlier emails in a chain," which "materially reduced Plaintiffs' ability to search for all correspondence within a date range." For example, the defendant's email threaded production "removed plaintiffs' ability to see if anyone was blind-copied on lesser included emails, even though this information was among the metadata the parties agreed in the discovery protocol to produce." Magistrate Judge Aaron therefore ruled that the defendant must produce all responsive ESI to the plaintiffs, including earlier-in-time emails suppressed from production previously. Magistrate Judge Aaron also required parties to meet and confer about privilege log protocol after first observing that the use of categorical privilege logs would be appropriate.

EDITOR'S NOTE

This decision highlights a disturbing trend of requesting parties objecting to the use of threaded productions on the argument that an inclusive e-mail will deprive them of case-dispositive information. We would note that threaded productions promote tremendous cost-savings and efficiencies consistent with Rule 1. In addition, parties can

reach agreements regarding the use of threaded productions while preserving the lesser e-mails for production upon a showing of good cause by the requesting parties; this bargain does not have to be all or nothing.

DR DISTRIBUTORS, LLC v. 21 CENTURY SMOKING, INC.

In **DR Distributors, LLC v. 21 Century Smoking, Inc.**, 2022 WL 2905838 (N.D. Ill. July 22, 2022), United States Magistrate Judge Iain D. Johnston found that the defendants waived the spousal communications privilege and could not claw back documents. The defendants argued that they “acted reasonably in focusing on complying with the Court’s order, while relying on the Court’s statement that it would apply FRE 502(d) to [the] ‘fullest extent possible’ and Rule 26(b)(5)(B) ‘liberally.’” Judge Johnston stated that “[t]he chutzpah of Defendants’ argument is almost too much to take” and that “the Court refuses to accept any blame for Defendants’ failures,” especially given the length of the case (10 years), and “Defendant’s monumental ESI production blunders.” Judge Johnston stated that “besides the boldness of the Defendants’ position, there are at least three significant problems with Defendants’ premise that the framework of Rule 502 applies and excuses their failures. The first is textual. The second is causal. The third is analytical.” The textual problem is that “the plain language of Rule 502 makes clear” that “the rule only applies to the attorney-client privilege and the work-product doctrine.” Judge Johnston refused “to graft Rule 502 onto another common-law privilege, such as the marital communications privilege,” arguing that “[i]f the drafters of Rule 502 wanted the rule to apply to other privileges, they could have stated so. Instead, they specifically chose to state that the rule does not apply to other privileges.” The second problem Judge Johnston noted is that “some of the documents Defendants seek to claw back” were produced before the Court’s February 2, 2021 order. The third problem is that “a simple cost-

benefit analysis counsels against blindly relying on a Rule 502(d) order to justify the failure to implement a reasonable document review process.”

Having ruled that Rule 502 does not apply to the spousal communications privilege, Judge Johnston analyzed the case using “the balancing test used in the Seventh Circuit before the promulgation of Rule 502.” Judge Johnston stated the three-step test as follows: “First, as a threshold matter, the court must determine if the document is privileged. If the document is not privileged, the inquiry ends. If the document is privileged, the court must determine if the disclosure was inadvertent. Lastly, even if the document is found to be privileged and inadvertently produced, the court must still determine whether the privilege was waived... In the third part of the test, the court balances five factors: (1) the reasonableness of precautions taken to prevent disclosure; (2) the time to rectify the error; (3) the scope of discovery; (4) the extent of the disclosure; and (5) the overriding issue of fairness.” Judge Johnston found that all five of these factors weighed in favor of finding that defendants waived the spousal communications privilege.

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION v. SCOTTSDALE HEALTHCARE HOSPITALS

In **Equal Employment Opportunity Commission v. Scottsdale Healthcare Hospitals**, 2021 WL 4522284 (D. Ariz. Oct. 4, 2021), the parties submitted conflicting proposals for the ESI discovery protocol. The plaintiff asked the court to enter a 14-page ESI protocol that contains three exhibits outlining “the presumptive scope of ESI to be searched” and 26 metadata fields required to be included with the ESI production. The defendant asked the court to adopt “a more straightforward ESI approach and attached the model order from the Northern District of California to their motion. Plaintiff argued that a

more detailed ESI protocol is required to prevent future discovery disputes. The defendant argued that the “detailed protocol” proposed by plaintiff would create additional discovery disputes. United States District Judge Michael Liburdi decided to adopt defendant’s proposed protocol from the Northern District of California. Judge Liburdi also adopted any portion of the plaintiff’s proposal that the parties agreed on. If there was a conflict between the Northern District of California Model order and agreed upon provisions, the agreed-upon provisions were adopted in their place.


IN RE GOOGLE RTB CONSUMER PRIVACY LITIGATION

In **In re Google RTB Consumer Privacy Litigation**, No. 4:21-cv-02155-YGR (N.D. Cal. Aug. 10, 2022), Magistrate Judge Virginia K. Demarchi entered Google’s proposed Rule 502(b) order. The parties initially agreed on all terms of a proposed order except a single issue, which Magistrate Demarchi resolved largely on Google’s behalf. At the time, Magistrate Demarchi entered an order regarding the issue she resolved and asked the parties to agree to the rest of the order. Google here asked the Court to enter the order previously agreed upon but which the plaintiffs no longer agree to. The plaintiffs argued that “it is procedurally improper for Google to move for entry of a Rule 502(d) order at this time” and that “such an order is unnecessary because ‘the parties already have the legal tools and resources they need to resolve disputes over privilege waivers as they may arise in this case.’” Magistrate Demarchi found that Google’s motion was procedurally proper, as Rule 502(d) enables a court to enter an order “whether on motion of one or more parties or on its own motion” and the previous order merely stated the rule of law that “in the absence of a [Rule] 502(d) order, the other provisions of Rule 502 apply.” Magistrate Demarchi also found that a 502(d) order was warranted, noting that “this case has featured many disputes that are not easily addressed, as well as a lack of cooperation.” Finally, Magistrate

Demarchi agreed with Google “that it would suffer prejudice if, having conducted a substantial portion of its document review based on that prior understanding, it must now defend against challenges to any clawed back documents by demonstrating compliance with Rule 502(b).”

IN RE KEURIG ANTITRUST LITIGATION

In **In re Keurig Antitrust Litigation**, 2022 WL 1082087 (S.D.N.Y. Apr. 11, 2022), United States Magistrate Judge Sarah Cave addressed the parties’ cross-motions for spoliation sanctions. The defendant manufactures coffeemakers that use disposable, plastic cups containing ground coffee, as well as plastic cups used in the coffeemakers. The plaintiffs manufacture plastic cups for use in the defendant’s coffeemakers as competitors with the defendant. The plaintiffs accused the defendant of multiple anti-competitive acts, including re-designing its coffee machines to prevent the use of competitors’ cups and threatening companies that do business with competitors. Early in the litigation, the parties agreed on a stipulated ESI order that incorporated general language that they would “take reasonable steps in good faith to prevent the loss, destruction, alteration, overwriting, deletion, shredding, incineration, or theft of any document or data the party knows, or reasonably should know, falls within the scope of Federal Rule of Civil Procedure 26(b)(1).” The parties agreed that these steps included issuing preservation notices, preventing automatic or manual deletions, and performing custodian interviews. During discovery, the defendant revealed that it had sent litigation preservation notices to 400 personnel within six days of receipt of the complaint, followed by an additional 300 people at a later time. However, it did not send hold notices to six of the 54 employees ultimately defined as key custodians in the litigation, and it did not perform timely custodian interviews of 11 of those 54 custodians.



Magistrate Judge Cave found the defendant failed to preserve certain ESI and hardcopy records. With respect to the hardcopy records, one of the key custodians the defendant did not interview for custodial purposes testified that he had maintained hard-copy notes of meetings and calls that were likely to contain relevant information, but that he had disposed of the notes upon leaving the company. Magistrate Judge Cave found that the failure to interview the custodian, as the defendant committed to do by entering the ESI order, led to the loss of the notes.

As for ESI, the defendant's legal hold policies required its IT staff to sequester the hard drive or computer of any departing employee subject to a litigation hold notice. Despite this, it failed to maintain an inventory of a departed employee's preserved hard drives, and it ultimately took no preservation steps concerning equipment issued to current personnel subject to the hold. Likewise, when discovery in the case ultimately began, its IT staff had failed to preserve encryption keys for 16 hard drives defendant did preserve, rendering them inaccessible, and it entirely failed to preserve multiple other drives and computers.

The court found that the defendant violated both Rule 37(e), by failing to take reasonable steps to preserve ESI, and Rule 37(b)(2), by failing to follow the parties' stipulated, court-adopted ESI order. Performing a custodian-by-custodian analysis, the court ruled that the unavailability of three of the missing hard drives prejudiced the plaintiffs, as did the missing hardcopy notes. The court noted that preservation efforts, including interviews, extend to former personnel, and that the defendant's failure to interview certain custodians was negligent and possibly grossly negligent. Magistrate Judge Cave found insufficient evidence that the defendant intended to deprive the plaintiffs of the missing information, however, precluding severe sanctions under Rule 37(e)(2). As a curative measure, she

ordered that the plaintiffs could present evidence "regarding [defendant's] failure to preserve" the three missing hard drives and hardcopy notes to the jury.

Privilege and Waiver

Privilege review, production, and side litigation is one of the largest cost components of e-discovery. To that end, the Federal Rules Committee is taking another look at whether it is time to address this issue. These cases continue to highlight that organizations and individuals should explore entering into Rule 502(d) orders as a matter of course, when litigating in federal courts, and determine whether similar protections are provided by state courts. In addition, the use of categorical privilege logs should be used to reduce the overall burden associated with preparing privilege logs. With this said, parties and courts are still struggling with how best to use such logs and when additional information is needed.

REKOR SYSTEMS, INC. v. LOUGHLIN

In **Rekor Systems, Inc. v. Loughlin**, 2021 WL 5450366 (S.D.N.Y. Nov. 22, 2021), United States District Judge Lewis J. Liman denied the defendants' motion for an order requiring the plaintiff to produce a privilege log that described the basis for the withholding or redacting any document on a document-by-document basis, as opposed to the categorical privilege log the plaintiff had already provided. Judge Liman cited Local Civil Rule 26.2(c) of the Local Civil Rules for U.S. District Courts for the Southern and Eastern Districts of New York, which states that "when asserting privilege on the same basis with respect to multiple documents, it is presumptively proper to provide the information required by this rule by group or category." The information required is set forth by subsection (a) of this rule, and includes: the type of document; its general subject matter; its date; its author; its addressees; any other recipients; and the relationship of the author, addressees, and recipients to each other, if not obvious. The Rule also states that a party receiving a categorical privilege log "may not object solely on that basis,

but may object if the substantive information required by this rule has not been provided in a comprehensible form."

Judge Liman reviewed the plaintiff's privilege log and found that the categories were clear and "appear[ed] plainly to be privileged." Additionally, he found that third parties were identified with sufficient detail, so that the defendants could make a privilege challenge. Hence, the defendants were not entitled to an order requiring the plaintiff to provide another privilege log.

SURE FIT HOME PRODUCTS, LLC v. MAYTEX MILLS INC.

In **Sure Fit Home Products, LLC v. Maytex Mills Inc.**, 2022 WL 1597000 (S.D.N.Y. May 20, 2022) United States Magistrate Judge Gabriel W. Gorenstein found that the plaintiffs waived privilege related to three documents. The plaintiffs first turned over "all three documents to its adversaries in a separate patent litigation." The defendants in the other case marked the documents as exhibits for trial, and the plaintiffs "asserted neither attorney-client privilege nor work product protection" despite "rais[ing] seven separate objections to the admission of the documents." In this case, the plaintiff again turned over the three documents to the defendants. When defendants requested the plaintiff to admit the authenticity of the three documents, the plaintiff only asserted privilege over one of the documents. The plaintiff did not assert privilege over the other documents for another two weeks.

Because there was a protective order in place, Magistrate Judge Gorenstein analyzed the waiver under the "completely reckless" standard, and not the FRE 502(b) standard. Magistrate Judge Gorenstein noted that this was "a high bar," stating that "[f]or a production to be 'completely reckless,'

the producing party must have shown no regard for preserving the confidentiality of the privileged documents.” Magistrate Judge Gorenstein found that “[t]he fact that plaintiffs have produced Exhibits 88, 89, and 90 to their adversaries in two separate matters — and did so in circumstances that later drew the specific attention of plaintiffs to the existence of these documents without their taking corrective action — reflects the highest degree of carelessness in handling purportedly privileged material.” This recklessness was “heightened by the fact that plaintiffs necessarily had to carefully review the documents more than three years ago when they were relied on in support of the summary judgment motion in *Kartri*, which put them on unmistakable notice that the documents had been disclosed to the other side.” Magistrate Judge Gorenstein concluded that “[t]his course of conduct, spanning several years, two disclosures, and multiple clear opportunities to claim the privilege, evidences ‘a total disregard for the confidentiality of any of the documents.’” Magistrate Judge Gorenstein thus held that the plaintiff waived privilege despite the protective order.

VASOLI v. YARDS BREWING CO.,

In *Vasoli v. Yards Brewing Co.*, 2021 WL 5045920 (E.D. Penn. Nov. 1, 2021), United States District Judge Wendy Beetlestone granted the plaintiff the sanction of a Rule 30(b)(6) deposition to inquire as to the defendant’s discovery methods. This was an employment discrimination and retaliation case, in which the defendant’s initial search for responsive documents was underinclusive. For example, the plaintiff’s supervisor testified he forwarded an email containing the plaintiff’s complaints to the chief executive officer of the company two days before the plaintiff was terminated. This forwarded email, which was integral to the plaintiff’s retaliation claim, was not produced by the defendant, even though three versions of the plaintiff’s email to her

supervisor were produced. The defendant produced the email after the supervisor’s deposition, and the court thereafter held a discovery dispute conference, in which they realized there were shortcomings in the search and considered sanctions. This led to this present question, which is whether the steps a party takes in producing documents to respond to a discovery request are protected from disclosure under either the attorney-client or work-product privilege.

Judge Beetlestone decided these steps are not protected by any privilege. She stated that a factual description of what the party did to meet discovery obligations does not necessarily require the disclosure of confidential client communications, and practical steps taken to identify responsive documents do not encroach on the thought processes of counsel. She further emphasized that “at each stage of the discovery process outlined in [Rule 26], counsel are expected to be transparent and communicate with one another,” and this is “even more true for electronic discovery.” Therefore, the defendant should have been more transparent about its discovery methodology.

Cross-Border Discovery

Few issues present as thorny questions in the practice of discovery as the impact of international laws governing cross-border data transfers on domestic U.S. litigation. For international litigants in U.S. courts, the prospect of producing documents in domestic discovery raises the specter of complicated, expensive, and potentially onerous steps to comply with the privacy and sovereign data laws of the sending jurisdiction. While in years past we have seen many courts wrestling with these questions in the context of the EU General Data Protection Regulation (GDPR) and similar European laws, this year we have noted an uptick in courts addressing issues presented by the growing body of Chinese data privacy and security laws.

CADENCE DESIGN SYSTEMS, INC. v. SYNTRONIC AB

In **Cadence Design Systems, Inc. v. Syntronic AB**, 2022 WL 2290593 (N.D. Cal. June 24, 2022), Chief Magistrate Judge Joseph Spero was asked to reconsider the court's prior order requiring the defendant to produce computers from China for inspection in the United States. Judge Spero denied the motion for reconsideration, finding that China's Personal Information Protection Law ("PIPL"), a data privacy law enacted in 2021, did not bar compliance with the court's previous order. The defendant argued that Article 39 of the PIPL prohibited transfer of the computers across international borders without the consent of current and former employees, who either declined or could not be located. PIPL provided an exception to the Article 39 rule in Article 13. Specifically, Article 13 allowed transmission of personal information when necessary to fulfill "statutory duties and responsibilities." Judge Spero concluded that the court's previous order created a

legal obligation under Article 13 and therefore, the defendant had to produce the computers for discovery purposes.

EDITOR'S NOTE

This case is significant in that it is one of the very first U.S. courts to deal with the PIPL in the context of a discovery dispute. In this instance, the court interpreted the PIPL and, specifically, separate consent for PIPL article 39 not to create an obstacle for U.S. discovery. While this holding is limited to the Northern District of California, it is significant nonetheless in that it provides a reference point for other courts dealing with a similar issue.

What is interesting here is that neither party raised PIPL articles 38 or 41. Article 38 requires the transferring party to comply with various requirements prior to the cross-border transfer, while article 41 requires consent from Chinese authorities prior to conducting a cross-border transfer of personal information to a "foreign judicial or enforcement authority," something the court noted in a footnote. Similar language exists in other Chinese laws, most notably PRC Data Security Law article 36. These clauses could also arguably complicate Chinese parties from complying with discovery obligations abroad and are deserving of closer scrutiny.

In fact, the Ministry of Justice (MOJ) of China in a recent FAQ has stated it would view this type of cross-border data transfer as a form of international judicial assistance, and advised Chinese parties to seek relevant approvals, conduct security assessments, and comply with requirements under Chinese laws such as the Civil Procedure Law and the Data Security Law as well as the PIPL. Further complicating the matter is the variety of authorities that would need to give approval in different circumstances. For example, while the MOJ is the authority for approval under The Hague Evidence Convention, the Cybersecurity Administration is charged with regulating and conducting security assessment of data and privacy matters.

While these positions regarding Chinese data security and privacy laws have not been tested significantly in U.S. courts, given this holding in Cadence, it is likely coming. Parties to litigation that involves discovery of data, documents, materials, or any information originating in China may run into similar issues. Companies and individuals

would be best advised to prepare a comprehensive cross-border discovery strategy ahead of time that can help advance discovery goals while minimizing risks and exposure to Chinese legal and compliance liabilities.

† Special thanks to Ya-Chiao Chang for this analysis.

KASHEF v. BNP PARIBAS S.A.

In **Kashef v. BNP Paribas S.A.**, 2022 WL 1617489 (S.D.N.Y. May 23, 2022), United States Magistrate Judge Jennifer E. Willis considered a motion seeking to compel the defendant to de-anonymize records previously produced to the Department of Justice subject to pseudonymization pursuant to compliance with the European Union General Data Protection Law (“GDPR”). The plaintiff brought claims alleging that the defendant had facilitated genocide in Sudan, and the plaintiff’s motion argued that the pseudonymized records could identify witnesses with information relevant to the claims and defenses in the case. Pseudonymization refers to a process by which names and other identifiers subject to GDPR restrictions are encoded in a consistent manner across a document population (e.g., “John Doe” is everywhere encoded as “Employee01”), and the producing party retains a key by which it is able to identify the person if required. The records in question had been produced to the DOJ in connection with a prior, related criminal investigation, but the DOJ had not sought to de-anonymize the records. In opposing the motion, the defendants argued that the French Bank Secrecy Law, the French blocking statute, and GDPR prevented the disclosure of de-anonymized identifying information in the records. After analyzing the issue using the factors set out by the Supreme Court in *Société Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987), Magistrate Judge Willis denied the motion. Magistrate Judge Willis agreed that the disclosure was prohibited by the laws cited by the defendant, including GDPR Article 49, which imposes a “necessity” element beyond the mere relevance and proportionality hurdles imposed by FRCP

26(b)(1)(B). Magistrate Judge Willis also found that the balance of the *Aerospatiale*’s comity factors weighed against compelling disclosure. In particular, Magistrate Judge Willis found that the fifth factor—balancing the competing interests of the United States against those of the foreign state—favored non-disclosure. Magistrate Judge Willis reasoned that the significant U.S. interest in pursuing justice for victims of genocide was comparatively lower than the relevant interest of “France and the European Union[, which] have demonstrated a strong interest in data privacy, and concurrently have an interest in having their laws apply to banks operating within their borders,” particularly where, as here, the domestic “interest is limited by whether the pseudonymized information is ‘actually material to Plaintiffs’ efforts’ to pursue their remedy, and ‘whether that information can be obtained through alternative means.’”

EDITOR’S NOTE

This is one of the most well-reasoned applications of the *Aerospatiale* factors in the context of GDPR and the French blocking statute in recent memory, in that it does not minimize the substantial risks presented to the international party should it be forced to discard protections prescribed by those laws, and it cogently balances both the nature of the competing sovereign interests and whether the specific relief requested would advance those interests.

PHILIPS MEDICAL SYSTEMS (CLEVELAND), INC. v. BUAN

In **Philips Medical Systems (Cleveland), Inc. v. Buan**, 2022 WL 602485 (N.D. Ill. Mar. 1, 2022), Magistrate Judge Young B. Kim denied the defendants’ motion for reconsideration of the court’s previous order granting the plaintiffs’ Request for Production of Documents (“RPD”) and ruling on the impact of Chinese law on the discovery process. This was a trade secrets case, in which the plaintiffs alleged the defendants, their former employees, used trade secrets at their new company. The defendants had previously sought a protective order to reduce the plaintiffs’ document requests. They claimed that the process would be

burdensomely long due to the need for any documents they produce to be reviewed by Chinese state authorities to ensure they do not contain state secrets. The court denied this request and issued a schedule to work through their objections to the RPDs. For RPD Nos. 1-60, the defendants objected on the grounds that they either violated Chinese privacy law by asking for employees' mobile devices, or that they violated Chinese state secrets law by requiring the collection, copying, and/or storing of information that may include state secrets. The court overruled all these objections, emphasizing that the defendants would not be required to violate domestic Chinese law. The defendants then filed this motion for reconsideration.


Before analyzing the defendants' arguments, Magistrate Judge Kim explained that foreign laws that block discovery production do not automatically excuse Rule 26 obligations. The threshold question is whether the foreign law bars the production at issue, and if a court determines the answer is yes, it must then conduct an "international comity" review involving "a more particularized analysis of the respective interests of the foreign nation and the requesting nation." The most important factor to consider in this review is the fifth factor, which requires balancing the interests of the United States and the foreign state where the discoverable information is located.

In this motion, the defendants contended that three different Chinese statutes prevented them from complying with the plaintiffs' discovery requests: (1) the Guarding State Secrets Law ("GSSL"), (2) the Personal Information Protection Law ("PIPL"), and (3) the Data Security Law ("DSL"). Magistrate Judge Kim went through the statutes, and concluded the defendants failed to meet their burden of establishing that Chinese law actually barred the production. As for the GSSL, the defendants had not identified any responsive documents for which production may be impacted by Chinese law, and

failed to demonstrate that the identified Chinese laws would even apply to any of the responsive documents they possess. As for the PIPL, Magistrate Judge Kim said the defendants had not demonstrated that any personal information within the meaning of the statute was at issue. Lastly, as for the DSL, he decided that its review and approval requirements did not apply to the American civil discovery process, and would fail an international comity analysis even if they did. This is because the defendant's interpretation would give Chinese courts too broad a power to delay and/or prevent discovery in American courts, infringing on United States sovereignty and violating the fifth factor in the analysis. For these reasons, as well as the fact that the defendants should not have raised new arguments on a motion for reconsideration, their motion was denied.

U.S. MOVES TOWARD NEW E.U.-U.S. DATA PRIVACY FRAMEWORK

On October 7, 2022, President Joe Biden issued a long-awaited executive order mandating new legal safeguards over U.S. national security agencies' access to and use of the personal data of E.U. citizens, Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities. The Order is an important step toward ratifying the E.U.-U.S. Data Privacy Framework, which the United States and the E.U. negotiated in May 2022 to replace the former E.U.-U.S. Privacy Shield Framework, which was struck down by the European Court of Justice in 2020. The Executive Order requires that all agencies involved in signals intelligence collection may conduct such activities only in pursuit of twelve "legitimate objectives" (defined in the order) and only as necessary to support those objectives. The Order also proscribes four "prohibited objectives," in support of which "[s]ignals intelligence collection activities shall not be conducted": "(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the



press; (2) suppressing or restricting legitimate privacy interests; (3) suppressing or restricting a right to legal counsel; [and] (4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.” The Order also directs agencies to limit “bulk” surveillance and to limit the retention of personal data obtained through all intelligence collection. Finally, the Order establishes redress mechanisms by which individuals may challenge surveillance practices they believe are unlawful. Specifically, the Order provides that individuals may submit complaints to the Director of National Intelligence’s Civil Liberties Protection Officer (CLPO), who is empowered to investigate and remediate claims, and it directs the Attorney General of the United States to establish a “Data Protection Review Court,” consisting of judges who are not employees of the United States government, which will have jurisdiction to review decisions of the CLPO.

The E.U.-U.S. Data Privacy Framework next must be ratified by the European Commission, which may take up to six months. The Commission issued a first draft of its adequacy decision on the Framework in light of the U.S. Executive order on December 13, 2022. The draft decision concludes that the proposed Framework and U.S. commitments provide a comparable level of privacy safeguards for personal data to that available under E.U. law. The Commission has transmitted the draft decision to the full European Data Protection Board so that it may conduct its own evaluation. ■

About Winston & Strawn's eDiscovery, Managed Review, and Legal Services Practice

900+

ATTORNEYS

16

OFFICES WORLDWIDE

1853

FOUNDED

Winston & Strawn has built a full-service vendor and consulting practice providing services to our clients and case teams in the complex areas of e-discovery and information governance both within the United States and around the world. Our team includes highly experienced partners, eDiscovery attorneys, review attorneys, project managers, and technologists dispersed among our offices who evaluate a company's e-discovery requirements and capabilities to develop an e-discovery or compliance program that meets a company's needs.

eDISCOVERY SERVICES

Winston serves as national counsel for eDiscovery issues for multiple companies across a wide variety of industries, dramatically reducing costs and eliminating the need to educate multiple firms on IT infrastructure and retention policies.

Winston team members are experienced on most commercially available litigation support tools and platforms, with technical certifications including:

- EnCase® Certified Examiner (EnCE®)
- AccessData Certified Examiner (ACE)
- International Society of Forensic Computer Examiners (IAC)
- Certified Computer Examiner (CCE)
- Int'l Society of Forensic Computer Examiners (ISFCE)
- Relativity
- Nuix
- Brainspace

“Winston has one of the most impressive e-discovery practices in the world. They have top tier e-discovery consulting and document/data review as well as one of the best e-discovery advocacy practices.”

THE LEGAL 500

MANAGED REVIEW

Document review = significant cost and risk

The volume of information at issue requires better people, greater use of analytical tools, and close coordination with case team members.

Winston's Approach

Reduce data set subject to “eyes on review” through use of:

- Continuous Multimodal Learning (CMML)
- Predictive coding
- Targeted and portable learning
- Clustering/categorization
- Metadata dashboard
- Communications/conversations/thread analysis
- Concept search

LOWER COST MANAGED REVIEW CENTER

The Winston Legal Innovation Center offers lower cost managed review services by Winston review attorneys charged at rates competitive with domestic LPOs.

SERVICES	
ENGLISH LANGUAGE REVIEW	FOREIGN LANGUAGE REVIEW
SOURCE CODE REVIEW	TRANSLATION
CONTRACT REVIEW	DEAL DUE DILIGENCE

CONSULTING SERVICES

LITIGATION RESPONSE	CROSS-BORDER	LITIGATION RESPONSE	CROSS-BORDER
Design and implement litigation response programs to include gap analysis, guidelines, managing RFI/RFP, tool selection/implementation and education.	With experts in various jurisdictions and across Winston & Strawn's international offices, we have unparalleled experience in handling multinational litigation and working through international data protection and privacy and compliance issues regarding data transfers.	Single resource to develop and implement corporate e-discovery processes, develop preservation best practices, manage the Rule 26(f) process, and draft/argue complex motion practice, including defending sanctions and spoliation claims.	Develop, implement and manage centralized written discovery programs to ensure consistency and reduce costs across your litigation portfolio.
INFORMATION GOVERNANCE PROGRAMS	SOCIAL MEDIA / EPHEMERAL COMMUNICATIONS	CLOUD MIGRATION	INVESTIGATIONS
Ability to design and implement information governance programs to include policies, schedules, education and compliance.	Understanding whether and how to adopt newer forms of social media and how to adopt newer forms of social media and ephemeral communications in alignment with legal and IG obligations.	Transiting data to cloud-based solutions and providers to ensure data integrity and continuity.	Uniquely suited to assist clients and teams in internal investigations.
3RD PARTY SUBPOENA RESPONSE PROGRAM	DEFENSIBLE DELETION	DEAL DUE DILIGENCE	CONTRACT LIFECYCLE MANAGEMENT
Design, implement and process for response to 3rd party subpoenas	Managing the elimination of electronic information that is redundant or outdated in a manner consistent with legal and regulatory hold obligations.	Conduct deal due diligence e-discovery/ legal hold, data security and information governance risk.	AI-based contract discovery, classification and organization



Contact

JOHN ROSENTHAL

+1 (202) 282-5785

jrosenthal@winston.com

SCOTT COHEN

+1 (212) 294-3558

scohen@winston.com