Relativity®

# 2021 Data Discovery Legal Year in Review

By David Horrigan


Seventh Edition

# Foreword

Not unlike most aspects of life, when the COVID-19 pandemic swept the nation in 2020, we didn't know what it would mean to the world of data discovery. Would closed courts lead to reduced court filings and less e-discovery? Would the steady movement of increasing data privacy and data protection law be stopped as both legislatures and litigants moved on to other things?

**A COVID-Caseload Correlation?**

We've lost many things in the pandemic. Litigation is not one of them.

In fact, in the fiscal year ending September 30, 2020, the Administrative Office of the United States Courts reported civil case filings in federal district courts actually increased 58 percent. To be fair, we should note that most of the increase was from the earplug multidistrict litigation (MDL) matter in the Northern District of Florida. Civil filings increased from 297,877 in Fiscal Year 2019 to 470,581 in Fiscal Year 2020—but 202,814 of those filings were for the earplug cases. Likewise, in state courts, data compiled by Lex Machina from several major state trial courts across the country indicated a substantial drop in filings in April 2020, shortly after the pandemic began to spread in the United States, but filings rebounded quickly in the following months. Likewise, the big jump in federal filings was temporary. In September 2021, federal filings were down 40.5 percent—but they were still up 7.6 percent from where they were five years ago.

2020 was a big year for federal civil litigation, but not because of COVID, because of earplugs. In 2021, we have returned to our pre-earplug levels. By the way, if you would like to read about the earplug litigation, you can see our coverage in the ***2020 Data Discovery Legal Year in Review.***

## Topics in 2021

### *GDPR Fine of the Year*

We've introduced a new feature this year, the *GDPR Fine of the Year.* In this segment, we look at the most impactful fine of the year as European nations move to enforce the General Data Protection Regulation (GDPR). Our finalists this year are Amazon, courtesy of the data protection authority of Luxembourg, and Meta's WhatsApp, courtesy of the data protection authority of Ireland. Amazon had the bigger fine by far, but please see page 25 to see who carried the day, winning this dubious distinction.

### Spoliators in e-Discovery

Closer to home, we can't have a *Data Discovery Legal Year in Review* without looking at some of the world's noteworthy e-discovery law decisions, and you can't talk e-discovery without talking spoliation of evidence. It's what keeps many corporate counsel, litigators, and e-discovery technologists up at night. 2021 did not disappoint us in providing interesting e-discovery law in the area of spoliation and sanctions. We started the year with U.S. Magistrate Judge Iain Johnston's 256-page sanctions order in *DR Distributors v. 21st Century Smoking* (please see page 18), and we saw Utah adopt the sanctions law of another circuit in *Diversified Concepts v. Koford* (see page 21). In addition, we saw a cautionary tale about spoliation of attorney billing records in *Besman v. Stafford* (see page 17).

### Data Privacy and Data Protection

GDPR fines were not the only data privacy and data protection action in 2021. We saw U.S. courts deal with this critical issues as well. In *United States v. Rubin* (see page 20), we saw courts address the data privacy issues of automated license plate recognition (ALPR) technology. There were data privacy considerations as the court considered whether to order production of a litigant's Fitbit data in *Bartis v. Biomet* (please see page 19), and in data protection law, we saw the court grapple with the attorney-client privilege vis-à-vis data breach investigative reports in *In re Rutter's Data Sec. Breach Litig.* (please see page 12).

Of course, this is just a sample of what's in our Seventh Edition of the D*ata Discovery Legal Year in Review.* As always, we send it with the disclaimer that it is not intended to be a comprehensive guide to all litigation. Instead, we try to make it a quick, informative selection of trends.

A former secretary of state once said, "It takes a village." It's certainly true with this e-book. Thanks to our Relativity team of Kristy Esparza, Natalie Andrews, and Tammie Josifovic. Their talent, dedication, and good cheer help make this project possible.

**Happy holidays, and here's to an excellent 2022.**

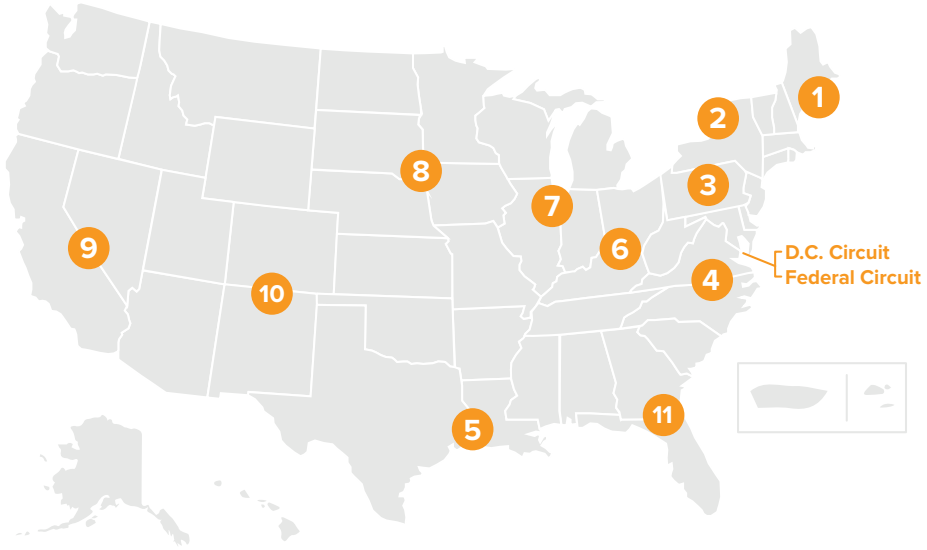

## David Horrigan

**Discovery Counsel and Legal Education Director, Relativity**

# Contents

*Denotes a U.S. Territory, Possession, or Federal District

# Jurisdictions of the U.S. Circuit Courts of Appeals




- **First Circuit:** Maine, Massachusetts, New Hampshire, Rhode Island, Puerto Rico*
- **Second Circuit:** Connecticut, New York, Vermont
- **Third Circuit:** Delaware, New Jersey, Pennsylvania, U.S. Virgin Islands*
- **Fourth Circuit:** Maryland, North Carolina, South Carolina, Virginia, West Virginia
- **Fifth Circuit:** Louisiana, Mississippi, Texas
- **Sixth Circuit:** Kentucky, Ohio, Michigan, Tennessee
- **Seventh Circuit:** Illinois, Indiana, Wisconsin
- **Eighth Circuit:** Arkansas, Iowa, Minnesota, Missouri, Nebraska, North Dakota, South Dakota
- **Ninth Circuit:** Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Washington State, Guam*, Northern Mariana Islands*
- **Tenth Circuit:** Colorado, Kansas, New Mexico, Oklahoma, Utah, Wyoming
- **Eleventh Circuit:** Alabama, Florida, Georgia
- **District of Columbia Circuit:** District of Columbia* and Appeals of Federal Administrative Decisions
- **Federal Circuit:** (Subject Matter Jurisdiction) Patents, International Trade, Federal Claims

# Analyses of Our Selected 2021 Cases

## U.S. Supreme Court

**DATA LAW: COMPUTER FRAUD AND ABUSE ACT OF 1986 (CFAA)**

# *Brandi the Cheerleader, Social Media Law, and the Limits of Free Speech on Campus*

***Van Buren v. United States,* No. 19-783 (U.S.)**



## The Facts

What could be more important than being a cheerleader for the Mahanoy Area Golden Bears?

When 14-year-old cheerleader Brandi Levy was rejected in her attempt to upgrade from the junior varsity to the varsity squad at Pennsylvania's Mahanoy Area High School, Levy did not go gently into that good night.

Instead, she did what many teenagers in the Digital Era do when things go wrong.

She took to Snapchat.

Crestfallen at the rejection, Levy authored a Snapchat missive her lawyers described as a "colorful expression of frustration."

Specifically, Levy included an image of herself extending her middle finger and wrote, "[Expletive] school [Expletive] softball [Expletive] cheer [Expletive] everything."

In this case, a fellow cheerleader—whose mother happened to be one of the cheerleading coaches—took a screenshot of Levy's post. Now, not only was Levy relegated to the JV squad instead of what she considered her rightful place on the Golden Bear varsity squad, she was suspended from the team entirely for a year.

Declining to leave the episode as a social media learning experience, Levy and her parents sued.

## The Law

Levy, by and through her parents, Lawrence and Betty Lou Levy, sued the Mahanoy Area School District, arguing the school's actions against Levy constituted government limitation of her free speech rights in violation of First Amendment to the U.S. Constitution.

There may have been death penalty cases or complex commercial litigation on the docket, but that didn't stop the U.S. District Court for the Middle District of Pennsylvania from swinging into action here, issuing a temporary restraining order restoring Levy to the cheerleading squad the day after the Levys filed their civil action.

Not only did the district court issue the restraining order, it granted summary judgment to the Levys, awarded them nominal damages, and ordered any record of the incident to be expunged from Brandi Levy's record.

Victory for Brandi the Cheerleader was short-lived.

The school district appealed to the U.S. Court of Appeals for the Third Circuit, but the appellate court also held for the Levys. However, on January 8, 2021, the U.S. Supreme Court granted certiorari, agreeing to hear the school district's case.

**For in-depth coverage, please see David Horrigan, *Brandi the Cheerleader, Social Media Law, and the Limits of Free-Speech on Campus,* *The Relativity Blog,* April 28, 2021.**

## Why Brandi the Cheerleader Matters

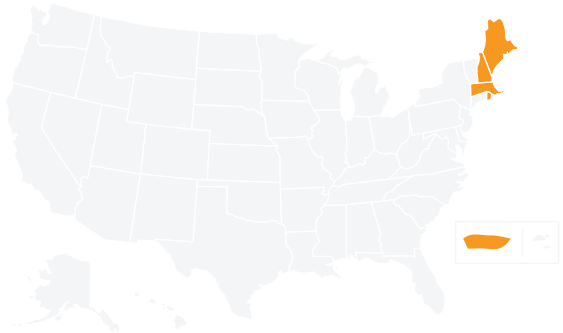
From "Bong Hits 4 Jesus" to black armbands during the Vietnam War, the jurisprudence of student speech has made it to the United States Supreme Court multiple times. However, as in so many areas of modern life, electronic data complicates things.

In the middle of the Vietnam War, three students wore black arm bands to school to protest United States involvement in the war. The school suspended the students, and the students sued, arguing the school's actions violated their First Amendment rights. In *Tinker v. Des Moines Ind. Sch. Dist.,* 393 U.S. 503 (1969), the Supreme Court held for the students.

The court held that, in wearing armbands, the students were not disruptive and did not impinge on the rights of others. Thus, the High Court held, the expression was protected under both the Free Exercise Clause of the First Amendment and the Due Process Clause of the 14th Amendment.

However, even the court in *Tinker* recognized student First Amendment rights were "subject to application in light of the special characteristics of the school environment." The pandemic, social media, and digital data have blurred the legal lines of what is on-campus and off-campus, and the case of Brandi the Cheerleader may help us figure it out.

## First Circuit: Maine, Massachusetts, New Hampshire, Rhode Island, Puerto Rico*



**E-DISCOVERY LAW: PROPORTIONALITY AND PRIVILEGE LOGS**

### *An e-Discovery Train Wreck: Judge Misstates the Law and Litigant Punts on Privilege Logs*

***Especias Montero, Inc. v. Best Seasonings Group, Inc.*, No. 20-1740 (D.P.R. Aug. 13, 2021).**

## The Facts

Founded in 1959 by Efraín Montero Acobes and based in Ponce, Puerto Rico, Especias Montero Inc. sells various seasonings, including Sazón Total, which is also part of the company's Premium Puerto Rican Seasoning Set. Meanwhile, Best Seasonings Group Inc., a company founded in 1990 and based in Juana Diaz, Puerto Rico, is also a spice company, doing business as Sofrio Montero.

Especias Montero sued Best Seasonings in 2020, alleging Best Seasonings infringed on Especias Montero's federally registered trademark for "Especias Montero Desde 1959" by, among other things, using the words, "Especias" and "Montero," with its products, creating a likelihood of confusion, and violating the federal Lanham Act. Best Seasonings filed a counterclaim against Especias Montero, claiming it used the marks in commerce before Especias Montero and seeking cancellation of the Especias Montero's trademark with the U.S. Patent and Trademark Office.

Best Seasonings moved the court to compel discovery from Especias Montero, including interrogatories, requests for production, and documents for which Especias Montero argued were protected by the attorney-client privilege.

## The Law

This discovery order got off to a bad start when U.S. Magistrate Judge Giselle Lopez-Soler misstated the law. Judge Lopez-Soler wrote, "Under Rule 26(b)(1) of the Federal Rules of Civil Procedure parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action." The judge, however, is citing the pre-December 1, 2015, version of Rule 26(b)(1) before the six-pronged proportionality test was added to the rule, most of it moved up from Fed. R. Civ. P. 26(b)(2)(C)(iii). She compounds her error by citing a 1978 U.S. Supreme Court decision, *Oppenheimer Fund, Inc. v. Sanders* for the proposition, "This provision has been interpreted to entitle parties to discovery of any matter that bears on any issue in the case in the absence of privilege."

Judge Lopez-Soler is citing bad law. The 2015 Federal Rules amendments negate *Oppenheimer* on this point. With this overly broad interpretation of Rule 26(b)(1), the judge went on to grant much of Best Seasonings' motion to compel.

The problems in the case stem also from Especias Montero attempting to claim attorney-client privilege without a privilege log. Especias Montero argued no privilege log was necessary because Especias Montero's witness, Mr. Montero, identified certain documents as protected by the attorney-client privilege during his deposition.

However, Judge Lopez-Soler rejected this argument. "Deposition testimony or an opposition to a motion to compel is not the proper mechanism to answer a request for documents or to assert privilege," she wrote. The judge cited the privilege log requirement of Fed. R. Civ. P. 26(b)(5)(A), noting, "When [a] party withholds information based on privilege the party is required to expressly make the claim and describe nature of the documents withheld with specificity so that the other party can assess the claim."

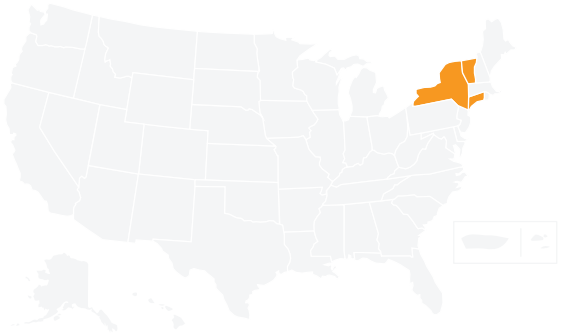
## Why *Especias Montero* Matters

We should not be too harsh on Judge Lopez-Soler. She is not the first judge to commit this error. Even in cases filed after December 1, 2015, litigants have attempted to use *Oppenheimer* to get very broad e-discovery, and judges have relied on the old version of the rule. Most judges are not experts in e-discovery. The problem with Judge Lopez-Soler's order is that it does not indicate whether she performed a proportionality analysis when granting Best Seasonings' discovery requests because she used an old version of the rule, cited outdated case law, and never mentioned proportionality in her order.

As for Especias Montero's attempt to get out of preparing a privilege log, nice try. Just about every e-discovery practitioner despises privilege logs. It's arguably just about the most painful part of e-discovery. However, Judge Lopez-Soler was absolutely correct here—you can't just mention your privilege claims in a deposition and get out of creating a privilege log. Rule 26(b)(5)(A) is clear. If you withhold documents based on attorney-client privilege, you must make the claim expressly, and you must do so in a manner that will enable other parties to assess the claim. A throwaway line in a deposition is not going to cut it.

e-Discovery is not easy. e-Discovery legal teams include lawyers, paralegals, and technologists with specialized knowledge of the law and technology of e-discovery. Our courts are overburdened with massive caseloads, and lawyers, too, face daunting case load challenges. Most do not have time to become e-discovery experts. Moral of the story? Consulting e-discovery legal teams with specialized knowledge is rarely a bad idea.

## Second Circuit: Connecticut, New York, Vermont



**E-DISCOVERY EVIDENCE**

### *When It Comes to e-Discovery, Hyperlinks Are Not Attachments*

***Nichols v. Noom, Inc.*, No. 20-CV-3677 (S.D.N.Y. Mar. 11, 2011).**

## The Facts

With over 50 million downloads of its weight-loss app, Noom is one of the fastest-growing weight-loss programs in the world and has almost quadrupled its annual revenue to over $237 million and counting. Part of Noom Inc.'s marketing strategy is to have a "low cost" or "zero cost" trial period followed by an automatically renewing regular subscription.

Alleging that Noom deceptively and fraudulently failed to advise consumers that they would be billed automatically for substantial fees and that Noom made it almost impossible to cancel once it had a consumer's credit card information, Mojo Nichols and others sued Noom in a class action, alleging violations of California and New York consumer protection laws, including the California Automatic Renewal Act.

During discovery, Mr. Nichols and his fellow class action plaintiffs said they discovered that—instead of using email attachments—most Noom employees used hyperlinks to other documents. Thus, Mr. Nichols argued, Noom should be required to produce the documents to which the hyperlinks linked. Noom objected, arguing producing all the hyperlinked documents would not be proportional and would produce non-responsive data.

## The Law

U.S. Magistrate Judge Katherine Parker rejected Mr. Nichols argument, writing, "To start, the Court does not agree that a hyperlinked document is an attachment. While the Court appreciates that hyperlinked internal documents could be akin to attachments, this is not necessarily so."

Judge Parker gave several examples where hyperlinks would not be the same as attachments, including legal memoranda where links are to cases, hyperlinks to SharePoint folders—where the entire SharePoint file would not be the same as an attachment—a hyperlink to a telephone number, and other examples.

Although the court ruled in favor of Noom, it refused to grant Noom attorney fees because—although the judge rejected Mr. Nichols' argument—she believed the argument was a reasonable one on an important issue. "The issue Plaintiffs raise is an important one and one on which the Court did not issue a fulsome written decision, instead opting to address the issue more informally as is the practice in this District," Judge Parker wrote.

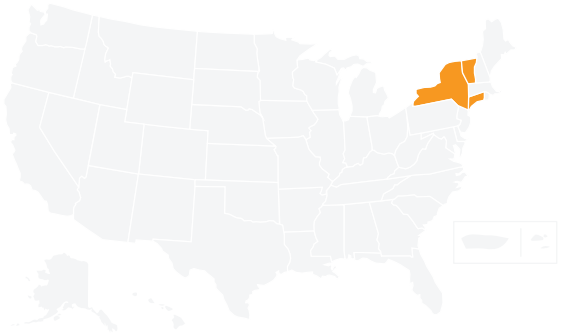
## Why *Nichols* Matters

*Nichols* is an important case for the simple reason that more people are using hyperlinks. Mr. Nichols and his fellow plaintiffs may have been surprised when they discovered just how prevalent Noom employees use of hyperlinks was, but it's not just Noom. People everywhere are substituting links for attachments.

The COVID-19 pandemic accelerated the move to the cloud, and with so many more people using SaaS, the use of hyperlinks should only increase as cloud computing allows users to access documents on remote servers through hyperlinks.

Hyperlinks present special challenges in e-discovery. Email attachments are static, allowing litigants to capture what was transmitted at a particular point in time. However, one of the advantages of hyperlinked documents in the cloud is that they can be worked on collaboratively. However, this workflow advantage is an e-discovery disadvantage because the documents are dynamic—they probably will have changed multiple times since the creation of the email. The law of hyperlinks is just beginning.

## Second Circuit: Connecticut, New York, Vermont



**E-DISCOVERY LAW: PRIVILEGE LOGS AND LOCAL RULES**

### *Local Rules Carry the Day as Court Allows Litigant to Submit a Categorical Privilege Log*

***Rekor Sys. v. Loughlin,* No. 19-cv-7767 (S.D.N.Y. Nov. 22, 2021).**

## The Facts

Suzanne Loughlin and Harry Rhulen, a sister and brother, grew up in the same neighborhood and were childhood friends with Robert Berman. Ms. Loughlin and Mr. Rhulen would go on to become owners of the businesses, Firestorm Solutions LLC and Firestorm Franchising LLC. Mr. Berman grew up to become the CEO of Rekor Systems Inc., a corporation providing government contracting, aerospace, and logistics services. The friends closed a business deal where Rekor's predecessor company bought the Firestorm companies with Ms. Loughlin and Mr. Rhulen becoming officers at Rekor Systems. Things did not go well for the former childhood chums.

Rekor Systems sued Ms. Loughlin, Mr. Rhulen, and others, alleging they committed fraud by misrepresenting the financial condition of the Firestorm companies. In addition, Rekor Systems argued Ms. Loughlin and Mr. Rhulen violated the federal Computer Fraud and Abuse Act (CFAA) by destroying emails upon resigning from their positions as officers at Rekor Systems. Ms. Loughlin and Mr. Rhulen denied the allegations.

During discovery, Rekor Systems attempted to submit a so-called categorical privilege log, one in which—instead of listing every document being withheld—a litigant groups withheld documents by category.

## The Law

U.S. District Judge Lewis Liman rejected the motion by Ms. Loughlin and Mr. Rhulen seeking an order requiring Rekor System to file a privilege log listing every withheld document. Interestingly enough, Judge Liman did not cite the Federal Rules of Civil Procedure in making his decision. Instead, the court relied on a local rule in the U.S. District Court for the Southern District of New York, Local Civil Rule 26.2(c).

Based loosely on Federal Rule of Civil Procedure 26(b)(5), Local Rule 26.2(a) sets forth the requirements for identifying the requirements for withholding documents based on the attorney-client privilege and the work product doctrine. Local Rule 26.2(c) modifies Local Rule 26.2(a) somewhat by providing, "Efficient means of providing information regarding claims of privilege are encouraged, and parties are encouraged to agree upon measures that further this end. For example, 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." Citing this local rule, Judge Liman allowed Rekor Systems to go with its categorical privilege log.

## Why *Loughlin* Matters

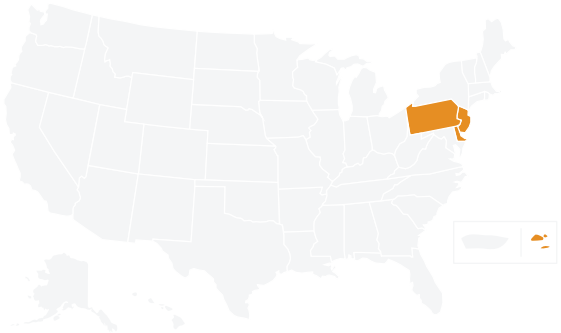
As we've said before on these pages, privilege logs are one of the most laborious and despised parts of e-discovery practice. We've never heard a litigant excited about the prospect of preparing one—but sometimes a local rule can help.

One of the biggest blunders legal teams make is failing to follow local rules, and in *Loughlin*, a local rule carried the day. Granted, the Southern District of New York's Local Rule 26.2(a) has similar provisions to Fed. R. Civ. P. 26(b)(5), but the local rule provides for more detailed requirements than the federal rule. More importantly, Rule 26(b)(5) does not have a categorical privilege log provision similar to Local Rule 26.2(c). Although Judge Liman never cited the Federal Rules, proportionality, or cooperation, *Loughlin* is also a proportionality and cooperation case.

The local rule encourages "efficient means of providing information," and the Committee Note observes that "with the advent of electronic discovery . . . traditional document-by-document privilege logs may be extremely expensive to prepare." Furthermore, the Committee Note reminds us of the importance of cooperation in e-discovery, citing both Fed. R. Civ. P. 1 and the Sedona Cooperation Proclamation.

Also, let's not forget judges' standing orders. Noted e-discovery attorney Phil Favro recalls his old boss, Judge Jeremy Fogel, calling them the 'local local rules."

## Third Circuit: Delaware, New Jersey, Pennsylvania, U.S. Virgin Islands*



**DATA PROTECTION LAW: ATTORNEY-CLIENT PRIVILEGE AND DATA BREACH REPORTS**

### *Neither Privilege nor Work Product Protected Data Breach Investigative Report*

***In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-382 (M.D. Pa. July 22, 2021).**

## The Facts

Rutter's operates a chain of dozens of convenience stores throughout Pennsylvania, West Virginia, and Maryland. The company received two Carbon Black Defense alerts on May 29, 2019, detailing the execution of suspicious scripts and indications of the use of potentially compromised credentials. On that same day, Rutter's retained outside legal counsel, BakerHostetler, "to advise Rutter's on any potential notification obligations." The following day, BakerHostetler hired Kroll Cyber Security, LLC "to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident." The breach resulted from malware being installed in the payment system used at the Rutter's' stores.

A class action of Rutter's customers sued Rutter's over the data breach during the Fed. R. Civ. P. 30(b)(6) deposition of Rutter's' corporate representative, the customers became aware of the Kroll investigation and sought production of Kroll's report of its investigation. Rutter's opposed the customers' request, arguing the report was protected by both the attorney-client privilege and the work product doctrine.

## The Law

The court rejected both Rutter's' attorney-client and work product arguments. On work product, U.S. Magistrate Judge Karoline Mehalchick held work product did not apply because there was not a reasonable anticipation of litigation, a requirement for protection under the work product doctrine.

"It is clear from the contract between Kroll and Defendant that the primary motivating purpose behind the Kroll Report was not to prepare for the prospect of litigation . . . The purpose of the investigation was to determine *whether* data was compromised, and the scope of such compromise *if it occurred*." (Emphasis in original.) The court added that Rutter's' corporate representative admitted that litigation was not contemplated at the time of the Kroll report.

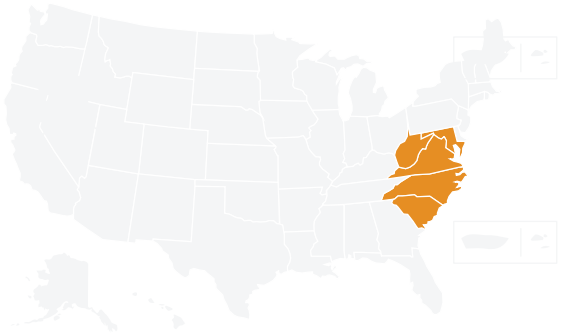
On the attorney-client privilege, the court noted that—because it "obstructs the truth-finding process"—it is construed narrowly, and added that the privilege does not protect facts, —only legal advice. "Here, Defendant does not establish that the Kroll Report and related communications involved 'presenting opinions and setting forth ... tactics' rather than discussing facts," the court wrote.

## Why the *In re Rutter's* Matters

When analyzing the importance of *In re Rutter's*, it's worth considering decisions that went the other way. *Capital One Customer Data Sec. Breach Litig.* is an interesting case because the Eastern District of Virginia issued two decisions. In a June 2020, decision, the court held a report was not protected, but in a November 2020, decision, the court held a different report was protected. In a 2017 California federal court decision, In re: *Experian Data Breach Litig.*, the court held a data breach investigation report was subject to the work product doctrine. *Experian* can be distinguished from *Rutter's* in that, in *Experian*, the investigative report was provided to Experian's outside litigation counsel, who then provided it to Experian's in-house counsel, and was not provided to Experian's Incident Response Team. In *Rutter's*, Kroll sent the report to Rutter's directly, and there is no evidence BakerHostettler was ever involved after retaining Kroll initially.

We don't give legal advice on these pages, but the friendly advice is to let the lawyers handle any reports on which you might want to claim privilege later.

## Fourth Circuit: Maryland, North Carolina, South Carolina, Virginia, West Virginia



**DATA PROTECTION LAW: DATA BREACH DAMAGES**

### *e-Discovery Legend Facciola Sets a Standard for Data Breach Monitoring Damages*

***In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.*, MDL No. 19-MD-2879 (D. Md. July 20, 2021).**

### The Facts

In 2016, Marriott International acquired Starwood Hotels & Resorts Worldwide, becoming the first hotel chain with over one million rooms. In buying Starwood, Marriott acquired not only Starwood's Sheraton, Westin, W, Le Meridien, and St. Regis hotels, it acquired a massive data breach.

Unbeknownst to Marriott—or Starwood, for that matter—Starwood had sustained a data breach sometime in 2014. The data breach went undetected until Marriott detected in 2018 that the 2014 data breach had occurred. In addition to regulatory fines, Marriott—as the accessor to Starwood—faced multidistrict litigation (MDL) under U.S. District Judge Paul Grimm of the District of Maryland with the noted e-discovery jurist, retired U.S. Magistrate Judge John Facciola serving as special master. Marriott challenged the MDL data breach plaintiffs' damages claims for monitoring their accounts, seeking information on how much time the plaintiffs actually spent searching for fraudulent purchases. The data breach plaintiffs submitted the hours they had spent, but they objected to producing documents related to the searches as overly burdensome.

### The Law

Serving as special master, Judge Facciola conducted a classic analysis, complete with graphs and charts. He noted the median time spent searching was 27 hours and that the average was 33 hours, adding that there was a vast disparity among the plaintiffs—with one consumer spending five times the median amount of time searching her accounts.

Judge Facciola said Marriott's demand that all plaintiffs produce all their records was overbroad. He noted that 27 hours over the three-and-a-half-year period was about the amount of time most Americans would spend reviewing their banking records—even if they had not sustained a data breach. Thus, Judge Facciola recommended to Judge Grimm that Marriott get no additional discovery on the issue from those plaintiffs. That left five consumer plaintiffs who claimed more than 27 hours. Even for those plaintiffs, Judge Facciola rejected Marriott's call for all the records. Special Master Facciola said a six-month period would suffice. Thus, he recommended Judge Grimm let Marriott have records from January to June 2021, noting that this limited discovery was proportional to the needs of the case using the six-pronged analysis of Fed. R. Civ. P. 26(b)(1).

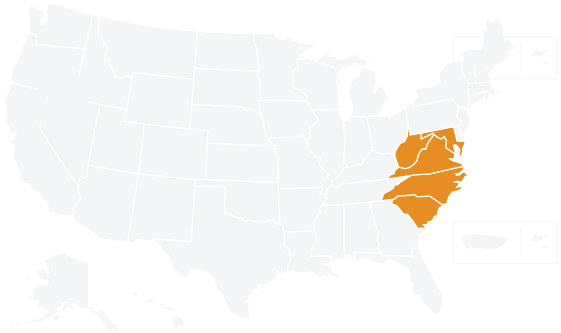
### Why *In re Marriott* Matters

John Facciola is a legend in e-discovery law, and he's taken his no-nonsense approach—complete with charts and graphs—to determining discovery for damages in data breach cases. As we've noted before on these pages, there are differences of opinion on data breach damages. Some have argued that the mere exposure of their personal data should suffice for damages, while others—usually organizations having sustained a data breach—argue that plaintiffs should have to show actual damages, such as having their identities stolen online, to prevail.

When it comes to discovery for data breaches damages, Judge Facciola noted that, had discovery not ended, the parties could have invested in another round of depositions or interrogatories, so he, instead, offered his approach, which he called, "another solution that will resolve this controversy."

Litigants and counsel in data breach litigation can look to the "Facciola Data Breach Monitoring" standard that you're not going to get discovery on anything less than an hour a month in monitoring. For discovery on bigger monitoring claims, you might get a legal legend applying Rule 26(b)(1)'s proportionality analysis.

## Fourth Circuit: Maryland, North Carolina, South Carolina, Virginia, West Virginia



**E-DISCOVERY LAW: SANCTIONS**

### *Court Sanctions Unite the Right Litigant with Expansive Definition of 'Intent to Deprive'*

***Sines v. Kessler,* No. 3:17-cv-00072 (W.D. Va. Oct. 22, 2021).**

## The Facts

Elizabeth Sines and various other plaintiffs sued Jason Kessler, Matthew Heimbach, the Ku Klux Klan, and others under federal and Virginia state law, alleging they sustained injuries from unlawful conduct at the so-called "Unite the Right" rally in Charlottesville, Va., on August 11 and 12, 2017.

The Sines plaintiffs moved for sanctions against defendant Matthew Heimbach, alleging Mr. Heimbach destroyed responsive electronically stored information (ESI) in violation of court orders under Fed. R. Civ. P. 27(b), and they sought a mandatory adverse inference instruction to the jury under Fed. R. Civ. P. 27(e)(2). Such an instruction would have the judge telling the jury Mr. Heimbach destroyed the evidence and that they could assume the evidence was favorable to the Sines plaintiffs. Mr. Heimbach countered that sanctions were inappropriate because the destruction of the evidence was accidental. He claimed his toddler "busted" one phone and that his wife destroyed data accidentally when she got him a new phone for his birthday.

## The Law

With the 2015 amendments to Rule 37(e)(2), Mr. Heimbach would had to have had an "intent to deprive" the Sines plaintiffs of the evidence, something Mr. Heimbach said he did not have.

However, U.S. Magistrate Judge Joel Hoppe held—and U.S. District Judge Norman Moon upheld on Nov. 19—that Mr. Heimbach's actions evidenced an intent to deprive, noting Mr. Heimbach's "testimony describing his conduct in pretrial discovery was at times evasive, internally inconsistent, or simply not believable. At bottom, however, he admitted under oath that he took minimal, if any, steps to preserve the ESI at issue in Plaintiffs' motion and that he made no effort to recover that information once he realized it was lost." *Citing Ungar v. City of New York*, 329 F.R. D. 8 (E.D.N.Y. 2018), Judge Hoppe held the actions of Mr. Heimbach's toddler and wife were irrelevant. It was Mr. Heimbach's "actions, or lack thereof" that demonstrated an intent to deprive.

## Why *Sines* Matters

Observers have noted that most drunk drivers do not think to themselves, "I think I'll go out and kill someone tonight." Nevertheless, the law now provides very serious sanctions because intent is established by having eight martinis and getting behind the wheel. The same principle applies here.

The 2015 e-discovery amendments to the Federal Rules of Civil Procedure were not without controversy. Among other things, the plaintiffs' bar and public interest groups argued the intent to deprive would make it too difficult to get the most severe sanctions, making it open season for spoliators to destroy evidence without fear of serious repercussions.

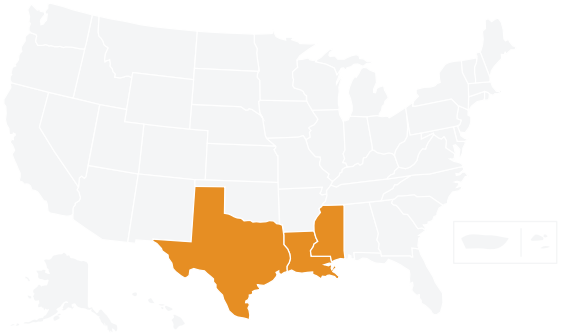
Judge Hoppe's decision should put some minds at ease. Passive dereliction of discovery duties qualifies for serious sanctions—even if wives and toddlers are involved. "Whether the spoliator *affirmatively* destroys the data, or passively allows it to be lost, is irrelevant; it is the spoliator's state of mind that logically supports the adverse inference." Thus, a party's "conscious dereliction of a known duty to preserve electronic data—whether passive or active—is both necessary and sufficient to find that the party acted with the intent to deprive another party of the information's use under Rule 37(e)(2)," the court wrote.

## Fifth Circuit: Louisiana, Mississippi, Texas

**E-DISCOVERY LAW: SANCTIONS**

### *Sandy Hook Families Prevail After InfoWars' Discovery Abuse*

***Heslin v. Jones,* No. D-1-GN-18-001835, Tex. 459th Dist. Ct., Travis Co. (Sept. 27, 2021).**



## The Facts

On a day that former President Barack Obama called the worst of his presidency, December 14, 2012, a 20-year-old neighbor shot and killed 26 people—including 20 children—at the Sandy Hook Elementary School in Newtown, Conn. Conservative conspiracy theorist and *InfoWars* host Alex Jones and his fellow *InfoWars* host, Owen Shroyer, claimed the Sandy Hook shooting was a hoax perpetrated by Second Amendment opponents.

The parents of some of the Sandy Hook children and an FBI agent who was at the school that day sued Mr. Jones, Stroyer, and InfoWars (the company) in Connecticut and Texas, alleging the Sandy Hook conspiracy theory defamed them. During discovery, the parents claimed the InfoWars defendants failed to produce responsive evidence, but InfoWars countered that it had produced thousands of documents and that more discovery was inappropriate while they appealed the merits of the case to the U.S. Supreme Court.

## The Law

Judge Maya Guerra Gamble of the 459th District Court of Travis County in Austin rejected InfoWars' arguments and granted default judgment for the families in what she said were continual and egregious discovery violations.

Judge Jones wrote that the InfoWars defendants engaged in a "pervasive and persistent obstruction of the discovery process in general" and showed a "deliberate, contumacious, and unwarranted disregard for the court's authority." Mr. Jones countered in a press release, "Nothing less than the fundamental right to speak freely is at stake in these cases. It is not overstatement to say the First Amendment was crucified today," adding that Judge Gamble had committed a "blatant abuse of discretion" in issuing the default judgment when the cases are pending before the U.S. Supreme Court, where Jones and his fellow defendants are seeking review of the Texas Supreme Court's denial of their motion to dismiss.

**For in-depth coverage, please see David Horrigan, *e-Discovery News: Sandy Hook Families Prevail After InfoWars' Discovery Abuse,* *The Relativity Blog,* Oct. 13, 2021.**

## Why the *Sandy Hook* Cases Matter

No matter what one's political beliefs may be, it's hard not to find *InfoWars'* Sandy Hook conspiracy theories to be beyond tasteless and offensive.

But should their case be thrown out of court for discovery violations when they did produce a lot of data? We should note that Judge Gamble ruled the production "does not satisfy Defendants' outstanding obligations." Also, this case occurred in state court. Were it in federal court, the "intent to deprive" standard of Fed. R. Civ. P. 37(e)(2) might apply because the case involves electronically stored information. Without such a finding, the nuclear option of a default judgment would not be available. However, Judge Gamble said InfoWars violated court orders. Thus, it could also trigger sanctions under Fed. R. Civ. P. 37(b) for "failure to comply with a court order.

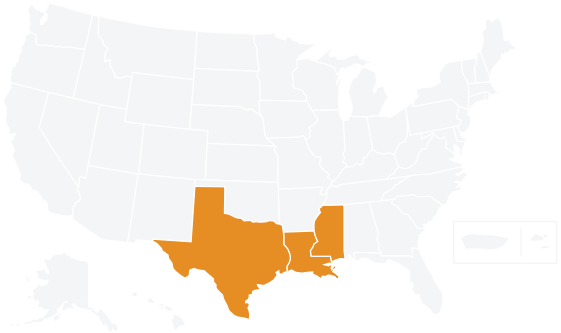
What about the First Amendment argument? Retired U.S. Magistrate Judge Andrew Peck, Senior Counsel at DLA Piper, isn't buying it. "The judicial system will grind to a halt if parties could disobey or ignore court orders with impunity because the case involves First Amendment issues," Judge Peck said.

## Fifth Circuit: Louisiana, Mississippi, Texas

**SOCIAL MEDIA LAW: DEFAMATION**

### *Summary Judgment Reversed on NFL Hall of Famer Deion Sanders' Social Media Claim*

***Sanders v. Sanders*, No. 05-20-00395-CV (Tex. App. 5th Dist. Nov. 19, 2021).**



## The Facts

Deion Sanders is a legend in professional sports. A nine-time All-Pro and a member of the Pro Football Hall of Fame, Mr. Sanders is the only person to have played in both the National Football League's Super Bowl and Major League Baseball's World Series, having been a professional baseball player as well. He has also been an analyst for CBS Sports, and he serves currently has the head football coach at Jackson State University.

Mr. Sanders was married to Pilar Sanders from 1999 to 2013. After their divorce, Mr. Sanders sued Ms. Sanders for defamation, alleging, among other things, that Ms. Sanders made social media posts claiming Mr. Sanders had abused her physically, had attempted to murder her, and had kidnapped at least one of their children. Mr. Sanders claimed Ms. Sanders' statements caused him damages, including the loss of his Oprah Winfrey Network show ($500,000), the loss of endorsement deals with Van Heusen and GMC ($2,000,000), reduction in NFL Network payments ($500,000), and legal costs ($74,500).

## The Law

On the last day of trial, the trial court granted summary judgment to Mr. Sanders as to liability. Ms. Sanders appealed, and an intermediate appellate court reversed. Two years later, a trial court granted Mr. Sanders a second summary judgment and awarded him almost $3 million in damages, $200,000 for injury to his character and reputation, and $2,774,500 for the special damages itemized above. However, once again, an appellate court reversed the summary judgment for Mr. Sanders.

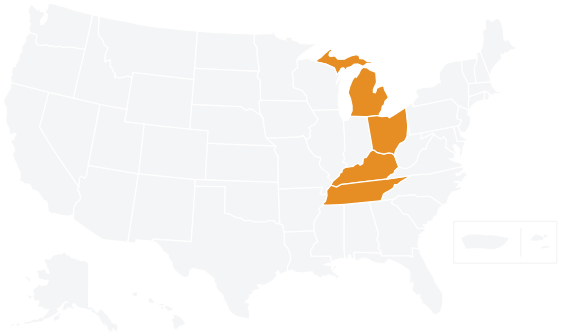
In reversing the summary judgment, the appellate court said Mr. Sanders failed to show the contracts were cancelled because of Ms. Sanders' statements and not due to some other cause. In addition, citing the Texas Supreme Court's decision in *Brady v. Klentzman*, 515 S.W.3d 878 (Tex. 2017), the court held it wasn't enough that people commented on the posts on social media and that the media reported on them. The court held that, to recover lost reputation damages, Mr. Sanders had to show people believed the posts and that his reputation was actually affected—something the court said Mr. Sanders failed to prove, with the court noting one of the accounts replying to the posts was an alias account of Ms. Sanders.

## Why the *Sanders* Cases Matter

*Sanders* is yet another example of people getting into trouble because of what they post on social media, but it's also an example of the challenges of proving damages. We should note that the appellate decision is merely a reversal of a summary judgment—it's not the final word on the matter. Having said that, the appellate court not only remanded the case for a new trial, it indicated it didn't want to see any more summary judgments from the lower court in this matter, writing, "Having reviews and reversed a summary judgment for the second time, we are satisfied there is a fact question in this case not appropriate for summary judgment."

A big takeaway from *Sanders* is: just because someone posted a false negative comment about you on social media doesn't mean you've been defamed. You must show people believed it and that your reputation was damaged. Perhaps at the new trial, Mr. Sanders will produce Oprah Winfrey to testify they cancelled his contract because of the alleged abuse along with someone from GMC telling the jury they cancelled his endorsements because they didn't want wife-beaters selling their trucks.

## Sixth Circuit: Kentucky, Ohio, Michigan, Tennessee



**E-DISCOVERY PROCEDURE: FORENSIC EXAMINATION OF DEVICES**

# *Beyond Proportionality: Confidentiality and Privilege Make Getting a Forensic Exam Difficult*

***Besman v. Stafford,* No. CV-19-915969-A (Ohio App. 8th Dist., Cuyahoga Co. Nov. 4, 2021).**

## The Facts

Sherri Besman retained attorneys Joseph Stafford and Nicole Cruz of Cleveland's Stafford Law Co., LPA, to represent her in various legal proceedings, including divorce, against her husband. After concluding the representation, Mr. Stafford and Ms. Cruz asked Ms. Besman if she wanted her file returned to her. Ms. Besman said she wanted only documents pertinent to her appeal. Ms. Besman informed the attorneys she had obtained new counsel, and she retrieved her file, executing acknowledgements that she had received her entire file, including 90 Bankers Boxes, a bag of dangerous materials, and poster boards.

Ms. Besman then filed a claim against Mr. Stafford and Ms. Cruz, alleging the attorneys had overbilled her. Ms. Besman filed a discovery request, but the lawyers reminded her she had picked -up her entire file. The attorneys filed discovery requests to Ms. Besman, but she informed them she had destroyed 53 of the 90 boxes. Ms. Besman then amended her complaint, accusing the lawyers of spoliation, and filed a motion to compel, seeking a forensic examination of the attorneys' computer.

## The Law

The trial court granted the motion to compel, but Mr. Stafford and Ms. Cruz filed an interlocutory appeal, arguing the trial court erred in granting the forensic examination of a computer containing privileged and confidential information.

In reversing and remanding, an Ohio state intermediate appellate court held the trial court erred in granting the forensic examination, agreeing with the appellant attorneys that the trial court had erred in failing to take precautions to protect the privileged and confidential data on the device. Specifically, the appellate court said the trial court failed to follow the precedent of *Bennett v. Martin*, 928 N.E. 2d 763 (Ohio App. 10th Dist 2009). In *Bennett*, a sibling Ohio intermediate appellate court held that, when ordering a forensic image, courts must weigh the significant privacy and confidentiality concerns involved in ordering a forensic image against the utility or necessity of the examination before compelling a forensic image. In addition, the appellate court held the trial court erred in failing to hold a hearing that it was Ms. Besman, not the attorneys, who were guilty of spoliation because Ms. Berman destroyed the 53 boxes.

## Why *Besman* Matters

There are multiple lessons from this case. The first may be that clients often have a lot of gall or audacity. Imagine having your client destroy over half the file—and then come after you for spoliation. Another lesson is from this author's days at *The National Law Journal*—we never destroyed notes or files until after the statute of limitations for defamation had passed. We were not in the business of defaming people—and we realized storage is not free—but lawyers should really preserve client files until the statutes of limitations for any potential claims has passed.

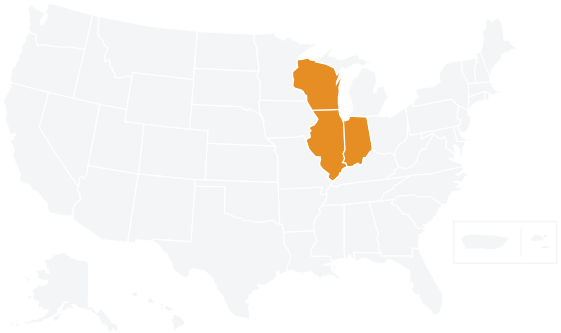
Finally, there was one glaring omission from this decision: proportionality. The appellate court quoted the *Bennett* court saying, "Generally, courts are reluctant to compel forensic imaging, largely due to the risk that imaging will improperly expose privileged and confidential material contained on the hard drive." That is partially true, but much of the time courts are hesitant because forensic imaging is often like launching a nuclear missile to deal with a few weeds in the backyard. Nevertheless, the case reminds us that proportionality is not the only reason to shy away from forensic imaging.

## Seventh Circuit: Illinois, Indiana, Wisconsin

**E-DISCOVERY LAW: SANCTIONS**

### *Missteps, Misdeeds, and Misrepresentations: Judge Johnston's Treatise on e-Discovery Sanctions*

***DR Distributors, LLC v. 21st Century Smoking, Inc.*, No. 12-CV-50324 (N.D. Ill. Jan. 19, 2021).**



## The Facts

e-Cigarettes, battery-powered devices that heat liquid into a smokable form, have become increasingly popular over the years, and that popularity continues to grow. A recent report by research firm Facts and Factors indicated that the global e-cigarette market, estimated at $14 billion in 2019, would increase to $45 billion by 2026.

Although still much smaller than the global tobacco market, which Grand View Research estimated to be $932.1 billion in 2020, the e-cigarette market is growing at a much faster rate. In 2021, e-cigarettes are where the action is—and that includes civil actions.

DR Distributors uses the trademark "21st Century Smoke" for its line of e-cigarettes, while "21st Century Smoking"—billing itself "the future of smoking today"—uses the eponymous brand name, 21st Century Smoking, for its line of products. Citing a likelihood of confusion, DR sued 21st Century for trademark infringement.

In addition to the intellectual property dispute, the parties had a big e-discovery dispute.

**For in-depth coverage, please see David Horrigan, *Missteps, Misdeeds, and Misrepresentations: Judge Johnston's Treatise on e-Discovery Sanctions,* *The Relativity Blog*, Feb. 23, 2021.**

## The Law

Brent Duke, 21st Century Smoking's president, had data in multiple places, including Yahoo! email, Yahoo! chat, and GoDaddy email.

Of course, having a veritable cornucopia of data in various venues is no problem for the sophisticated e-discovery practitioner. They initiate legal holds, conduct in-depth interviews with data custodians, develop data maps, and use the tools of the trade to ensure compliance with legal obligations in e-discovery. It didn't happen here.

Duke had a GoDaddy email account, but he failed to disclose its existence to his own lawyers. Of course, his lawyers weren't off the hook either. Their apparent lack of knowledge that web-based email and chats are held online and not on local servers became a spoliation factor.

Also, the lawyers' failure to instruct the president to disable auto-delete features resulted in even more destruction of evidence, as the GoDaddy email account deleted emails automatically.

Writing that the sanctions were intended to make DR Distributors whole and serve as a deterrent to such conduct in the future, the court issued sanctions—including issue preclusion, adverse inferences, and reimbursing DR Distributors for its reasonable attorney fees and costs, which Judge Johnston noted "will likely exceed seven figures" to be paid 50 percent by Duke and 50 percent by the lawyers.

## Why *21st Century Smoking* Matters

Is *21st Century Smoking* the most egregious example of bad behavior in e-discovery? Absolutely not.

So why a 256-page memorandum and order?

Some might call it overkill. Even Judge Johnston conceded that his practice of active case management was "perhaps hyperactive." However, in Judge Johnston's defense, he's provided a public educational service here.

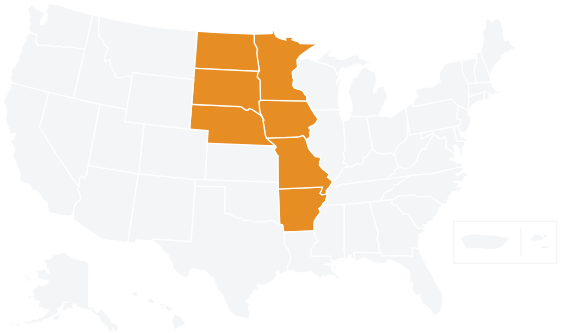
If there is ever a law school class, paralegal program, or technology training where someone needs to learn about what can happen when you spoliate evidence in discovery, Judge Johnston's treatise can serve as an educational asset.

Finally—and perhaps most importantly—Judge Johnston's treatise can serve as an educational asset for clients.

There's an old expression in construction that contractors are only as good as their subcontractors. Well, it can also be said that legal teams are only as good as their clients. If you ever feel your clients aren't being forthcoming about preserving data—or just don't want to take the time to "get" e-discovery—share Judge Johnston's treatise with them.

That part about the client being on the hook for the seven-figure sanction should get their attention.

## Eighth Circuit: Arkansas, Iowa, Minnesota, Missouri, Nebraska, North Dakota, South Dakota



**E-DISCOVERY LAW: BIOMETRIC DATA**

### *Fitbit in Court: Judge Orders Hip Implant Injury Claimant to Produce Data from Fitness Tracker*

***Bartis v. Biomet, Inc.*, No. 4:13-CV-00657 (E.D. Mo. May 24, 2021).**

## The Facts

John Bartis and Guan Hollins received M2a-Magnum metal-on-metal artificial hips manufactured and marketed by Biomet Inc. The Magnum is a three-piece device where a surgeon attaches the "acetabular cup" to the hip bone, removes the top of the femur, installs a taper insert and new artificial femoral head, and then seats the femoral head into the acetabular cup.

Bartis and Hollins alleged the Magnum implant was defective, requiring revision surgery. They sued Biomet, alleging strict product liability, negligence, fraudulent misrepresentation, and other causes of action. Bartis and Hollins were two of hundreds of people claiming injuries from the Magnum, and the cases were joined in the multidistrict litigation matter, *In re Biomet M2a Magnum Hip Implant Prods. Litig.* Although many plaintiffs settled, the matter with Bartis and Hollins was one remanded to the transferring courts for independent consideration.

During discovery, Biomet sought production of all data from any wearable device or fitness tracker, and Mr. Hollins admitted he used a Fitbit. However, he objected to production of its data, arguing it was overly broad, unduly burdensome, unreliable, etc.

## The Law

Noting that federal district courts have "considerable discretion" in pretrial discovery, U.S. District Judge John Ross noted, "There is surprisingly little precedent on this issue given the ubiquitous presence of wearable devices." In *Spoljaric v. Savarese,* a New York State court ruled a request for Fitbit data was an "overly broad fishing expedition not based upon any supportable evidence." However, in *Cory v. George Carden Int'l Circus, Inc.,* a Texas federal court held that a "mobile app that indicates Plaintiff performs strenuous activities may be relevant to claims of injury or disability."

The court noted, "Like most discovery disputes, the discoverability of wearable device data depends upon the facts of the particular case." The court held that Hollins' post-operative activity levels were relevant and that a portion of the Fitbit data should be produced, especially given the extremely low burden of production.

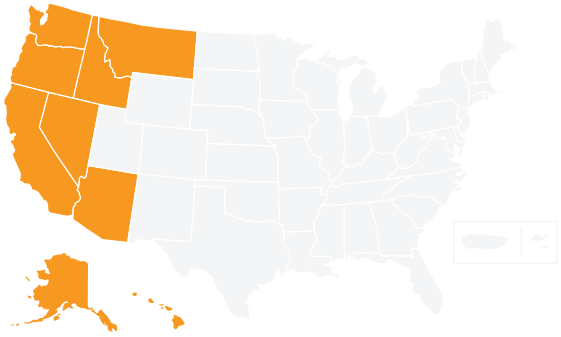
## Why *Bartis* Matters

*Bartis* helps create a body of law in an area where the court said there was "surprisingly little precedent." Biometric data—such as that contained in a Fitbit—is growing more important in litigation and investigations. As we examined in *State v. Debate*—where data from his late wife's Fitbit contradicted a husband's timeline in a murder investigation—as the use of biometric data expands, so do the legal implications.

Although the *Bartis* court allowed the use of the biometric data from the Fitbit, six states—Arkansas, California, Illinois, New York, Texas, and Washington State—have passed laws limiting the use of biometric data.

Despite the ruling in *Bartis,* as data privacy becomes a more important issue to many, look to see more restrictions on the use of biometric data in the future.

## Ninth Circuit: Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Washington State, Guam*, Northern Mariana Islands*



**DATA PRIVACY LAW: AUTOMATED LICENSE PLATE RECOGNITION**

### *Automated License Plate Recognition: Court Holds No Fourth Amendment Violation*

***United States v. Rubin,* No. 18-CR-00568 (N.D. Cal. Aug. 25, 2021).**

### The Facts

After a suspect brandishing a firearm stole various medications from a Safeway pharmacy, surveillance video captured the suspect entering the passenger side of a blue Jaguar. Using an automated license plate recognition (ALPR) system, the San Francisco Police Department determined that Lembrent Rubin was the owner of the Jaguar. A Safeway pharmacist described the alleged robber as a thin, Black man in his mid-twenties with a buzz cut and a mustache, a description closely matching Mr. Rubin.

As a result of the ALRP identification, police obtained a search warrant to place a global positioning system (GPS) device on the Jaguar, and arrested Mr. Rubin at a motel in Oakland. Police also obtained a search warrant to search Mr. Rubin's apartment, where they found narcotics, firearms, and ammunition, as well as clothing matching what the suspect in the surveillance video was wearing.

Mr. Rubin was charged with various crimes, but he moved to suppress the ALPR evidence, arguing police use of the ALPR system violated the Fourth Amendment's prohibition against unreasonable searches and seizures.

### The Law

In an apparent case of first impression—both in the Ninth Circuit and in U.S. Supreme Court jurisprudence—the U.S. District Judge Charles Breyer rejected Mr. Rubin's constitutional argument. Distinguishing Mr. Rubin's case from the cell tower data in the U.S. Supreme Court's decision in *Carpenter v. United States*, the court held that ALPR data was not the kind of "detailed, encyclopedic, and effortlessly compiled" data the Supreme Court described in *Carpenter* and thus, the ALPR use with Mr. Rubin was not a search for Fourth Amendment purposes.

"Unlike the cell-site location records there, the data here provided no more information than what could have been obtained through police surveillance. And the Supreme Court's instruction to pay careful attention to advancing technology does not support holding that a Fourth Amendment search occurred based merely on Rubin's prediction that '[i]t will not be long before' ALPR databases contain significantly more detailed information." After all, police still had the pharmacist's description of the alleged robber.

**For in-depth coverage, please see David Horrigan, *Data Privacy vs. Crime Prevention: The Automated License Plate Recognition Debate,* *The Relativity Blog,* Jan. 27, 2021.**

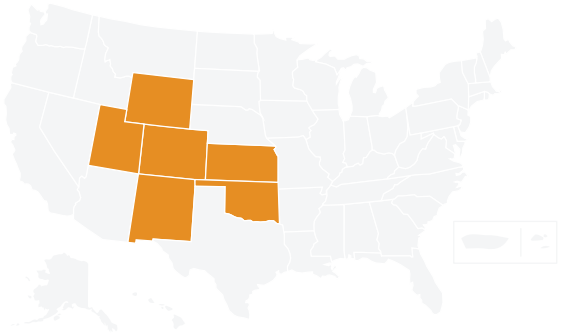
### Why the **ALPR Debate Matters**

Although law enforcement won this round, the debate over automated license plate recognition is not over. California community activist Cesar Lagleva and other community activists represented by the American Civil Liberties Union (ACLU), sued the sheriff of Marin County in *Lagleva v. Doyle* in October 2021, arguing Marin County's use of ALPR violated California law, including the California Values Act, which prohibits state and local law enforcement from sharing personal information with federal immigration agencies for immigration enforcement activities.

However, last year in *Neal v. Fairfax Cty. Police Dep't.,* the Virginia Supreme Court reversed a lower court and held a local police department's use of ALPR technology did not violate Virginia's Government Data Collection and Dissemination Act.

As litigation continues, so does the debate: Are automated license plate recognition systems a victory for safety or an unconstitutioal data privacy nightmare?

## Tenth Circuit: Colorado, Kansas, New Mexico, Oklahoma, Utah, Wyoming



**DISCOVERY LAW: SPOLIATION**

### *Utah Appellate Court Follows Third Circuit in Establishing Utah State Spoliation Standard*

***Diversified Concepts, LLC v. Koford,* No. 20191071-CA (Utah App. July 1, 2021).**

## The Facts

Rod and Jill Koford retained Diversified Concepts and Landform Design Group to construct stone retaining walls at their home as part of a comprehensive remodeling of the backyard of their home in Ogden, Utah. The home was situated on a hill with a significant slope, and the engineered stone retaining walls would allow them to add a swimming pool and playground.

Before the project was finished, the Kofords alleged the stone walls began to collapse. Unsatisfied with the response by Diversified and Landform, the Kofords had their attorney send a letter to Diversified and Landform demanding that they repair the alleged defects and telling them, among other things, "If we do not hear from you within five (5) business days, we will assume you have no intention of performing remedial work and will seek to have another contractor finish and/or repair your work." Five days later, the attorney sent a letter informing the companies they were terminated from the project. The following month the Kofords informed Diversified and Landform they had consulted engineering experts who said the companies caused the problems. They then rebuilt the walls with new contractors.

## The Law

The Kofords then sued Diversified and Landform in Utah state court, bringing various causes of action due to the allegedly defective work of the two companies. During discovery, Diversified and Landform moved for sanctions under Rule 37 of the Utah Rules of Civil Procedure. As a spoliation sanction, the companies sought dismissal of the suit, arguing the Kofords had intentionally destroyed evidence, namely, the retaining walls that were the subject of the litigation.

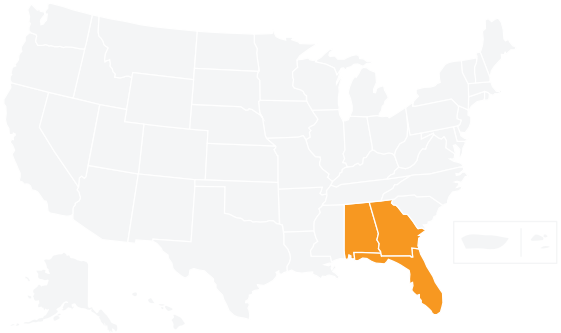
Recognizing that the record was undeveloped and that Utah appellate courts had not addressed directly the issue of Utah Rule 37 spoliation, the trial court applied case law from other jurisdictions. The trial court rejected the companies' motion for dismissal as a sanction, holding that the Kofords' attorneys' letters had given Diversified and Landform "general notice" of anticipated litigation, triggering a duty for Diversified and Landform to investigate and preserve evidence. The court said the companies should not be rewarded for their inaction by dismissal. The companies appealed, and the Utah Court of Appeals reversed, remanding the case for the trial court to apply the Third Circuit's standard in *Schmid v. Milwaukee Elec. Tool Corp.,* 13 F.3d 76 (3d Cir. 1994).

## Why *Diversified Concepts* Matters

*Diversified Concepts* presents an interesting question: What should one do when preserving evidence creates practical problems—in this case, having allegedly dangerous, crumbling retaining walls in your back yard? Readers will notice this case is labeled "Discovery Law" as opposed to "e-Discovery Law" because, after all, we're dealing with stone retaining walls, not Facebook posts or emails. Nevertheless, the case is noteworthy for e-discovery practitioners because the *Schmid* spoliation standard has proliferated across the nation—even though it is a case about the spoliation of a chain saw.

*Schmid* calls on courts to consider: (1) the degree of fault of the party who altered or destroyed the evidence, (2) the degree of prejudice suffered by the opposing party, and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party—while still deterring serious spoliators in the future. Sure, the ESI provisions of the Federal Rules of Civil Procedure take many e-discovery matters out of this *Schmid* spoliation standard—but we should always remember the overwhelming majority of litigation happens in state court.

## Eleventh Circuit: Alabama, Florida, Georgia



**E-DISCOVERY: MOBILE DATA FORENSIC EXAMINATIONS**

### *Litigant's Discovery Behavior Leads to Mobile Forensic Examination Order*

***Measured Wealth Private Client Grp., LLC v. Foster,* No. 20-cv-80148 (S.D. Fla. Mar. 31, 2021).**

### The Facts

Lee Ann Foster and Richard Kesner were employees of Measured Wealth Private Client Group LLC from 2014 to 2019. Measured Wealth sued Foster, Kesner, and their new employer, Stoever, Glass & Co., Inc., and its corporate affiliate, arguing the former employees stole client information and other trade secrets and used them to help Stoever, Glass & Co., in its business.

During discovery, Measured Wealth filed a motion to compel, seeking a forensic examination to obtain text messages and iMessages from Ms. Foster's iPhone for a one-year period. Ms. Foster objected, arguing the requested discovery was overly broad and that requesting data for an entire year was a litigation fishing expedition potentially revealing personal and private information unrelated to the issues in the case.

### The Law

In granting Measured Wealth's request for a forensic examination of Ms. Foster's phone, U.S. Magistrate Judge William Matthewman made five findings of fact:

- Measured Wealth propounded properly the written requests for the data—with Judge Matthewman noting that the court gave the parties opportunities to meet and confer.
- Text messages for the one-year period were relevant and proportional.
- Ms. Foster still possessed the phone, and a forensic examination of it was the best way to "put an end to this discovery dispute."
- Ms. Foster appeared to have been obstructionist vis-à-vis the production of text and iMessages from her phone.
- Based on sealed filings, Measured Wealth was not engaging in a litigation fishing expedition.

### Why *Measured Wealth* Matters

Ordering a forensic examination of a device is not considered a best practice in e-discovery. It's expensive, it's intrusive, and it's not unlike ordering a nuclear bomb when a mere handgun would get the job done.

So why did Judge Matthewman deviate from standard practice?

Of the judge's findings of fact, the fourth may have been the most important. If one looks at the three cases the court cited in granting the request for a forensic examination—*Barton & Assocs., Inc. v. Liska; Health Mgmt. Assocs., Inc. v. Salyer;* and *Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp.*—all three involved some sort of discovery failure by the party being compelled to submit devices for forensic examination. Whether it was the failure to produce copies of text messages and preserve a phone in *Barton & Assoc.,* a party's failure to cooperate in *Health Mgmt. Assocs.,* or a litigant's unwillingness or inability to search its computer system in *Wynmoor Cmty. Council,* Judge Matthewman's selection of cases sends a clear message.

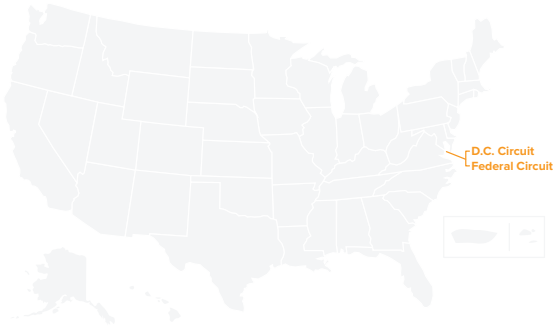
Forensic examination of devices may not be a best practice, but if you abuse the discovery process, there may be one in your future.

## District of Columbia Circuit: District of Columbia*

**E-DISCOVERY LAW: PROPORTIONALITY**

### *Pornography, Proportionality, Protective Orders, and Rule 45*

***Strike 3 Holdings, LLC v. Doe,* No. 21-2621 (D.D.C. Oct. 26, 2021).**




## The Facts

Strike 3 Holdings LLC is a company that may be known for its litigation strategy as much as its artistic offerings. An adult film producer operating under the sites, Blacked, Tushy, and Vixen, the company has filed thousands of lawsuits across the nation against alleged "porn pirates," people allegedly downloading Strike 3 adult films illegally online through systems such as BitTorrent. This case involves one of those lawsuits.

Strike 3's litigation strategy is to take the Internet Protocol (IP) address of the alleged infringer, file suit against a "John Doe," and then compel internet service providers—in this case, Verizon—to disclose the owner of the IP address. In this matter, Strike 3 sought a third-party subpoeana of Verizon's records, as it has in past cases. What does not usually happen in these cases is a court giving a thorough analysis of the six-pringed proportionality test of Fed. R. Civ. P. 26(b)(1) in deciding whether to order the release of the IP address.

## The Law

The court began its legal analysis by noting that courts have used traditionally a "good cause" standard in deciding whether to grant such discovery. However, the court noted that—under current law in the District of Columbia Circuit as articulated in the DC Circuit's 2020 decision, *In re Clinton*—a court is bound by Rule 26(b)'s limitations on discovery, including the six-pronged proportionality test.

Applying the Rule 26(b)(1) test, the court held discovery of the requested IP address was both relevant and proportional to the needs of the case. Relevance is relatively easy, and—as we've noted on these pages in the past—courts construe it broadly. Proportionality can be more challenging, but the court held Strike 3 passed the six-pronged test.

In analyzing the six factors, the court said, (1) "the importance of the issues at stake in the action" was met by alleged infringement under the Copyright Act, (2) "the amount in controversy" was sufficient, (3) "the parties' relative access to the information" was met because only Verizon had it, described as "extreme information asymmetry" by the court, (4) "the parties' resources," (5) "the importance of discovery in resolving the issues" is satisfied because discovery is the only way, and (6) the balance of the burden of the discovery versus benefit was met because the burden on Verizon was insignificant.

## Why *Strike 3* Matters

The underlying merits of the case may seem unsavory. After all, in other matters among the thousands Strike 3 has filed, the company has been sanctioned for its discovery practices—and some have argued the Strike 3 litigation is legalized extortion. Nevertheless, the case provides an excellent tutorial of proportionality in e-discovery in 2021.

Since December 1, 2015, when the six-factor test of Rule 26(b)(1) took effect, we've seen the "Proportionality: Sword or Shield" problem develop as litigants weaponize the well-intended proportionality provisions. It wasn't supposed to be this way.

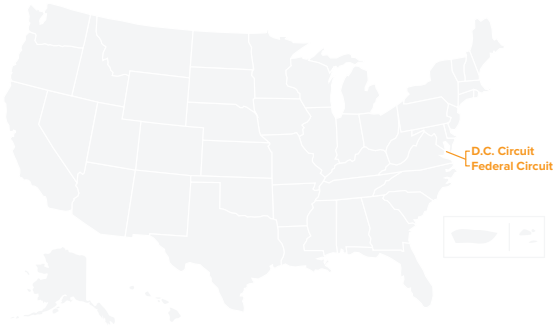
In this case, U.S. Magistrate Judge Robin Meriweather did an outstanding job of addressing this problem by providing a thorough analysis of the proportionality factors. Some may argue this case was an overly easy one. After all, we're talking one IP address, and granted, there are proportionality cases that are much more complicating. However, for one hoping to learn the nuances of proportionality, Strike 3 is a great place to start.

## Federal Circuit: (Subject Matter Jurisdiction) Patents, Trademarks, International Trade, Federal Claims

**E-DISCOVERY PRACTICE AND PROCEDURE: TIME ZONES FOR DISCOVERY DEADLINES**

### *Is Eastern Time the Standard for Discovery Deadlines?*

***Island, LLC v. JBX Pty Ltd,* 2021 U.S.P.Q. 2d 779 (T.T.A.B. 2021).**




## The Facts

JBX Pty Ltd, an Australian company, filed applications for trademarks with the U.S. Patent and Trademark Office to obtain registered marks for "Bio Island, U.S.," "Bio Island JBX," and "JBX Bio Island," for what it described as nutritional products, including supplements. Island, LLC, a U.S. company based in Wyoming, opposed JBX's application. Island holds United States Trademark Registration No. 5680487 for the mark, "Island," for goods in International Class 005 for "dietary supplements."

Island argued granting JBX's application would create a likelihood of confusion in violation of federal law, and initiated proceedings in opposition to JBX's trademark before the Trademark Trial and Appeals Board (TTAB).

On December 3, 2020, the discovery deadline Island served its discovery requests at 11:43 p.m.—from California in the Pacific Time Zone. However, at the moment of filing, it was: 12:43 a.m., December 4, at Island's principal place of business in Wyoming; 1:43 a.m., December 4, at JBX's counsel's office in Iowa; and, 2:43 a.m., December 4, at the TTAB in Washington, DC. Noting the date in the other time zones, Island objected to each of JBX's discovery requests as served untimely, and based on that objection, did not provide any substantive responses.

## The Law

We can start our analysis of the applicable law by noting what law does not apply. In this case, the non-applicable law includes Fed. R. Civ. P. 6(a)(4) and Trademark Rule 2.195, 37 C.F.R. § 2.195.

Island argued Trademark Rules and the Federal Rules of Civil Procedure applied to the dispute and that both sets of rules mandated Eastern time as controlling in the matter. Specifically, Island argued that Fed. R. Civ. P. 6(a)(4) and Trademark Rule 2.195, 37 C.F.R. § 2.195 mandate a deadline in Eastern time. However, the court rejected the argument, noting that both Trademark Rule 2.195 and Fed. R. Civ. P. 6(a)(4) pertained to submissions to the Board and the Court respectively—not with documents served between the parties, such as discovery requests. Furthermore, the Board held, "In inter partes proceedings before the Board, the timeliness of discovery requests is based on when the requests are served, not when they are received."

In addition, the cases of *Mittman v. Casey,* 329 B.R. 43 (Bankr. S.D. Ohio 2005) and *Gargula v. Streeter,* No. 05-66419 (Bankr. N.D. Ind. Sept. 10, 2010) can be illustrative of why *Island, LLC* matters.

## Why *Island, LLC* Matters

In *Mittman,* a litigant lost his argument that because he began the federal courts' Electronic Case Filing (ECF) system submission before midnight on the date of the deadline, the filing was timely even though the complaint itself came through the system after midnight.

In *Gargula v. Streeter,* No. 05-66419 (Bankr. N.D. Ind. Sept. 10, 2010), a classic case of "What time is it in Indiana?" the state with multiple time zones and different applications of Daylight Saving Time, a filing was timely in one part of a federal district and untimely in another. The filing litigant lost the timeliness argument because the court held the location of the court's ECF service controlled.

However, should we really be litigating these issues? Perhaps cooperation should carry the day. Retired U.S. Magistrate Judge James Francis IV had a response to this kind of "Gotcha!" litigation:

"My response to the party claiming that the deadline had been missed would be to send them copies of the Sedona Cooperation Proclamation and Fed. R. 1."

**For in-depth coverage, please see David Horrigan, *e-Discovery Practice and Procedure: Is Eastern Time Standard for Discovery Deadlines?, The Relativity Blog,* Sept. 7, 2021.**

**DATA PRIVACY AND DATA PROTECTION: GENERAL DATA PROTECTION REGULATION (GDPR)**

## *GDPR Fine of the Year: Amazon and Meta's WhatsApp Vie for the Top Spot*

**Commission Nationale pour la Protection des Données (CDNP) Luxembourg: €746 Million Fine to Amazon Europe Core S.a.r.l., 16 July 2021.**
**An Coimisiun um Chosaint Sonrai (Data Protection Commission) Ireland: €225 Million Fine to WhatsApp Ireland Inc. *In re WhatsApp Ireland Limited*, DPC Reference: IN-18-12-2, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018, and Articles 60 and 65 of the General Data Protection Regulation, 2 Sept. 2021.**

### The Facts

On 25 May 2018, Europe's long-awaited General Data Protection Regulation (GDPR) came into effect. Replacing Europe's 1995 Data Protection Directive, the GDPR is an effort to harmonize the laws of the various nations in the European Economic Area and provide greater data privacy and data protection.

Almost immediately after the GDPR became effective, complaints and fines began. Before this year, the largest GDPR fine was a €50 million fine in 2019 against Google. However, this year, the Europeans have outdone themselves. In July, Luxembourg's data protection authority fined Amazon €746 million, and in September, Ireland's data protection authority fined Meta's WhatsApp €225 million. The fine to Amazon was over its collection and use of user personal data obtained from digital cookies, and the fine to WhatsApp involved a defective privacy notice.

### The Law

There is less known about the legal rationale of the Amazon fine because, under Luxembourg law, details of proceedings such as the one involving Amazon remain largely private until appeals are exhausted. However, Amazon disclosed the fine in a U.S. regulatory filing, saying it would appeal vigorously. The French public interest group, La Quadrature du Net, filed the complaint against Amazon—and Apple, Facebook, Google, and LinkedIn as well—in 2018, arguing the companies violated the GDPR provisions governing the use of cookies.

The WhatsApp fine was initially much smaller, but—after Ireland's data protection authority proposed fines of €50 million or less, the European Data Protection Board (EDPB), the organization overseeing GDPR enforcement, said the fine was too low, the Irish DPA increased it to €225 million. WhatsApp's violations included an alleged lack of transparency in its privacy policies, including disclosures on how it shares personal data with other companies, in violation of Articles 60 and 65 of the GDPR.

### Why *Fines of the Year* Matters

In 2021, Amazon and WhatsApp have broken the record for the highest fines ever issued under the GDPR. So which one should be our Fine of the Year? At €746 million, Amazon's fine is over three times larger than the second largest fine, WhatsApp's penalty of €225. However, does that mean Amazon should win automatically?

Noted European e-discovery expert Chris Dale has lamented the obsession with fines under the GDPR, stressing that we should be paying more attention to GDPR principles, such as privacy by design. With this Dale Doctrine in mind, it seems WhatsApp should win Fine of the Year.

Yes, it's fine was a fraction of Amazon's, but transparency in privacy policies is a tremendously important issue affecting most organizations. Second, and perhaps more importantly, the WhatsApp fine represents the largest fine by far from the Irish DPA. With Ireland being the European home to most of the large American tech firms, Irish Data Protection Commissioner Helen Dixon and her team have been criticized for not being tough enough. Dixon and Company just got tough.

# About the Author

**David Horrigan** is Relativity's discovery counsel and legal education director. An attorney, law school guest lecturer, e-discovery industry analyst, and award-winning journalist, David has served as technology and intellectual property counsel at the Entertainment Software Association, reporter and assistant editor at *The National Law Journal,* and analyst and counsel at 451 Research.

His articles have appeared also in *The American Lawyer, Corporate Counsel, The New York Law Journal, Texas Lawyer, The Washington Examiner,* and others, and he has been quoted by The Wall Street Journal, American Public Media's *Marketplace, TechRepublic,* and publications of the law schools of Yale, Northwestern, Emory, and others.

A contributor to ALM's *Legaltech News* for the past 20 years, he founded *LTN*'s long-running *Technology on Trial* column after seeing the legal technology challenges faced by lawyers as he and *LTN* editor-in-chief Monica Bay reported from the ruins of the World Trade Center on September 11, 2001.

David serves on the Global Advisory Board of the Association of Certified E-Discovery Specialists (ACEDS), the Planning Committee and Faculty of the University of Florida Law E-Discovery Conference, and the Advisory Board of the *MIT Computational Law Report* at the Massachusetts Institute of Technology, where he is co-host of the law.MIT.edu podcast.

David was First Runner-Up for Best Legal Analysis in the 2020 LexBlog Excellence Awards. He started the *Data Discovery Year in Review* in 2015, and he has served as the moderator of the Relativity Fest Judicial Panel since its inception in 2014. He holds a juris doctor from the University of Florida and a certificate in international law from Universiteit Leiden in The Netherlands.

**Cover Photo Attribution:**
Charlottesville / Photo by Scott Elmquist
Cheerleaders in Uniform Holding Pom-Poms / Photo from shutterstock.com
Deion Sanders / Photo by CBS Sports
If You Feel the Desire to Write a Book, What Would It Be About? / Photo by Glenn Carstens-Peters on Unsplash
Sandy Hook Elementary School / Photo from wcvb.com
Seasonings / Photo by Luísa Schetinger on Unsplash

Relativity®