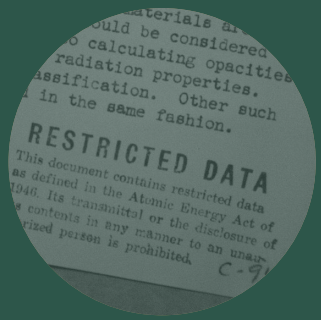
Relativity®

# 2022 Data Discovery Legal Year in Review

by David Horrigan


Eighth Edition

# Foreword

Welcome to the *2022 Data Discovery Legal Year in Review*, our eighth annual look back at the year's important developments in e-discovery and related data law disciplines. As always, the goal of the *Year in Review* is to highlight some of the key data law issues of the year in an easy-to-read and hopefully entertaining manner.

Rather than focus only on the major cases you've seen throughout the year, we bring you some of the cases you may not have seen before. We look for cases with interesting fact patterns and intriguing people to illustrate the legal issues and bring data law to life.

The cast of characters in our 2022 edition includes Texas Governor Greg Abbott, Alaska Airlines, Apple Inc., the actor Robert De Niro, the entrepreneur Elon Musk, a neophyte e-discovery consultant, a college student who had artificial intelligence scans of his bedroom, and various characters from Pokémon. We also cover the data law ramifications of newsworthy events, including the January 6 imbroglio at the United States Capitol and the raid on Mar-a-Lago to recover classified documents allegedly taken unlawfully by former President Donald Trump. These people and events bring to life important issues, including:

### Third-Party Subpoenas in e-Discovery

In 2022, we've all become miniature data centers. Our phones, our cars, and our homes all produce a veritable cornucopia of data. Not all the data are under our possession, custody, and control. As a result, third-party subpoenas, whether they are directed to our mobile phone provider, our IT vendor, or our employers, have increased substantially. We've seen an increase from 62 third-party subpoena matters in 2012 to 916 cases in 2022.

We've selected two cases from 2022 to illustrate the use of third-party subpoenas under Federal Rule of Civil Procedure 45—one where a party used Rule 45 successfully and one where it didn't work out. In *In re Pork Antitrust Litig.* where employer pork producers did not have possession, custody, and control of the mobile phones of present and former employees, the court allowed Rule 45 subpoenas to the non-party employees. However, in *Martley v. City of Basehor* a court rejected an attempt to use a Rule 45 third-party subpoena to the city's non-party IT provider despite the city's lackluster e-discovery production. *Martley* is also interesting because it involves a male former police chief who claimed he was the victim of gender discrimination.

### The Attorney-Client Privilege

The attorney-client privilege is one of the most important issues in e-discovery. In *La Union del Pueblo Entero v. Abbott*, we saw the limits of the attorney-client privilege and the ways it can be waived. In addition, the case illustrated the various types of privilege, including the investigative and legislative privileges. Speaking of waiver of the attorney-client privilege, in *Twitter, Inc. v. Musk*, we saw the issues that can arise with the privilege when employees communicate with their lawyers in the workplace.

### Data Privacy and Data Protection

After the demise of the both the U.S.-EU Safe Harbor Framework in *Schrems I* and the EU-U.S. Privacy Shield Framework in *Schrems II*, 2022 saw progress on a new initiative for data transfers between the United States and Europe with the *EU-U.S. Data Privacy Framework*. Back in the States, we saw the increasing impact of biometric data protection laws in *Barnett v. Apple, Inc.*, but we saw municipal data privacy regulations have limits in the Pokémon and police adventure in *Lozano v. City of Los Angeles*.

### Thanks to the Team and Looking Forward

This e-book would not be possible without the great work of the team here at Relativity. For years now, Kristy Esparza has brought her editing prowess to ensure my prose doesn't become a *War and Peace*-length soliloquy, and Sarah Vachlon, a Relativity veteran whose skillful artwork you've seen in *The Relativity Blog*, joined us this year to lend her considerable talents to our graphics. In addition, Beth Kallet-Neuman and Mark Bussey of Relativity's legal department provided helpful advice and counsel on the data privacy issues. We also have a new feature this year. We have included links to the actual court decisions from our friend Kelly Twigger and her eDiscovery Assistant platform, one of the best legal research tools we use in writing this e-book.

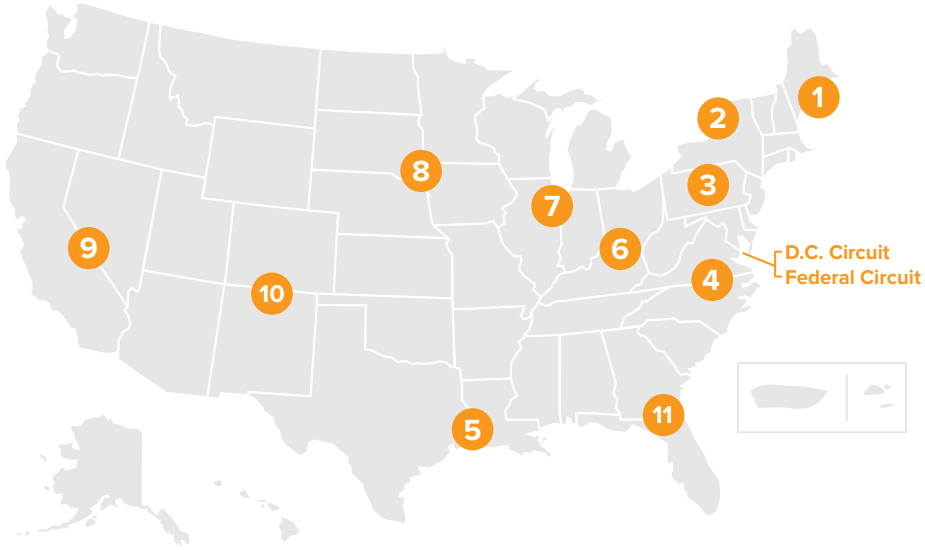
As always, this eBook is an educational resource, and it does not constitute legal advice. The topics we've covered here aren't going away any time soon, and, at Relativity Legal Education, we look forward to covering them for you in 2023.


## David Horrigan

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

# Contents

# 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 2022 Cases

## U.S. Supreme Court

**INTERNATIONAL LAW: 28 U.S.C. §1782**

# U.S. Supreme Court Holds Arbitration Doesn't Qualify for Discovery under Section 1782

***ZF Auto. US, Inc. v. Luxshare, Ltd.*, 142 S. Ct. 2078, Nos. 21-401, 21-518 (U.S. June 13, 2022).**

Read the full court decision



## The Facts

Luxshare, Ltd., a Hong Kong-based company, alleged fraud in a sales transaction with ZF Automotive US, Inc., a Michigan-based automotive parts manufacturer and a subsidiary of a German corporation. The sales contract signed by the parties provided that all disputes would be resolved by three arbitrators under the Arbitration Rules of the German Institution of Arbitration (DIS), a private dispute-resolution organization based in Berlin.

In a second matter, Bankas Snoras AB (Snoras), a failed Lithuanian bank, was declared insolvent and nationalized by Lithuanian authorities. The Fund for Protection of Investors' Rights in Foreign States—a Russian corporation assigned the rights of a Russian investor in Snoras—initiated a proceeding against Lithuania under a bilateral investment treaty. The treaty provided four means of dispute resolution and the Fund an ad hoc arbitration in accordance with Arbitration Rules of the United Nations Commission on International Trade Law.

In both matters, parties sought discovery in the United States pursuant to 28 U.S.C. §1782.

## The Law

28 U.S.C. §1782, a section of the United States Code entitled, Assistance to foreign and international tribunals and to litigants before such tribunals, provides that a U.S. district court may order a person residing in that district "to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal." In both the ZF Automotive and Lithuanian bank matters, parties to the arbitrations sought discovery in the United States pursuant to section 1782.

However, in both matters, the parties facing section 1782 discovery moved to quash the applications, arguing the arbitration panels were not "foreign or international tribunals" for section 1782 purposes. The Second and Sixth Circuits upheld district court rejections of this argument, but, in a unanimous decision, the U.S. Supreme Court reversed the consolidated cases. "These consolidated cases require us to decide whether private adjudicatory bodies count as 'foreign or international tribunals.' They do not. The statute reaches only governmental or intergovernmental adjudicative bodies, and neither of the arbitral panels involved in these cases fits that bill," Justice Amy Coney Barrett wrote for the court.

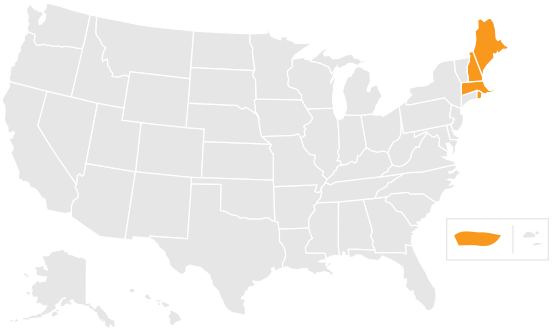
## Why the Section 1782 Cases Matter

Arbitration has become much more prevalent in the United States, but these section 1782 cases illustrate that arbitration has its limits—at least in the world of discovery.

In these section 1782 cases, the Supreme Court reasoned that it was logical to exclude arbitrational panels from section 1782 discovery because of the limits on discovery under the Federal Arbitration Act (FAA). The unanimous Supreme Court noted that the FAA permits only the arbitration panel to request discovery. "In addition, prearbitration discovery is off the table under the FAA but broadly available under §1782," Justice Barrett wrote. To summarize this point, the High Court quoted the Seventh Circuit in *Servotronics, Inc. v. Rolls-Royce PLC*: "It's hard to conjure a rationale for giving parties to private foreign arbitrations such broad access to federal-court discovery assistance in the United States while precluding such discovery assistance for litigants in domestic arbitrations."

As more and more matters go to arbitration, these matters remind us that they're not going to a forum with robust discovery.

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



**E-DISCOVERY LAW: SANCTIONS, SHORT MESSAGE DISCOVERY**

# Slack Collection and Vendor Selection Matter as Court Issues Case-Terminating Sanctions

***Red Wolf Energy Trading, LLC v. BIA Capital Mgmt.*, No. C.A. 19-10119 (D. Mass. Sept. 8, 2022).**

Read the full court decision

## The Facts

Red Wolf Energy Trading, LLC, a virtual electricity products trading company, alleged that its former employee, Christopher Jylkka, took Red Wolf's confidential information and trade secrets and disclosed them to Gregory Moeller and BIA Capital Management. Red Wolf sued Jylkka, BIA, Moeller, and others, alleging violations of the federal Defend Trade Secrets Act and the Massachusetts statute prohibiting unfair and deceptive trade practices. Red Wolf settled with Jylkka, but the action continued against BIA, Moeller, and others, and during discovery, BIA and Moeller failed to produce responsive data, including Slack messages, despite multiple discovery orders.

BIA and Moeller claimed their failure to produce the Slack messages was unintentional. Moeller claimed that, in 2019, "there was no ready mechanism to export the messages so they could be produced in litigation," and that—because BIA was a start-up with limited financial resources—they could only afford to retain a novice technician rather than an experienced e-discovery vendor to work with the Slack data.

## The Law

"Because 'federal law favors the disposition of cases on the merits,' default judgment is generally disfavored and is considered a 'drastic' sanction to be used only in 'extreme' situations," wrote U.S. District Judge Mark Wolf, citing First Circuit precedent. Nevertheless, Judge Wolf issued default judgments against BIA and Moeller, pursuant to Federal Rule of Civil Procedure 37(b)(2), due to their repeated violations of court orders.

In his default judgment order, Judge Wolf rejected Moeller's assertion that there was no ready mechanism to export and produce Slack messages in 2019, adding that there was reason to believe Moeller knew his Slack claims were not true because one of his own attorneys had stated that she had consulted a vendor who could have produced the Slack messages in an Excel spreadsheet. In addition, Red Wolf's consultant testified that "a standard eDiscovery processing tool" could have been used in 2019. The court held the failure to retain an experienced vendor and the repeated failure to produce all documents constituted a reckless disregard for duties under Rule 26 and the duty to obey court orders.

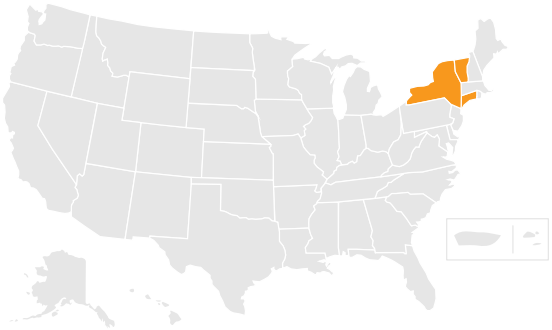
## Why *Red Wolf* Matters

Even if a default judgment is a disfavored, drastic action to be used only in extreme situations, litigants risk that outcome when their conduct inspires a federal judge to write, as Judge Wolf wrote here, that a 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 addition, *Red Wolf* illustrates that, despite the challenges of obtaining case-terminating sanctions under Federal Rule of Civil Procedure 37(e), if the discovery failures include the violation of court orders, as was the case in *Red Wolf*, Federal Rule of Civil Procedure 37(b)(2) provides for case-terminating sanctions.

Equally important takeaways from *Red Wolf* are that short message platforms such as Slack are an increasingly important part of modern e-discovery and that a failure to retain e-discovery consultants with the expertise to handle them can derail a case. Moral of the story: Slack collection and vendor selection matter.

## Second Circuit: Connecticut, New York, Vermont



**DISCOVERY LAW: SEALING OF DOCUMENTS**

# No Public Right of Access to Deposition Transcript in Robert De Niro Litigation

***Robinson v. De Niro,* No. 19-CV-9156 (S.D.N.Y. Jan. 26, 2022).**

Read the full court decision

## The Facts

In 2008, the actor Robert De Niro and his production company, Canal Productions, hired Graham Chase Robinson to be an executive assistant to Mr. De Niro. Ms. Robinson's responsibilities expanded, and she later became a vice president. However, Mr. De Niro and Canal claimed that in 2019 suspicions arose about Ms. Robinson's honesty and work ethic, and Ms. Robinson resigned later that year. After an audit, Canal sued Ms. Robinson in New York State Court, alleging she charged hundreds of thousands of dollars of personal expenses to the business credit card, used millions of dollars of company frequent flier miles for personal use, and—as was reported widely in the media—that she binge-watched 55 episodes of the television show, *Friends*, on company time. Ms. Robinson denied the allegations and sued Mr. De Niro and Canal in federal court, alleging gender discrimination and retaliation for complaining about her pay.

One thing on which the parties agreed was that Ms. Robinson's deposition transcript in the federal action should be sealed, arguing it contained highly sensitive testimony involving personal, confidential, financial, and medical information.

## The Law

In granting the motion to seal portions of the deposition, U.S. Magistrate Judge Katharine Parker noted that, under Federal Rules of Civil Procedure 5.2(d) and 26(c)(1), courts may issue orders to protect a party from 'annoyance, embarrassment, oppression, or undue burden or expense,' including by ordering the sealing of documents filed with the court." Judge Parker noted also the presumption of a public right of access applies to "judicial documents" and that the mere filing of a document with the court was insufficient to make it a judicial document. Instead, the court wrote, judicial documents "must be relevant to the performance of the judicial function and useful in the judicial process."

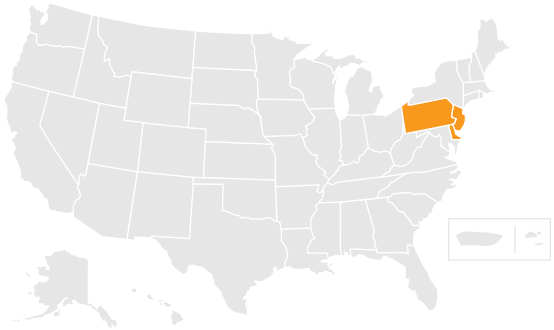
With this standard in mind, the court wrote, "documents submitted in connection with discovery disputes typically are not covered by the same qualified right of access as judicial documents, adding, "Indeed, the majority of documents and information exchanged in discovery are never even submitted to the Court in connection with dispositive motions or trial." She added, "the public has no right to access information obtained through discovery and that is subject to a protective order."

## Why *Robinson v. De Niro* Matters

*Robinson v. De Niro* illustrates the important point that discovery documents are subject to a different standard than judicial documents. Of course, discovery documents can become judicial documents, and Judge Parker wrote that there was "good cause to seal (for now) sensitive parts of the deposition transcript." She wrote "for now" because she warned the parties that the sealed portions would "not necessarily remain under seal to the extent the deposition or portions thereof are submitted in connection with dispositive motions or trial."

Few would dispute that the United States has the broadest—some would argue most intrusive—discovery in the world. However, this matter shows courts have the ability to protect parties' privacy. As we noted in *Protective Orders in U.S. E-Discovery: A Panacea for Privacy?*, protective orders under Federal Rule of Civil Procedure 26 can provide privacy protection for parties, and Judge Parker put it to good use here. The alleged binge-watching of *Friends* was a little different—that allegation ended up in a pleading filed with the court.

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



**E-DISCOVERY LAW: TECHNOLOGY-ASSISTED REVIEW (TAR)**

# In 2022, Technology-Assisted Review Is Commonplace—But Courts Will Still Disallow It

***In re Allergan Biocell Textured Breast Implant Prods. Liab. Litig.*, MDL No. 2921, No. 2:19-MD-2921 (D.N.J. Oct. 25, 2022).**

Read the full court decision

## The Facts

For over 20 years, patients across the nation received BIOCELL breast implants sold by Allergan Inc., and its predecessor companies. Women who had the implants alleged they caused Breast-Implant Associated Anaplastic Large Cell Lymphoma ("BIA-ALCL"), a cancer of the immune system that develops in the area around an implant, often between the implant and the surrounding scar tissue. Allergan recalled the implants after the U.S. Food and Drug Administration (FDA) concluded that patients were six times more likely to develop BIA-ALCL with the BIOCELL implant than other implants. Civil actions sprouted up around the nation, and in December 2019, the U.S. Judicial Panel on Multidistrict Litigation (MDL) transferred several of the matters to the District of New Jersey as an MDL.

After some discovery had been completed, Allergan moved to implement a technology-assisted review (TAR) protocol. The patient plaintiffs opposed the motion, arguing Allergan should be required to continue with search terms and linear review or apply TAR to the entire corpus of documents, including documents that had been reviewed previously.

## The Law

Retired U.S. Magistrate Judge Joseph Dickson served as special master in the case and considered the arguments of both sides. Judge Dickson noted that Allergan argued using TAR after the application of search terms was a common practice and that producing parties were best positioned to determine the means of production in discovery. In addition, Allergan cited prior TAR case law, including *In re Biomet, Livingston, Huntsman, and Bridgestone* for the proposition that TAR after keyword search is an acceptable practice. However, Judge Dickson also noted that the patients argued Allergan had not said how much money would be saved with TAR, and thus, there was no way to perform the proportionality analysis of Fed. R. Civ. P. 26(b)(1).

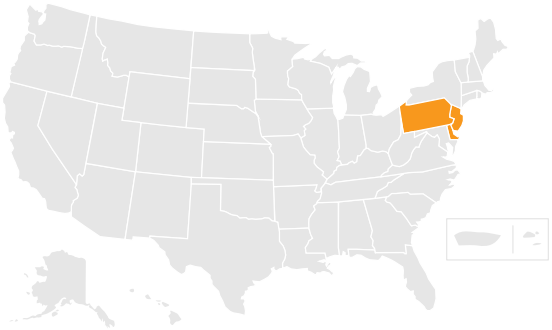
In siding with the patients, Judge Dickson rejected Allergan's interpretation of the case law. For example, the special master wrote that, *In re Biomet*, the court agreed with using TAR because Biomet provided a cost analysis that indicated continuing with linear review instead of TAR would have run into the seven figures. Judge Dickson noted that Allergan provided no such analysis.

## Why *In re Allergan* Matters

In siding with the plaintiff patients here, Judge Dickson noted the unfairness of the rules of the ballgame in the middle of the game, writing, "Because Plaintiffs did not bargain for this at the outset, over a year ago, it is inappropriate to force them to accept it now." There are arguments for and against adopting an electronically stored information (ESI) protocol at the beginning of a matter. *In re Allergan* is an illustration of why it's a good idea in some cases. Allergan will not have an opportunity to benefit from the use of technology-assisted review—and they might have been able to use TAR if they had an ESI protocol.

Another takeaway from *In re Allergan* is to quantify the savings of TAR as much as possible when moving the court to permit its use. If you want to change horses midstream, you're already starting with a disadvantage. Having detailed, quantified cost savings could help you overcome the burden.

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



**E-DISCOVERY LAW: ATTORNEY-CLIENT PRIVILEGE**

# No Workplace Waiver in Musk-Twitter Attorney-Client Privilege Dispute

***Twitter, Inc. v. Musk, No.* 2022-0613 (Del. Chan. Ct. Sept. 13, 2022).**

Read the full court decision

## The Facts

Elon Musk, of Tesla and SpaceX fame, entered into an agreement to purchase the social media company, Twitter Inc., and take it public. Claiming that, after doing due diligence, he discovered misrepresentations in Twitter's value, including due to fake accounts, Mr. Musk sought to rescind the deal. However, arguing there was no misrepresentation in the sale, Twitter sued Mr. Musk in Delaware Chancery Court, seeking to enforce the terms of the agreement.

The case would end up providing a veritable cornucopia of e-discovery law decisions on issues ranging from data collection from messaging apps to the attorney-client privilege. During discovery, Twitter sought emails that Mr. Musk had written on the email systems of his companies, SpaceX and Tesla. Mr. Musk objected to their production, arguing they were subject to the attorney-client privilege. However, Twitter countered that the companies' policies provided that the companies had the right to view the emails. Therefore, Twitter argued, Mr. Musk had waived the privilege.

## The Law

Mr. Musk argued that he had not waived the privilege because, he claimed, he was not subject to the companies' policies allowing them to review employee email. In addition, employees of the companies testified that no one had reviewed Mr. Musk's email and that they would not have.

In deciding whether Mr. Musk had waived the privilege, the court sought to determine whether Mr. Musk had maintained a "confidential" conversation pursuant to Delaware Rule of Evidence 502. In making this determination, the court relied on a four-pronged test for determining whether the use of corporate email waived privilege that was articulated by the court in *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (S.D.N.Y. 2005).

Using the *Asia Global* test, the court rejected Twitter's attempts to get Mr. Musk's email, holding Mr. Musk demonstrated a reasonable expectation of privacy over his SpaceX and Tesla emails, thus preserving the privilege.

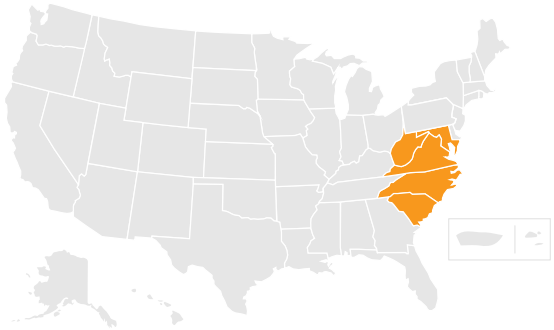
## Why *Musk* Matters

First things first. As we've said in the *Legal Year in Review* before, having conversations with your lawyer about personal legal matters on company email is a really bad idea. Mr. Musk dodged the bullet here, but his situation is somewhat unique.

Readers of the *2017 Year in Review* will remember we discussed *Peerenboom v. Marvel Entertainment, LLC*, 148 A.D.3d 531 (N.Y. App. Div. 2017), the saga of the CEO of Marvel, a subsidiary of Disney, who emailed his lawyer about a personal legal matter on the work email. In Musk, the court gave Elon Musk a break under the *Asia Global* standard, but in *Peerenboom*, the court held he waived the privilege because, as CEO, he should know the corporate policies.

Mr. Musk was lucky here with his "special rules for special people" exception to the SpaceX and Tesla computer use policies. The *Musk* court concedes, "A cynic might doubt that Musk-specific policies exist at SpaceX and Tesla," but the judge did. Nevertheless, although the Mail of Musk matter illustrates an exception, the general rule remains: stay off work email when talking with your personal attorney.

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



**TECHNOLOGY AND ACCESS TO JUSTICE: UNAUTHORIZED PRACTICE OF LAW**

# Can Software Engage in the Unauthorized Practice of Law?

***In re Peterson*, No. 19-24045 (Bankr. D. Md. June 1, 2022).**

## The Facts

When Rohan Pavuluri was a student at Harvard, he developed an interest in technology and access to justice. He observed that bankruptcy was one area often left out of the access to justice conversation. With bankruptcy and access to justice in mind, Pavuluri teamed up with New York lawyer Jonathan Petts in 2008 to co-found Upsolve, a nonprofit 501(c)(3) organization dedicated to helping people who could not afford the cost of legal representation in Chapter 7 bankruptcy proceedings. Describing itself as "TurboTax for bankruptcy," Upsolve's program includes a software application it calls its "Free Filing Tool."

Without legal counsel, Renee Patterson in *In re Patterson* and Kimya Crawford in *In re Crawford* both filed voluntary Chapter 7 bankruptcy petitions in 2019 in the U.S. Bankruptcy Court for the District of Maryland. They filed declarations of pro se assistance stating that they had received free legal assistance in preparing their forms from Upsolve, noting that—because Upsolve provided its services pro bono—Upsolve was not a petition preparer under section 110 of the Bankruptcy Code.

## The Law

Seeing Upsolve's involvement in both proceedings and noticing the similarity in the language, the court entered an Order to Show Cause to Upsolve. The court believed Upsolve's website indicated Upsolve was doing more than a bankruptcy petition preparer was authorized to do under 11 U.S.C. § 110. Upsolve argued there was no practicing of law, noting that the "user-driven" software had screening criteria that filtered out "users whose situations might require specialized advice or the exercise of legal judgment." In addition, the nonprofit said it was not subject to section 110 of the Bankruptcy Code because it did not receive compensation for its services. Although the court agreed that Upsolve did not fall under section 110, it held the way the software worked constituted the practice of law. "Upsolve fails to recognize that the moment the software limits the options presented to the user based upon the user's specific characteristics—thus affecting the user's discretion and decision-making—the software provides the user with legal advice," U.S. Bankruptcy Judge Stephen St. John wrote. Even before the order, Upsolve had agreed to suspend the use of its software in Maryland and modify it to pass legal muster vis-à-vis the unauthorized practice of law.

## Why the Upsolve Cases Matter

Judge St. John provided an excellent summation of the access to justice-legal ethics conundrum in the Upslove matters: "Providing affordable and zero-cost options to assist the impecunious in accessing their legal rights is, without question, the greatest challenge faced by the bar and courts at every level and in every jurisdiction. Technology may enhance such access; however, it does not obviate the concurrent need to ensure that all such mechanisms, regardless of their moniker, operate in a competent, ethical, and responsible manner and in accordance with applicable law."

The judge added that the court did not doubt Upstart conducted itself "with good intentions and in good faith" and that Co-Founder Pavuluri's testimony was "sincere and grounded in good motives." Upsolve is working with the court and the United States trustee to resolve the legal advice issue. It's a great example of people coming together, helping others, and following Federal Rule of Civil Procedure 1's call for the court and the parties "to secure the just, speedy, and inexpensive determination of every action and proceeding."

**See also David Horrigan, Can Software Engage in the Unauthorized Practice of Law?, *The Relativity Blog*, June 23, 2022.**

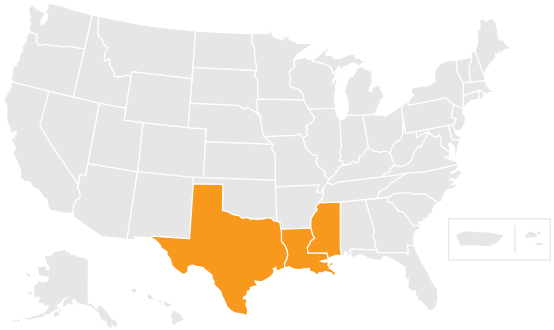
## Fifth Circuit: Louisiana, Mississippi, Texas

**E-DISCOVERY LAW: ATTORNEY-CLIENT, FIRST AMENDMENT, INVESTIGATIVE, AND LEGISLATIVE PRIVILEGES**

# Various Privileges Fail to Derail Discovery in Voting Rights Case

***La Union del Pueblo Entero v. Abbott,* No. SA-21-CV-00844 (W.D. Tex. May 25, 2022 and Dec. 9, 2022).**

Read the full court decision



## The Facts

In 2021, the Texas Legislature passed Senate Bill 1, and Governor Greg Abbot signed it into law. The omnibus voting bill made substantial changes to Texas election law, including limiting drive-through voting and prohibiting 24-hour voting. Arguing the law was passed with the intent to discriminate against racial minorities, several organizations, including La Union del Pueblo Entero and the League of United Latin American Citizens (LULAC), as well as the United States government, filed suit against the state, the governor, and several state officials.

LULAC served Federal Rule of Civil Procedure 45 third-party subpoenas on various state legislators, including the legislative sponsors of Senate Bill 1. The legislators objected to the subpoenas, asserting legislative, attorney-client, and investigative privileges and protection under the work product doctrine. After the parties failed to resolve the issue despite numerous meet and confer conferences, LULAC filed a motion to compel, seeking discovery of various documents over which the legislators claimed the various privileges.

## The Law

In granting LUCAL's motion to compel on all documents except one, U.S. District Judge Xavier Rodriguez held the legislators waived the legislative privilege on any communications with parties outside the legislature, including lobbyists, party leaders, and executive branch officials. For documents where the privilege was not waived, the court applied the five-factor test articulated in *Rodriguez v. Pataki*. Although the court said the fifth factor, the possibility of future timidity by government officials, weighed against disclosure, it said the need for accurate fact finding outweighed any chill to the legislature's deliberations.

On the attorney-client privilege, the legislators argued there was no waiver because all parties' communications shared a common legal interest in drafting legislation. However, the court rejected this argument as well, holding the common interest doctrine applied only where the parties had a common interest in litigation, not legislation. Judge Rodriguez also rejected the legislators' work product claims, noting that the work product doctrine applied only to documents prepared for the underlying litigation. Finally, the court rejected the claim of investigative privilege as well, noting the legislators had not shown there was an ongoing criminal investigation.

## Why *La Union del Pueblo Entero* Matters

*La Union del Pueblo Entero* illustrates the limitations of various privileges. The non-party legislators claimed several privileges, and the court rejected all of them, ordering them to produce all documents except one. Waiver is a constant threat when attempting to preserve privileges, and this matter was no exception.

There are a veritable cornucopia of privileges protecting confidential communications, even beyond the ones claimed by the legislators here, including spousal, priest-penitent, and even an accountant-client privilege in some jurisdictions. Should these privileges be so limited and so fragile that they are waived easily? After all, these privileges were developed for important societal reasons.

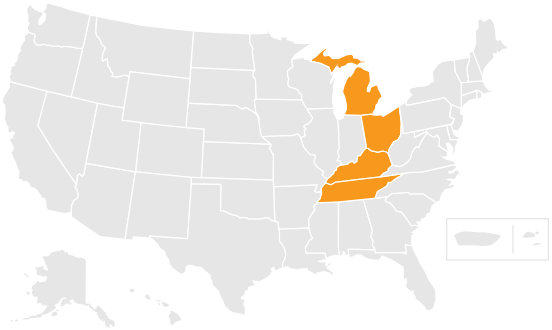
However, it's important to remember these privileges deny parties access to evidence that could affect the outcome of their cases. Justice Frankfurter articulated this point in 1960 in *Elkins v. United States* when he wrote that privileges should be "very limited" and used only for "a public good transcending the normally predominant principal of utilizing all rational means for ascertaining the truth."

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

**ARTIFICIAL INTELLIGENCE: FOURTH AMENDMENT RIGHTS**

# University's AI-Based Room Scans During Testing Violated Fourth Amendment

***Ogletree v. Cleveland State Univ.*, No. 1:21-cv-00500 (N.D. Ohio Aug. 22, 2022).**



## The Facts

To help ensure the integrity of its online remote classes, Cleveland State University used multiple proctoring tools, including Respondus and Honorlock. With Respondus, its Respondus Browser prevents students from accessing the internet or other computer programs, and its Respondus Monitor records the student taking the exam and uses artificial intelligence to flag suspicious activity. Likewise, Honorlock uses a student's camera and artificial intelligence monitoring.

Aaron Ogletree, a student a Cleveland State, took a remote chemistry test in February 2021. Ogletree lived with his mother and two siblings, and—because Cleveland State policy required students to take tests where they would be alone and uninterrupted—Ogletree had to take the test in his bedroom, which he said was the only suitable testing environment in the house. At the start of the exam, the proctor asked Ogletree to perform a room scan of his bedroom, and Ogletree complied. However, he sued Cleveland State, arguing the process violated his Fourth Amendment rights.

## The Law

Ogletree argued Cleveland State's policy of conducting warrantless room scans of students' homes violates the Fourth Amendment's prohibition against unreasonable searches as it applies to the State of Ohio through the Fourteenth Amendment. He argued he had a subjective right of privacy in his home—especially in his bedroom. Cleveland State conceded that the Fourth Amendment applied in non-criminal matters, but the university countered that the remote virtual scans did not constitute a search with the meaning of the Fourth Amendment.

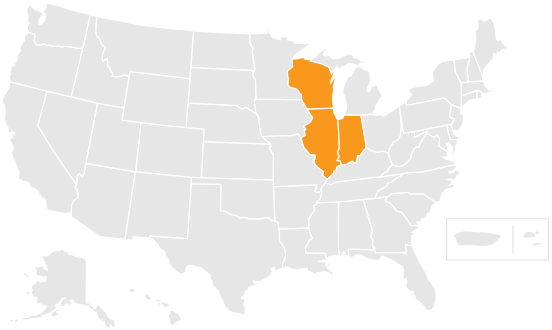
In granting summary judgment to Ogletree, the court held the room scan violated the Fourth Amendment and distinguished the case from the U.S. Supreme Court's 1971 decision in *Wyman v. James*, where the court held a public assistance caseworker's home visit to a recipient's home was not a search for Fourth Amendment purposes. In addition, the court noted that suspicionless searches were permissible where the government has "special needs," but that those cases required a balance between those needs and an individual's privacy expectations. "Ogletree's privacy interest in his home outweighs Cleveland State's interests in scanning his room," U.S. District Judge J. Philip Calabrese wrote.

## Why *Ogletree* Matters

*Ogletree* is important because it is almost certainly a precursor of legal issues to come. As technology advances—especially with continuing advances in artificial intelligence—new and novel legal issues will develop. As Judge Calabrese wrote when distinguishing *Ogletree* from *Wyman v. James*, "*Wyman* dates to 1971, more than fifty years ago. Since then, society, technology, and Fourth Amendment jurisprudence have changed markedly." As we continue in the AI era, there's a chance the next five years may rival the past 50 in technological change.

The higher education proctoring of *Ogletree* is worth noting as well. As OpenAI's release of ChatGPT in November 2022 took the world by storm, a major topic of discussion has been how to preserve academic integrity as Cleveland State was trying to do here. It's been suggested we could go back to handwritten blue book exams, but new and improved technology may solve the challenges for us.

## Seventh Circuit: Illinois, Indiana, Wisconsin



**DATA PRIVACY: BIOMETRIC DATA**

# No Illinois Biometric Information Privacy Act Violation in Apple Touch ID and Face ID

***Barnett v. Apple, Inc.*, 2022 IL App (1st) (Dec. 23, 2022).**

## The Facts

David Barnett, Ethel Burr, and Michael Henderson were residents of Illinois, when they used Apple devices with "Touch ID" and "Face ID." Touch ID is a fingerprint recognition feature giving users the option of allowing their devices to extract their fingerprints, and, as the name implies, Face ID is a facial recognition feature giving users the option of extracting their facial geometry. Users can then use Touch ID and Face ID to unlock their devices, authorize purchases on Apple Pay, and authorize purchases in Apple's App Store. Touch ID and Face ID software work by creating a unique mathematical representation stored on the user's device. If the user is enrolled in Touch ID or Face ID, the device compares the user's fingerprint or face with the saved mathematical representation already on the device.

Mr. Barnett and his fellow plaintiffs sued Apple Inc. in Illinois state court, alleging Apple violated the Illinois Biometric Information Privacy Act by offering Touch ID and Face ID without first instituting a written policy for the retention and destruction of users' biometric data and without first obtaining users' written consent.

## The Law

Enacted in 2008, the Illinois Biometric Information Privacy Act (BIPA) was the first biometric data privacy law in the United States. BIPA's provisions include a private right of action for parties aggrieved by BIPA violation, data protection obligations, prohibitions on profiting from biometric information and more. Importantly in Barnett, BIPA also requires retention guidelines and informed consent prior to collection of biometric information.

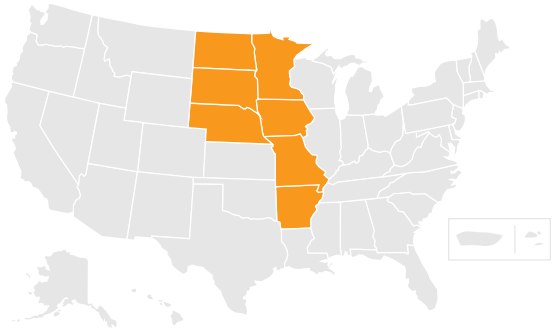
After a state trial court granted Apple's motion to dismiss, the Barnett plaintiffs appealed, but the First District Appellate Court of Illinois affirmed. The appellate court held there was no BIPA violation because Mr. Barnett and the other users chose to use the optional Touch ID and Face ID, because the biometric data are stored only on the users' devices—not in any Apple data centers—and because users can delete the biometric information from their devices without affecting the device and without any data collection by Apple. Distinguishing Barnett from other Illinois BIPA decisions, Justice Oden Walker wrote, "By contrast, in the case at bar, the feature is wholly optional, the information is stored exclusively on plaintiffs' devices, and they may delete the information at will."

## Why *Barnett* Matters

As the nation's first—and strictest—state biometric data privacy law, BIPA has triggered a substantial amount of litigation, not only by being first, but because BIPA is the only state biometric-specific data privacy law with a private right of action. For several years, Illinois, Texas, and Washington State were the only states with biometric data privacy laws, but other states have joined the biometric bandwagon. For instance, both the California Consumer Privacy Act and the Virginia Consumer Data Protection Act have biometric data privacy provisions, and several states have introduced bills addressing biometric data privacy.

Despite this biometric privacy wave sweeping across the nation, *Barnett* illustrates these laws have limits. However, we should note a lot of BIPA litigation is going the other way. Since we first covered BIPA in the *2019 Data Discovery Legal Year in Review*, we've seen substantial settlements of BIPA claims, including a $32 million settlement with Snapchat (Snap), a $92 million settlement with TikTok, and a $650 million settlement with Facebook (now Meta). In addition in October 2022, an Illinois jury returned a $228 million verdict for BIPA violations in *Rogers v. BNSF Ry. Co.*

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



**E-DISCOVERY LAW: TEXT EVIDENCE, BRING YOUR OWN DEVICE, RULE 45 SUBPOENAS**

# Rule 45 Subpoena Brings Text Message Discovery Where Employer's BYOD Policy Does Not

***In re Pork Antitrust Litig.*, No. 18-cv-1776 (D. Minn. Mar. 31, 2022).**

Read the full court decision

## The Facts

Several classes of potential class action plaintiffs sued major pork producers, including Hormel Foods Corp., Smithfield Foods Inc., Tyson Foods Inc., and others. They alleged the pork producers violated federal and state antitrust law by conspiring to control the supply of pork and fix prices by exchanging competitive, non-public information through a data company, Agri Stats, and by signaling the need to cut production through public statements aimed at one another.

During discovery, the parties agreed to an ESI protocol and a protocol for the preservation of phone records. After negotiations between the parties, the class plaintiffs sought discovery from 30 present and former employees, including text messages on personal devices. However, many custodians claimed they did not use their mobile devices for work purposes, and all custodians objected to subpoenas issued directly to them from the class plaintiffs. Hormel argued that it did not have possession, custody, or control over the text messages on its employees' personal cell phones. The class plaintiffs filed a motion to compel, seeking texts within Hormel's possession, custody, and control, as well as texts from the custodians they subpoenaed directly.

## The Law

In a split decision, U.S. Magistrate Judge Hildy Bowbeer noted varying definitions of "control," centering on whether there were a "legal right" or a "practical ability" to obtain the data. Noting the Eighth Circuit had not decided the issue, and that other circuits were split, Judge Bowbeer cited the Sedona Conference, which favored the legal right standard and criticized the practical ability standard, describing it as "inherently vague." However, Judge Bowbeer wrote that she did not need to decide the issue because—under either standard—Hormel did not have control of the data on the personal devices. Perhaps most importantly, the court rejected the class plaintiffs' arguments that Hormel's bring your own device (BYOD) policy gave it control of the data.

However, the court allowed discovery of most of the employees' texts pursuant to the subpoenas served on them directly under Rule 45 with limitations. Noting the scope of discovery under Rule 45 was the same as under Rules 26 and 34, the court considered, among other things, the burden on the custodians, and ordered Hormel and the class plaintiffs to split the costs.

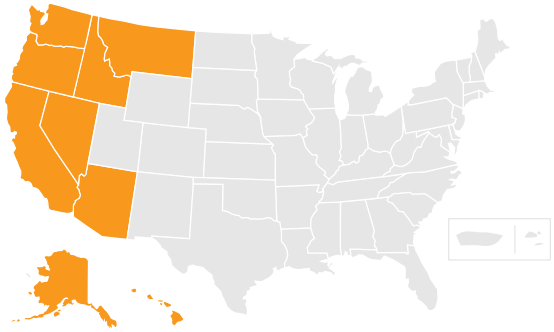
## Why *Pork Antitrust* Matters

The case highlights two important concepts in e-discovery and mobile devices: the importance of BYOD policies and the availability of subpoenas under Federal Rule of Civil Procedure 45.

On BYOD policies, although a circuit split brings uncertainty to the "control" dilemma of "legal right" versus "practical ability," the decision illustrates the influence of the Sedona Conference. "The Sedona Conference has taken the position that an employer does not legally control personal text messages despite a BYOD policy when the policy does not assert employer ownership over the texts and the employer cannot legally demand access to the texts," Judge Bowbeer wrote. Whether an employer wants that legal right is another question.

On Rule 45 subpoenas, it's worth comparing *Pork Antitrust* with what we saw in *Martley v. City of Basehor* (See page 18). Although unsuccessful in *Martley*, *Pork Antitrust* shows a Rule 45 subpoena can be used to obtain discovery when it's not available from a party in the litigation.

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



**DATA PRIVACY LAW: VIDEO EVIDENCE**

# Pokémon, Privacy, and the Police: California Appellate Court Rejects Data Privacy Challenge

***Lozano v. City of Los Angeles,* No. B307412 (Cal. App. 2d Dist. Jan. 7, 2022), review denied, No. S273136 (Cal. Apr. 20, 2022).**

## The Facts

After a police cruiser failed to respond to a robbery at a Los Angeles area Macy's store, police investigators asked the officers in question about the incident, and the officers said they did not hear the police call about the robbery. However, the officers' police cruiser had a digital in-car video system (DICVS). Not only did the DICVS reveal the officers had, in fact, heard the radio calls, it indicated they were playing Pokémon GO in their cruiser that day.

The DICVS footage revealed that—instead of responding to the robbery at Macy's—Officer Mitchell was alerting Officer Lozano that "Snorlax" had "just popped up at 46th and Leimert." The DICVS also revealed that, for the next 20 minutes, the officers discussed Pokémon GO while they drove to different locations where the virtual Pokémon GO creatures appeared on their mobile phones, noting that a "Togetic" character had just popped up in the game. Although the officers claimed they were merely discussing Pokémon, the LAPD charged both officers with on-duty misconduct.

**For in-depth coverage, please see David Horrigan, Pokémon, Privacy, and the Police: California Appellate Court Rejects Data Privacy Challenge *The Relativity Blog*, Jan. 18, 2022.**

## The Law

In an administrative hearing, the officers sought to exclude all evidence from the DICVS, arguing that their conversations were private because they did not know the DICVS was operating, and that—under Board of Police Commissioner's Special Order No. 45—the DICVS was not to be used to "monitor private conversations between Department employees."

The LAPD countered that, under Professional Standards Bureau Notice 13.5, unintentionally recorded personal communications could be used in disciplinary matters if there were "evidence of criminal or egregious misconduct."

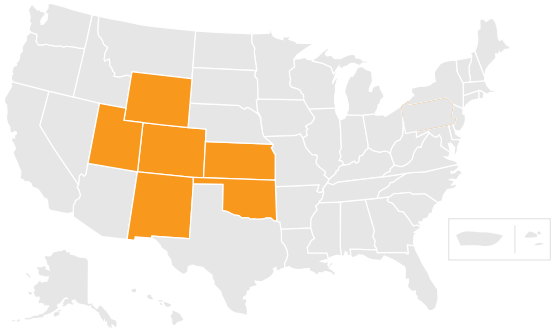
The administrative board recommended firing the officers, and LAPD's chief issued orders for their termination. The officers challenged their dismissal in a petition for administrative mandamus against the city of Los Angeles, but a trial court entered a judgment denying the officers' petition, and they appealed to the California Second District Court of Appeal. In affirming the trial court, the appellate court held the LAPD's use of the DICVS footage in the officers' disciplinary proceeding was proper, relying on 13.5's exclusion for "evidence of criminal or egregious misconduct."

## Why *Lozano* Matters

California is one of 11 states—along with Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington State—that require consent of all parties to record conversations. Maryland's law was the one that famously tripped up Linda Tripp in the Clinton-Lewinsky imbroglio when Ms. Tripp recorded her telephone conversations with Ms. Lewinsky without Ms. Lewinsky's knowledge and consent. Ms. Tripp got into legal trouble because—although Monica Lewinsky was in Washington, DC, when Ms. Tripp recorded their phone calls, Ms. Tripp was in Maryland.

Does *Lozano v. City of Los Angeles* gut the intent and spirit of California data privacy law? Granted, the LAPD did not install the DICVS to hear Officers Lozano and Mitchell playing Pokémon. Nevertheless, they did install intentionally an eavesdropping system in the vehicle, and there were conflicting administrative regulations. On the other hand, Cal. Penal Code section 632(c) contains an exception for situations where it's reasonable to believe a communication may be overheard. The Pokemon and the Police story of Lozano illustrates that California's substantial data privacy initiatives only go so far.

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



**E-DISCOVERY LAW: RULE 45 THIRD PARTY SUBPOENAS**

# Can You Use a Rule 45 Subpoena to Go Straight to an IT Vendor for e-Discovery?

***Martley v. City of Basehor,* No. 19-02138 (D. Kan. May 2, 2022).**

Read the full court decision

## The Facts

Lloyd Martley served both as police chief and city administrator of the city of Basehor, Kansas. After he retired, the chief sued the city and various city employees, arguing the city violated the federal Equal Pay Act by paying the successor city administrator, a woman, more than they paid him. The city countered that—because the chief was only a part-time city administrator—it was reasonable and lawful for the city to pay the woman, a full-time administrator, more.

By most accounts—including the judge's—the city's discovery production was somewhat lousy. In an e-discovery version of self-help, the retired chief simply went around the city, by serving a non-party subpoena under Fed. R. Civ. P. 45 to the city's former IT provider, NetStandard Data Center, to obtain documents the former chief claimed the city failed to produce during discovery. The city moved to quash the subpoena, arguing the former chief failed to give proper notice and that his subpoena was simply an attempt to get around discovery rules.

## The Law

Former Chief Martley countered that notice was proper and that the only reason he issued the Rule 45 subpoena was because of the city's repeated discovery failures. The court agreed that notice to the city was proper, but legal issue of the subpoena itself was more complicated. Although the court stressed that it was not accusing the city of misconduct, the judge was not impressed by the city's e-discovery, writing that the city's team "might not have been up to the technical nature of the task," adding, "Where there are more questions than answers regarding the document production in this case, it is not surprising that Plaintiff distrusts Defendants' efforts to search for responsive documents."

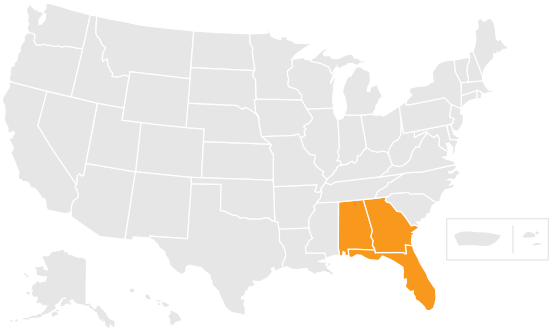
Nevertheless, the judge quashed the Rule 45 subpoena, writing, "The Court is uncomfortable with Plaintiff's tactic of going around Defendants to their former IT vendor." Nevertheless, it was not a complete win for the city. The court ordered the parties to cooperate and hire a neutral e-discovery vendor and split the cost to search for the documents sought in the Rule 45 subpoena, and it rejected the city's request for attorney fees, writing that the former chief had legitimate arguments.

## Why *Martley* Matters

Frustration with e-discovery productions is nothing new, and it can be clever to use the Federal Rules of Civil Procedure to find new ways to get the discovery you need if a party is failing at e-discovery obligations. However, as the court in *Martley* noted, quoting The Sedona Conference's *Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*, "It is a well-established principle that the burdens of discovery should fall on the parties to the litigation instead of non-party." The court noted that a party to the litigation may be the best positioned and have incentive to address properly questions of privilege, data privacy, and confidentiality, where a non-party often has no such capability or incentive.

As the *Martley* court noted, questions of possession, custody, and control, and the Stored Communications Act make discovery by Rule 45 subpoena tricky. Of course, although the city got the subpoena quashed, it should remember that it's never a good look when a federal judge orders you to cooperate after speculating that your legal team may not be up to the technical task at hand, a legal ethics issue in many jurisdictions.

## Eleventh Circuit: Alabama, Florida, Georgia



**DISCOVERY LAW: CRIMINAL MATTERS**

# Eleventh Circuit Blocks Former President Trump's Effort to Get Special Master for Mar-a-Lago

***Trump v. United States,* No. 22-13005 (11th Cir. Dec. 1, 2022).**

Read the full court decision

## The Facts

When former President Donald Trump left the White House, he allegedly took a substantial number of classified documents with him to his Florida estate, Mar-a-Lago. The former president's staff returned some of the documents, but—after months of negotiations between Mr. Trump's staff and the federal National Archives and Records Administration (NARA) proved unsuccessful, the U.S. Department of Justice obtained a search warrant and the FBI executed it at a raid on Mar-a-Lago. The FBI obtained about 22,000 pages of material from Mar-a-Lago, including more than 100 documents marked confidential, secret, or top secret. Mr. Trump filed a civil action requesting "judicial oversight," including the appointment of a special master to review the materials, and halting the government's use of the seized documents until a special master could review them. A district court granted the former president's request, and appointed a special master. The government appealed.

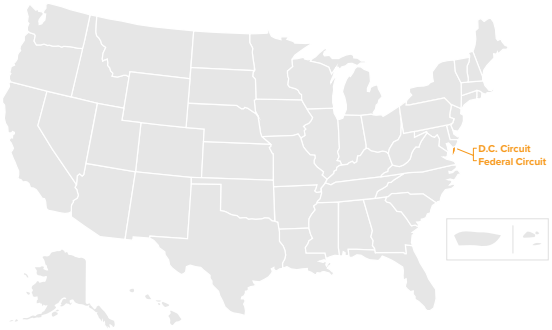
## The Law

In siding with the government, the Eleventh Circuit held the district judge lacked jurisdiction—including so-called "equitable jurisdiction"—to consider Mr. Trump's motion or to issue any orders in response to it. In rejecting Mr. Trump's argument that the court had equitable jurisdiction to intervene, the Eleventh Circuit relied, in part, on the four-pronged test it articulated in *Richey v. Smith*. The appellate court ruled there was no "callous disregard" for Mr. Trump's constitutional rights and wrote, in an unsigned decision, "Only the narrowest of circumstances permit a district court to invoke equitable jurisdiction," adding, "It is a familiar rule that courts of equity do not ordinarily restrain criminal prosecutions." The Eleventh Circuit then addressed the elephant in the room: "Only one possible justification for equitable jurisdiction remains: that Plaintiff is a former President of the United States. It is indeed extraordinary for a warrant to be executed at the home of a former president—but not in a way that affects our legal analysis or otherwise gives the judiciary the license to interfere in an ongoing investigation."

## Why the Mar-a-Lago Imbroglio Matters

Once upon a time, e-discovery was almost always only an issue in complex commercial litigation. Not anymore. Discovery has increasingly become an issue in criminal matters. Should we allow courts to use their equitable jurisdictional powers every time someone wants to use a civil action to halt discovery in a criminal matter? In *Trump v. United States*, the Eleventh Circuit took time to note the unique fact pattern where the person on whom the warrant is executed is a former president, but the appellate court did not see a need for special presidential treatment. The Eleventh Circuit summarized the importance of the decision, writing, "We are faced with a choice: apply our usual test; expand the availability of equitable jurisdiction for every subject of a search warrant; or carve out an unprecedented exception in our law for former presidents. We chose the first option . . . The law is clear. We cannot write a rule that allows any subject of a search warrant to block government investigations after the execution of a warrant. Nor can we write a rule that allows only former presidents to do so."

## District of Columbia Circuit: District of Columbia and Appeals of Federal Administrative Decisions




### E-DISCOVERY LAW: TEXT MESSAGES IN CRIMINAL MATTERS

# January 6 Defendant Was not Entitled to Discovery on Deleted Secret Service Texts

***United States v. Sheppard,* No. 21-203 (D.D.C. Dec. 28, 2022).**

Read the full court decision

## The Facts

Alexander Sheppard traveled to Washington, D.C., in early January 2021 to protest the results of the November 2020 presidential election. On January 6, as the U.S. Congress convened in the Capitol for a joint session to certify the electoral vote count, rioting erupted as protestors overwhelmed the U.S. Capitol Police and forced their way into the Capitol at around 2:00 p.m. The incident resulted in deaths, substantial damage to the Capitol, the postponement of the joint session, and it forced the evacuation of members of Congress and then-Vice President Mike Pence from the Capitol.

Social media posts and video footage showed Mr. Sheppard inside the Capitol around 2:15 p.m. The government alleges that, while inside the Capitol, Mr. Sheppard confronted the officers guarding the doors while members of Congress were being evacuated from the House Chamber and recorded video of the evacuation and of himself announcing, “They’ve shut down Congress; let’s [expletive] go!” A grand jury indicted Mr. Sheppard on six violations of federal law related to his activities in the Capitol.

## The Law

Sheppard moved to compel additional discovery from the government, including data from the U.S. Secret Service. Although, under the U.S. Supreme Court’s 1963 decision in *Brady v. Maryland*, the government has a duty to disclose evidence in its possession that is favorable to the accused, the government argued that the Secret Service was not part of the prosecution team for *Brady* purposes. However, the court held Secret Service materials were not categorically outside the prosecution’s possession or control.

Nevertheless, the court held Sheppard was not entitled to broad discovery from the Secret Service, including evidence about the phones of 10 Secret Service agents where metadata suggested text messages from January 6 were not retained, based on the materiality requirement. The court noted that Shepard had advanced no credible argument that the destroyed evidence was potentially exculpatory. “There is nothing obviously relevant about the USSS agents’ messages—whatever they may be—to Sheppard's knowledge of the restricted area, his disorderly conduct, or any other elements of the crimes charged,” U.S. District Judge John Bates wrote.

## Why *Sheppard* Matters

*Sheppard* illustrates the limits of discovery in criminal matters. Although Sheppard argued more discovery about the deleted Secret Service texts might allow him to rebut the government’s claim that all areas were clearly restricted at all times, materiality carried the day, with the court noting that evidence suggested the Secret Service agents were involved in protecting former Vice President Pence and monitoring former President Trump’s movements—not setting up or maintaining the restricted area. As the court noted, “In short, there must be some clearer link between the evidence alleged to have been destroyed and the defense's case to order the wide-reaching discovery.”

*Sheppard* is also another example of the importance of text messages in discovery whether in civil or criminal matters. In this decision, the parties were not arguing over emails. In fact, in 2022, there were over 200 e-discovery decisions involving text messages. Of course, no matter how ubiquitous text messages have become in life and law, *Sheppard* still shows that they have to be relevant to get into evidence.

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



**DISCOVERY LAW: INTERLOCUTORY APPEALS**

# No Appellate Jurisdiction over Interlocutory Appeal on 'Attorney Eyes Only' Designation

***Modern Font Applications LLC v. Alaska Airlines, Inc.*, No. 21-203 (Fed. Cir. Dec. 29, 2022).**

Read the full court decision

## The Facts

Non-practicing entities, described pejoratively by some as "patent trolls," are organizations that acquire patents for licensing or litigation purposes without using them to produce goods or services. Modern Font Applications LLC (MFA), a non-practicing entity, held a license to a patent for operating systems to read and display fonts. MFA sued Alaska Airlines in the U.S. District Court for the District of Utah, alleging Alaska infringed on the patent.

The District of Utah has a standard protective order it uses in all cases. Under the standard protective order, Alaska designated some of its source code files as "Attorney Eyes Only." MFA sought to amend the protective order so its in-house counsel could review all disclosed information, including the Attorney Eyes Only documents, but a magistrate judge declined to modify the protective order, ruling that the in-house counsel was a "competitive decisionmaker" because of his licensing activities and because MFA's "entire business model revolves around the licensing of patents through litigation with the assistance of its in-house counsel." The district judge affirmed the magistrate judge, and MFA sought an interlocutory appeal to the Federal Circuit.

## The Law

Although the U.S. Court of Appeals for the Federal Circuit has subject matter jurisdiction over patent matters, it held it lacked jurisdiction because—despite the collateral order doctrine—it did not have jurisdiction to hear an interlocutory appeal of a discovery matter. Citing the U.S. Supreme Court's decision in *Swint v. Chambers Cnty. Comm'n,* the Federal Circuit held that courts of appeal may allow interlocutory appeals that "(1) are 'conclusive;' (2) 'resolve important questions separate from the merits;' and (3) are 'effectively unreviewable on appeal from the final judgment in the underlying action.'" The court held MFA failed on the third prong because the discovery order was not "effectively unreviewable" after final judgment.

"Generally, pretrial discovery orders are not 'final'—and therefore, not reviewable—under the collateral order doctrine," the court said, citing the U.S Supreme Court's decision in *Firestone Tire & Rubber Co. v. Risjord*. "Routine appeal from disputed discovery orders would disrupt the orderly progress of the litigation, swamp the courts of appeals, and substantially reduce the district court's ability to control the discovery process," the court wrote, citing Wright, Miller, and Cooper's *Federal Practice and Procedure*.

## Why *Modern Font Applications* Matters

*Modern Font Applications* illustrates both the rule that discovery orders are not generally appealable through interlocutory appeals and the role of in-house counsel in discovery matters. Although the collateral order doctrine permits some interlocutory appeals, *Modern Font Applications* shows the difficulty in having a court hear an interlocutory appeal in a discovery matter. However, it's important to note that there are exceptions. For instance, in *Apple Inc. v. Samsung Elecs. Co.,* the Federal Circuit agreed to hear an interlocutory appeal of order denying requests to seal various confidential exhibits attached to pretrial and post-trial motions, noting, "once the parties' confidential information is made publicly available, it cannot be made secret again."

Prohibiting MFA's in-house counsel from reviewing Attorney Eyes Only documents presents another important discovery issue. As we've seen in *The General Counsel Report* from FTI Consulting and Relativity, corporate counsel are becoming trusted business advisors. As the American Bar Association has noted, "the dual role of in-house counsel as a trusted legal advisor and a business advisor and the various different scenarios in which privilege can arise further complicate the issue of attorney-client privilege for in-house counsel."

INTERNATIONAL LAW: CROSS-BORDER DISCOVERY

# EU-U.S. Data Privacy Framework: A Successor to the Safe Harbor and the Privacy Shield?

## Background: The Safe Harbor and the Privacy Shield

Before Europe's General Data Protection Regulation (GDPR) became effective in 2018, data privacy in Europe was governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, known commonly as the EU Data Protection Directive. The 1995 Directive—which went into effect in 1998—placed substantial restrictions on the processing of personal data, forbidding the transfer of personal data on Europeans to non-EU nations not meeting European adequacy standards for data privacy and protection, including the United States.

Europe's data protection legislation places substantial restrictions on the transfer of personal data from the European Economic Area (EEA) to non-EEA nations (such as the United States). The most common method for ensuring a lawful transfer of personal data from the EEA to a non-EEA country is either by (i) a determination from the European Commission that the non-EEA country is deemed adequate by upholding substantially the same data privacy standards in that non-EEA country as are required in the EEA; or (ii) the transferring parties put in place a contract that engages the European Commission's Standard Contractual Clauses, again designed to provide the same data privacy protections as those provided in the EEA.

In an effort to ensure that personal data, when transferred from the EEA remains protected to the requisite standard, the U.S. Department of Commerce and the EU created the **U.S.-EU Safe Harbor Framework** to certify U.S. Enterprises as compliant with the European adequacy standard. The U.S. created a corresponding Safe Harbor program with Switzerland. The Safe Harbor Framework was unpopular with many European data privacy advocates (including Max Schrems' privacy rights group, None of Your Business (NOYB)), who argued the Safe Harbor's self-certification meant the proverbial fox was guarding the data privacy henhouse and that enforcement was lax.

In 2013, in what has become known as *Schrems I*, Max Schrems filed a complaint against Facebook (now Meta, whose European headquarters is in Dublin) with the Irish Data Protection Commission. The Irish Data Protection Commission rejected Schrems's case, but The High Court of Ireland granted review and referred the matter to the European Court of Justice, the high court of the European Union and one of the two branches of the Court of Justice of the European Union (CJEU). In *Schrems v. Data Protection Comm'r*, No. C-362/14, the court ruled in October 2015 for Schrems, invalidating the Safe Harbor. Although Ireland is a very pro-business environment, its Data Protection Commission has issued substantial GDPR fines, including a €405 million fine in September 2022, the largest GDPR fine of the year.

In an effort to fix the shortcomings of the Safe Harbor, the U.S. and EU negotiators developed the EU-U.S. Privacy Shield Framework (July 2016). The Privacy Shield addressed some of the criticism of *Schrems I* by providing data subject access rights and enforcement provisions (among other things). On that basis, the European Commission determined that the Privacy Shield contained adequate data protection under EU law. However, Max Schrems still wasn't satisfied. In the case of *Data Protection Commissioner v. Facebook Ireland Ltd.* (known as "*Schrems II*"), Schrems argued that data subjects (i) were not protected from what he perceived to be intrusive U.S. surveillance laws; and (ii) did not have any real court of redress in the event of any data privacy dispute. He continued his data privacy crusade. *Schrems II* was not only an attack on the Privacy Shield, it was also an attempt to invalidate the European Commission's 2010 issued Standard Contractual Clauses (SCC).

On July 16, 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield Framework and the 2010 Standard Contractual Clauses, replacing them with updated Standard Contractual Clauses in June 2021 to be implemented in all contracts (including those relying on the 2010 SCCs) by no later than December 27, 2022.

## The EU-U.S. Data Privacy Framework

Seeking to address the Court decision in *Schrems II*, on March 25, 2022, European Commission President Ursula von der Leyen and United States President Joseph Biden announced an agreement in principle on a successor to the Safe Harbor and the Privacy Shield, the EU-U.S. Data Privacy Framework (DPF). It's worth noting that all three frameworks and the GDPR have covered not just the EU but the entire EEA, which includes the EU member states plus Iceland, Lichtenstein, and Norway.

On October 7, President Biden signed an Executive Order, Enhancing Safeguards for United States Signals Intelligence Activities. Along with regulations issued by the attorney general, the executive order implements into U.S. law the agreement in principle announced in March. Then, on December 13, the European Commission published its draft adequacy decision recognizing the essential equivalence of U.S. data privacy and protection standards. The DPF provides for binding safeguards that limit access to data by U.S. intelligence authorities and a new Data Protection Review Court to investigate and resolve complaints regarding access to data by U.S. national security authorities. The completion of the process is anticipated by Summer 2023. European and U.S. negotiators have worked on the DPF, in large part, because more data flows between the United States and Europe than anywhere else in the world, a fundamental part of the $7.1 trillion U.S.-EU economic relationship. However, Max Schrems has promised a *Schrems III*. Stay tuned.

## About the Author

**David Horrigan** is Relativity's discovery counsel and legal education director. An attorney, law school guest lecturer, former e-discovery industry analyst, and award-winning journalist, David has served as 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 over 20 years, he founded *LTN*'s long-running *Technology on Trial* column after seeing the legal technology challenges faced by legal professionals as he and then-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 Resource Board of the National Association of Women Judges (NAWJ), and the Planning Committee of the University of Florida Law E-Discovery Conference, and he is co-host of the law.MIT.edu podcast.

David has received the ILTA Publication Award and First Runner-Up for Best Legal Analysis in the LexBlog Excellence Awards, among others. He started the *Data Discovery Legal 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 Levin College of Law, and he is licensed to practice law in the District of Columbia.