Litigating Platform Design: Lessons from Technology Litigation Discovery

Working Draft, October 31, 2025

Background

Litigating Platform Design: The Role of Discovery and Remedy is a collaborative project between the Knight-Georgetown Institute (KGI), the Tech Justice Law Project (TJLP), and the USC Marshall Neely Center.

Overview

In recent years, an increasing number of technology-related cases have progressed beyond the pleading stage into discovery. This shift reflects courts' growing willingness to go beyond the threshold and allow fact finding and development in cases alleging algorithmic harms, data misuse, and design defects in digital platforms and products.

Contemporary discovery practices encompass conventional communications and internal records, but also technologically complex datasets, products, and digital artifacts that introduce novel procedural and legal considerations. This memorandum outlines key discovery disputes in several cases, and the adjudication of those disputes, with particular attention to the judicial treatment of discovery in litigation centering tech-related harms. The analysis is intended to inform discovery strategy in future litigation involving harmful platform design considering the following:

- *How has discovery unfolded in recent tech-related lawsuits and what insights can be gained from these proceedings?*
- *What are the major themes and most significant challenges in tech litigation?*
- *What are priorities for discussion?*

The focus here is the trajectory of discovery, the various points of contention between counsel, and the courts' resolution of these issues. It is intended to provide a high-level overview of key discovery issues, with case examples, and in complement to the project's remedy framework and taxonomy. Together, these materials offer an emerging understanding of both the procedural and substantive dimensions of emerging tech-related litigation.

Methodology and Scope

This project surveys recent discovery rulings in technology and platform-liability cases, identifies recurring patterns in judicial reasoning, and highlights strategic considerations for counsel and experts preparing to litigate discovery-intensive claims in the digital context. It draws primarily from publicly available case dockets, transcripts of court proceedings, and judicial orders, as well as informal interviews with several litigators and technical experts.

Materials reviewed include transcripts of discovery hearings, joint discovery letters and briefs, rulings on discovery disputes and related motions, and preservation orders. The scope of this review is limited to discovery-specific disputes, with particular emphasis on:

- Identification and requests of relevant documents, data sources, and preservation obligations;
- Questions of scope, proportionality, and privilege under the Federal Rules; and
- Judicial management and oversight of discovery proceedings.

This project focused on discovery in tech litigation across various areas including addictive design of social media platforms, gaming and gambling platforms, data privacy, antitrust, and civil rights violations.

Approximately 140 documents were analyzed across 10 cases. Below are summaries of key discovery issues that were contested in the litigation analyzed, along with case examples illustrating how courts addressed and resolved those disputes.

Key Findings Across Discovery Proceedings

I. Scope of Discovery

The Court has broad discretion to manage all aspects of discovery, including tailoring the scope and sequence of discovery. This authority allows the Court to expand, limit, or otherwise control discovery to ensure efficiency and proportionality, such as by restricting requests that are cumulative, duplicative, or obtainable through less burdensome means. Generally, the

scope of discovery in the analyzed cases tracks recurring disputes across several areas, including:

- proportionality under Rule 26,[1]
- custodians
- legal privilege
- confidentiality,
- trade secrets,
- technical ambiguity and vagueness of terms
- burden,
- relevancy, and
- the scope of discovery.

For instance, courts grapple with how to define the boundaries of specific platform features (e.g., whether age verification is a feature of a product) as well as what features are relevant for the merits of a case (e.g. the relevance of geolocation data to the core claims of design defect, negligence, and failure to warn). A fundamental issue in discovery disputes across cases is the inconsistent definition of key terms, like “algorithmic tool”, “location information” and what constitutes a “recommendation.” This underscores the importance of precise framing at the outset of discovery, and perhaps signals the need for a broader discovery taxonomy that shapes future cases.

A. Determining Relevant Time Period for Discovery

Particularly in product liability and negligence actions, discovery often centers on uncovering what the defendant companies knew regarding the risks associated with their products and what alternative designs or safeguards were considered prior to launch. Plaintiffs typically advocate for a discovery period extending back to the initial development and release of the relevant products or features, aiming to uncover information about the defendants’ design rationales, the evolution of product features over time, and the extent of their prior knowledge or foreseeability of harm. To broaden the scope of discovery, Plaintiffs should be able to show the technical nexus of core components of the platform or product at issue to any predecessor platform(s) and/or product(s). Courts have calibrated the temporal scope of discovery to correspond with the launch or modification dates of key product features.

- ***In re: social media adolescent addiction***: Plaintiffs contended that the recommendation algorithms used in predecessor products informed and shaped the core technological architecture of subsequent applications. They argued that TikTok was developed using technical components derived from its predecessor platforms.

[1] Rule 26. Duty to Disclose; General Provisions Governing Discovery

While recognizing the importance of identifying similarities among these products, Plaintiffs emphasized that their distinctions are equally significant, as they bear directly on issues of knowledge, intent, notice, and the feasibility of alternative designs. With respect to TikTok, Toutiao, and Douyin, the Court agreed that discovery can extend back to January 2016, approximately one year prior to TikTok's launch.

- ***In re: social media adolescent addiction***: Meta offered up a relevant time period that was based on certain features (agreed to go back to 2015 generally and then back to 2008 for feature-specific terms). Plaintiffs explained why this would be devastating and too limiting. Plaintiffs made the argument that Meta's early years are critical to understanding the design and implementation of addictive features that cause kids and young adults to become addicted to the platform. The court set feature-specific start dates in favor of the plaintiffs as follows:
    - **Facebook Newsfeed:** January 1, 2006
    - **Facebook Chat & Friend Recommendations:** January 1, 2008
    - **Algorithmic Recommendations, Endless Scroll, and "Like" button:** January 1, 2009
    - **CSAM Reporting & Geolocation:** January 1, 2010
    - **Hashtags:** January 1, 2011
    - **All other issues:** January 1, 2012

- ***Soucek v. Roblox***: Plaintiffs sought to set the start date for discovery in 2017 or 2018, asserting that relevant evidence predated the defendants' proposed start date. Defendants maintained that no pertinent documents existed prior to 2019. Plaintiffs, however, identified third-party Robux gambling websites operating as early as June 2016, that exhibited similar technical characteristics and the allegedly predatory mechanisms to those implicated in the Roblox platform at issue. Specifically, RBXWild.com used "Roblox's technology, platform, virtual content,and proprietary currency in the exact same ways as Roblox's Co-Defendants later would starting in 2019."

B. Defining Relevant Systems, Products, and Design Features

Defining key technical concepts is a pivotal part of discovery, as those definitions determine both the scope of relevant evidence and the volume and type of data each party is required to produce. Courts wrestled with the definition and functionality of digital services and whether platform features such as algorithms, notifications, or age gates are analogous to defects in physical goods. Litigators must anticipate and counter narrow definitions of such terms proposed by defendants that may conceal essential facts.

- ***In re: Google Location History Litigation*****,** the parties could not agree on the foundational definition and scope of **"location information."** Plaintiffs advocated for a broad definition encompassing any data reflecting a user's physical location—whether determined, estimated, or inferred from device sensors like GPS, Wi-Fi, Bluetooth, or cellular signals—so long as it was stored in any Google system. Google sought a narrower definition limited to location data explicitly linked to a user's Google Account, excluding information stored only on devices or in non-Google systems. Google argued that Plaintiffs' expansive definition was disproportionate and would demand excessive data production, while Plaintiffs contended that Google's narrow view concealed essential facts—such as how frequently Google receives and stores users' location data—and hindered their ability to conduct effective depositions. This definitional dispute directly shaped discovery.

C. Defining Geographic Scope

Foreign Versions/Other Products: To demonstrate the feasibility of alternative designs, plaintiffs requested discovery into other versions of the product at issue or other products that fall within the defendant's purview, provided they can establish a basis for substantial similarity and relevance. Uncovering key design elements of designs in foreign versions of products undermines companies' claims that an alternative design is "technically impossible" or too burdensome to implement. Plaintiffs argue that international platform versions informed design and marketing decisions; defendants pushed back on similarity grounds. The issue of "substantial similarity" is central—plaintiffs must show relevance between foreign and domestic products for such discovery to be allowed.

- ***In re: social media adolescent addiction***: Courts limited discovery to jurisdictions with direct relevance (e.g., U.S. and France for TikTok and the U.K. EU, and Australia for YouTube), denying global fishing expeditions.

D. Custodians

Analyzed cases involved disputes concerning the identification and preservation of custodial sources of evidence. Plaintiffs sought to preserve data from key individuals—typically key employees (e.g. CEOs) or agents who communicated about relevant issues, and the engineers and managers responsible for the development of the products at issue.

- ***In re: social media adolescent addiction***: The parties disputed whether YouTube was required to include both its former CEO, Susan Wojcicki, and its current CEO, Neal Mohan, as document custodians in discovery. YouTube maintained that only Mohan should be designated, arguing that adding both executives would result in duplicative production given the significant overlap in their tenures, that Plaintiffs had not demonstrated that Wojcicki possessed uniquely relevant information, and that including both would impose an undue burden. Although YouTube acknowledged that "the apex doctrine"[2] does not formally apply to document discovery, it invoked similar principles of proportionality and relevance to support its position. Plaintiffs, by contrast, contended that both CEOs were necessary custodians, emphasizing that Mohan did not join YouTube until 2015—after Wojcicki's appointment in 2014—and therefore their records would not be wholly redundant. Plaintiffs further argued that the apex doctrine does not restrict document discovery, that YouTube's limited data retention period mitigated any burden, and that Wojcicki's tenure encompassed key events such as the creation of the internal "Roomba" committee, the 2019 FTC COPPA enforcement action against YouTube, her 2021 congressional testimony, and several major product and feature launches in 2015, 2018, and 2019. The Court agreed with Plaintiffs and ordered that both Wojcicki and Mohan be added as custodians. To address concerns regarding duplication and proportionality, the Court limited the temporal scope of Mohan's custodial searches to documents dated on or after January 1, 2023, corresponding to the year he assumed the role of CEO, and denied YouTube's request to shift the cost of these searches to Plaintiffs.

II. Data Requests, Data Preservation, and Protective Orders

In the litigation analyzed, Requests for Production (RFPs), interrogatories, preservation orders, and protective orders were used to obtain, preserve, and seal various types of data. For the purposes of this analysis, the information was categorized into two buckets: upstream and downstream data. **Upstream discovery** targets internal company behavior and information, including the company's product design choices, data collection and storage methods, and testing and research on how their products and platforms affect user behavior and cause harm. **Downstream discovery** involves user behavior and data, particularly information reflecting user dependence or critical changes in behavioral interactions with a product or platform like usage metrics, browsing history, location data, and health data.

Overall, Defendants consistently opposed discovery into the internal mechanics of their products, citing concerns over confidentiality and competitive harm. Defendants frequently asserted that they did not possess the information sought by Plaintiffs or challenged requests

[2] The apex doctrine gives the court discretion to prevent or limit the deposition of a high-level corporate employee in certain circumstances. It is used to protect high-level executives who may lack unique knowledge. (Bloomberg Law)

on the grounds of relevance, burden, confidentiality, proportionality, or claims that the information sought was proprietary in nature. Court-issued protective orders attempted to balance discovery obligations with the need to safeguard trade secrets and prevent overly broad disclosure.

A. Upstream Disputes

Discovery Area	Specific Discovery Requested and Rationale	Case Examples / Outcomes
Internal Knowledge and Testing, Product Harm, & Causation Data	**Overview:** Plaintiffs sought documents detailing the **defendants' own training, testing, observations, and knowledge** of how their technology performs and impacts downstream user behavior, including any internal research and audits as well as communications between defendants. Plaintiffs sought data needed to prove causation, including the underlying design features and how they directly caused harm, and the defendant's own testing of its products.	• ***Mobley v. Workday***: Workday argues that some data — its Candidate Skills Match audits conducted at the direction of counsel — is protected by attorney-client, work-product, or "common interest" privilege. The court agreed with defendants and ruled that information may be accessible through other non-privileged documents. • ***In Re: Clearview AI, Inc., Consumer Privacy Litigation*:** Plaintiffs sought documents showing how Defendants "trained" their facial recognition software to match uploaded probe images to those in the database. The requests aimed to determine whether Plaintiffs' or class members' images were used in the training datasets and were also relevant because Defendants promote their technology based on its purportedly high identification accuracy. • ***In re: social media adolescent addiction:*** Plaintiffs requested "Communications with any other Defendant(s) concerning: (1) the use of social media platforms by Children; (2) the use of social media platforms by Teens; (3) age verification or age estimation for users; (4) parental controls; (5) CSAM reporting; or (6) age-appropriate design. Snap, Inc. in particular pushed back on this request arguing that the request was unduly burdensome and not proportionate to the needs of the case, and any relevant communications would be captured by existing terms and a separate RFP. Snap also argued that the proposed additional search term that would capture this information might be technologically impractical and would cause the eDiscovery system to crash. The court ordered Snap to produce attestations from its vendor confirming burden.

Design and Design Rationale	To establish defendants' knowledge and obligation to warn, plaintiffs requested documents concerning the technical design and design choices of specific product or platform features.	• ***In re: social media adolescent addiction:*** Discovery focused heavily on specific "named features" that plaintiffs alleged were defective and addictive. Plaintiffs sought information about these named features, including their technical implementation. (e.g., Newsfeed, Algorithmic Recommendations, Endless Scroll, Like button, Ephemeral messaging, Snapscore). Defendants argued that many features (like personalization and algorithmic recommendations) were barred from discovery by Section 230 and the First Amendment.
User Behavior	Plaintiffs requested data that the company uses to analyze user behavior.	• In ***FTC v. Meta Platforms***, the FTC issued a set of document requests to Meta seeking data that the company uses to analyze user and advertiser behavior, infrastructure capacity, and integrity-related issues and solutions. This information was intended to help the FTC assess Meta's market power and the competitive impact of its conduct in the personal social networking services market. • ***In re: social media adolescent addiction:*** The court required plaintiffs to produce an image from each Device routinely used to access Defendants' platforms (and other apps).

Source Code	Source code – and the versioning and archiving of such code – is crucial evidence in tech litigation because it provides the most direct, objective record of how a system actually functions, not just how a company describes it. Source code reveals what data a product collects, how that data is stored, shared, or processed, and whether those actions align with (or violate) stated privacy policies, user consents, or regulatory requirements. In tech product liability or algorithmic harm cases, the code can show whether a defect, design choice, or automated process directly caused a privacy breach, data misuse, or harm to users. Code analysis can reveal hidden or secondary data flows—such as undisclosed tracking, retention, or profiling—that may not appear in documentation or logs. Because source code is highly sensitive IP, defendants seek to limit access or require on-site inspections, while plaintiffs argue that meaningful review requires broader access creating recurring discovery conflicts.	• In ***Re: Tiktok, Inc., Minor Privacy Litigation***, Plaintiffs moved to compel enforcement of the Court's prior order requiring Defendants to produce source code related to the handling of non-TikTok user data. Plaintiffs argued that, despite the Court's April 8, 2024 order directing production of "all current and historical source code," Defendants failed to comply, offering only limited, on-site inspection in Los Angeles without specifying what code was included and imposing restrictive conditions and delays that obstructed meaningful review. • In ***In Re: Clearview AI, Inc., Consumer Privacy Litigation***, the plaintiffs requested all documents and communications related to the Clearview and Rocky Mountain facial recognition applications or software. This included all versions of their source code and all materials detailing policies, protocols, or procedures governing the collection, storage, processing, disclosure, use, or destruction of biometric data, identifiers, information, or face templates. Defendants sought to avoid discovery obligations by claiming plaintiffs' requests sought discovery of proprietary source code.
Third-Party Safety Evaluations and Risk Assessments	Documents related to the company's use of third-party organizations to evaluate its safety and appropriateness for child and teen users. This data helps to demonstrate the company's external accountability and awareness.	• In ***Soucek v. Roblox*** **and** ***Mobley v. Workday***, the court ordered Roblox to produce all documents related to its "use of third-party organizations to evaluate its safety and appropriateness for child and teen users," including organizations referenced in Roblox's safety guides, with the exception of materials solely related to Child Sexual Abuse Material (CSAM), sexual exploitation, grooming, terrorism content, hate speech, and/or bullying. Defendants objected to providing this type of data stating that it is held by other entities and should be available through third-party discovery. The court ordered the defendants to provide the documents requested.

Data Preservation Snapshots	Counsel for Plaintiffs recognized the value of requesting "snapshots" of all user data for a representative period and within a relevant jurisdiction, especially for identifying users whose claims might be obscured by changing systems or deletion policies.	• In ***Griffith v. TikTok Inc.***, plaintiffs challenged websites' use of pixel software to share non-users' data with TikTok and ByteDance. The case involved massive amounts of visitor data from thousands of sites. Still, the court found that preserving only a one-day sample of a subset of that data was relevant and proportional to the case's needs. The court attempted to balance proportionality under Rule 26, emphasizing the "vast amounts of data" and thousands of sites, while offering a solution that would satisfy the plaintiffs' need for evidence. The court determined that Defendants had not fully complied with its November 27, 2023 order requiring production of a complete one-day sample of non-TikTok user data and related documentation. As a result, the court ordered Defendants to produce by April 15, 2024, all raw data collected from domestic non-TikTok users on March 14, 2024, along with all documents showing how that data was processed, aggregated, combined, or reported through March 28, 2024.
Discovery on Defendant's Data Preservation Efforts	Productions on what defendants typically preserve and further discovery to assess the adequacy of preservation plans.	• In ***In Re: Tiktok, Inc., Minor Privacy Litigation***, plaintiffs argued they cannot fully assess the preservation plan without "discovery on discovery." Plaintiffs argued that they are not in a position to know what relevant data or information defendants are not currently preserving. • The "discovery on discovery" issue arose in ***In re: Google Location History Litigation*** and centered on the fundamental question of which party bore the burden and responsibility for identifying the massive volume of location data relevant to the case: Google (the defendant with possession of the data) or the individual Plaintiffs (who were asked to recreate years of movement). Google sought to compel Plaintiffs to produce location information, which Plaintiffs argued amounted to an impossible task that reversed the normal discovery flow. Plaintiffs challenged this request, arguing it was "unduly burdensome" because it would be extremely difficult, even impossible, "to recreate seven years of exact movements."

Discrimination Data	In discrimination-related cases, plaintiffs requested group membership data for the evaluation data used to evaluate bias.	• In ***Huskey v. State Farm*** plaintiffs requested this included classwide demographic and statistical data related to policyholders and claimants. State Farm's primary strategy for withholding statistical data was to establish a phased discovery schedule that explicitly excluded such materials from the initial phase.
Third-Party Data	Courts generally resisted access to third-party data. Defendants countered these requests based on arguments concerning lack of possession and/or control and privacy laws.	• In ***Mobley v. Workday*** Plaintiffs sought applicant flow data from twelve third-party companies, but Defendants argued they neither own nor have legal access to that customer information. They further contended that producing it could violate privacy laws such as the Stored Communications Act.
Use of Third-Parties for Technical Infrastructure	Plaintiffs requested information about defendants' use of third parties for technical infrastructure and design components primarily to gather evidence necessary to establish causation, demonstrate the feasibility of safer alternative designs, prove defendants' internal knowledge of risks, and define the defendants' actual control or possession of critical user data.	• In ***FTC v. Meta Platforms,*** the FTC requested documents related to Meta's operations, including materials sufficient to show Meta's "Use of third parties for infrastructure or integrity-related solutions". This information was sought by the FTC to help evaluate Meta's market power and the competitive effects of its conduct in the Personal Social Networking Services (PSNS) market. • In ***Huskey v. State Farm***, Plaintiffs resisted State Farm's motion for a protective order aimed at preventing discovery from vendors like Salesforce, Duck Creek, Eberl, Symbility, and Verisk. Plaintiffs asserted that these third parties had "direct ties to State Farm claims processing." This information was deemed relevant and appropriate to show that State Farm utilized algorithmic sorting tools supplied or supported by these vendors to flag fraud or potentially complex claims. Defendants contested plaintiffs' definition of algorithmic tool and stated that their request is beyond the first phase of discovery.

Protective Orders	Protective orders are legal tools that allow litigators to manage the handling of sensitive materials produced during discovery and to prevent their public disclosure. Defendants employ the Protective Order to justify severely restricting access, often insisting on specific security measures, such as secured, on-site computer inspection. Plaintiffs counter by filing motions to compel the production. Negotiating protective orders involves defining tiers of confidentiality, controlling access for experts and in-house counsel, and protecting highly sensitive intellectual property (IP).	• ***In re: social media adolescent addiction***: A key dispute arose over the Protective Order's adoption of Section 7.6, which mirrored the standard HCC Model Protective Order used in trade secret cases. This section required the sharing party to first identify the expert and provide basic conflict-of-interest information before sharing *Highly Confidential (Competitor)* materials, a measure specifically designed to protect against competitive harm. Plaintiffs argued this requirement was inappropriate for a mass tort products liability case, where such restrictions are less common. • In ***FTC v. Meta Platforms,*** Meta challenges the FTC's proposed protective order, arguing that it would unduly hinder Meta's ability to defend itself by prohibiting all in-house counsel from accessing materials designated by third parties as Highly Confidential. The FTC maintains that such restrictions are necessary to protect the competitively sensitive information of Meta's rivals, many of whom are third-party discovery participants. Meta contends that the restriction is unreasonable given the breadth of discovery—spanning materials from over 100 competitors and FTC investigations dating back to 2009—and notes that its own proposed order, modeled on prior FTC cases, included meaningful safeguards. After negotiations broke down, Meta largely accepted the FTC's terms but proposed two key modifications: allowing two non–decision-making in-house counsel access to Highly Confidential materials under a two-year restriction from competitive roles, and permitting four in-house counsel unrestricted access to lower-tier Confidential materials. Meta argues that these revisions are consistent with established legal practice and strike a fair balance between protecting sensitive information and ensuring a meaningful defense. • In ***Huskey v. State Farm***, Defendants filed a motion for a protective order to prevent the plaintiffs from seeking discovery from certain third parties. These third parties included technology vendors like Salesforce, Duck Creek, Eberl, Symbility, and Verisk. State Farm argued that the subpoenas violated the court's discovery phasing

		orders, as well as the relevance and proportionality requirements of Rule 26(b)(1).

B. Downstream Disputes

Discovery Area	Specific Discovery Requested	Case Examples / Outcomes
General User Dependence Data	Documents pertaining to user information and dependence data sources generally, including the data tech companies use to track and manage user engagement and reliance on the platform. Conflicts over dependence data occurred in the preservation phase, where defendants resisted broad, open-ended obligations.	• ***In re: social media adolescent addiction:*** Plaintiffs urged the Court to require preservation of all Potentially Relevant Information, including User Information, regardless of the data source, based on industry best practices. Defendants refused to discuss data sources outside a self-designated set and insisted on an "opt-in" preservation model. The Court ultimately abandoned the idea of entering a comprehensive preservation order due to the impasse. Instead, the Court issued orders requiring the use of the Plaintiff User Account Preservation Form (PPF) to facilitate preservation for relevant user accounts
Compensation to Users	Plaintiffs sought internal company data on user compensation structures. This information can reveal motives, incentives, and internal priorities that go to the heart of product liability claims. For instance, certain compensation structures can encourage platform engagement or reward behavior. In the case of antitrust suits, this information is especially helpful in defining relevant markets.	• In ***FTC v. Meta Platforms***, the FTC requested "documents sufficient to show" Meta's consideration of paying compensation to "personal networking services" (PSNS) participants, e.g. users, creators, and partners. Meta objected. • ***In re: social media adolescent addiction***: Plaintiffs sought contracts and correspondence between TikTok and specific high-profile minor influencers as well as documents regarding TikTok's general use of and compensation for influencers under the age of 18. Defendants argued that these requests were overly broad and in no way relate to the claims at issue in this litigation and invade certain privacy considerations.

Specific Privacy Data Categories	Plaintiffs requested information on how companies collected and preserved data categories, such as social data (likes/comments), biometric information (faceprints/voiceprints), Ad Targeting Profiles, data on ad clicks/purchases, and revenue earned from a user's account to uncover how user data is collected and monetized.	• In ***In Re: Clearview AI, Inc., Consumer Privacy Litigation***, plaintiffs requested URLs, Biometric Collection Dates, and Collection Reasons. Defendants stated that the app contains 8–12 billion URLs and therefore the production is highly burdensome, and relevance has not been adequately demonstrated.
Location Data	Clear definitions and documents regarding "location information" that is determined, estimated, or inferred from a user's mobile device sensors and saved to any data store under the company's control.	• ***In re: Google Location History Litigation*****:** The core argument over location data in the *Google Location History Litigation* was a dispute concerning the boundaries of user data subject to discovery.[3] Plaintiffs sought a broad definition of "location information" to ensure discovery captured all relevant data, regardless of how Google internally labeled or stored it. Plaintiffs asserted that Google's proposed narrow definition would preclude discovery of the exact data needed to assess these claims (e.g., data tracked via Web & App Activity or Wi-Fi Scanning). Google argued the plaintiffs' definition was too broad, making the discovery requests overbroad and burdensome. Initially, the court granted Plaintiffs' motion in part, adopting Plaintiffs' broader definition only for specific interrogatory requests (Interrogatories 4 and 5) and ordering Google to serve amended responses. A separate set of arguments arose when Google sought location data *from the Plaintiffs* themselves, arguing the information was necessary to their defense.

[3] Note: The dispute regarding the foundational definition of "location information" was so central to discovery proceedings that the Court later terminated a joint discovery letter brief on the issue without prejudice after the settlement was reported.

C. Other Discovery Disputes

Discovery Area	Specific Discovery Requested	Case Examples / Outcomes
Prior Regulatory Investigations	Plaintiffs sought requests for all subpoenas, civil investigative demands, or other requests for documents issued by any governmental authority (foreign, federal, or state).	• In ***In re: social media adolescent addiction***, plaintiffs requested that Meta produce all government-issued subpoenas, investigative demands, or similar requests—along with Meta's responses—related to any formal investigations into whether its platform or business practices pose risks to the health and safety of children or teens. • In, ***FTC v. Meta Platforms Inc***. Meta argued that the FTC's internal memoranda regarding their investigations into past acquisitions were not privileged, stating that the FTC waived any privilege by voluntarily sharing the documents with a third party (i.e. the House Judiciary Committee). The court disagreed.
Legal Memoranda from Prior Investigations	Counsel sought to gain insights – e.g., position statements and framing of key issues, in what ways the government allowed or disallowed certain behavior, definitions of terms, principles, markets, etc. – into prior investigations to help defend against current claims.	• In ***FTC v. Meta Platforms Inc.***, Meta asked the court to mandate that the FTC hand over eight internal memos from the FTC's past investigations into Meta's purchases of Instagram (in 2012) and WhatsApp (in 2014). The court denied this request.
Expert Witnesses	Defendants challenged plaintiffs' desire to share information with third-party experts to conduct discovery analysis.	• ***In re: Google Location History Litigation***: Plaintiffs moved for permission to disclose certain "Highly Confidential – Attorneys' Eyes Only" materials to their expert, Dr. Zubair Shafiq, a computer science professor at UC Davis. Plaintiffs sought his assistance in analyzing discovery related to how Google collects, stores, and processes user location data. Google opposed the motion, arguing that disclosure to Dr. Shafiq posed a risk of inadvertent or improper disclosure of its confidential information, despite the existing protective order. The court granted the motion, authorizing Plaintiffs to share the highly confidential materials with Dr. Shafiq under the terms of the protective order.

Data Spoliation	Data spoliation, the intentional loss or destruction of relevant evidence, specifically occurring when defendants prioritize their own interests over their legal duty to preserve information for pending or reasonably anticipated litigation. For plaintiffs, proving that spoliation has occurred as well as overcoming a Rule 37(f) challenge by defendants is difficult.[4]	• In ***Griffith v. TikTok***, plaintiffs directly sought sanctions for alleged data spoliation, which were ultimately denied. They argued that defendants continued to "delete data of non-users of TikTok after 14 days throughout the pendency of this litigation pursuant to Defendants' data retention policy." The Magistrate Judge denied the motion for sanctions. The District Judge later struck a subsequent motion for discovery sanctions, noting that the deletion of the 14-day non-user data was "not a new issue," and that plaintiffs had provided a preservation notice "well more than a year ago." The Court determined that Plaintiffs had not shown any basis for the Court to infer that the deleted data contained evidence necessary to support their claims that is materially different from the data in the sample that *had* been produced.

III. Future Topics to Explore

A. ESI Protocols

In tech litigation, the rules for handling Electronically Stored Information (ESI) is key. More work can be done to understand how ESI protocols factor into a robust discovery process and case outcomes. With mass volumes of data stored across many systems and entities, strong ESI protocols from the start of discovery ensures that critical evidence is preserved, collected, and produced.

B. Forensic Inspection Protocols

Forensic inspection protocols are formal procedures that govern the collection, preservation, and examination of electronic devices and digital data to ensure the process is accurate, reliable, and legally defensible. These protocols specify how data will be accessed, imaged, and analyzed, often by a neutral third-party expert, while protecting the integrity of the devices

[4] FRCP Rule 37(f) is a safe harbor that provides, in pertinent part: "[a]bsent exceptional circumstances, a court may not impose sanctions ... on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

and the privacy of the individuals involved. The goal is to prevent spoliation or inadvertent alteration or deletion of evidence and to establish a clear chain of custody that can withstand scrutiny in court. For instance, in the context of the Bellwether litigation in ***In re: social media adolescent addiction***, Defendants served RFPs seeking access to electronic devices used by plaintiffs to access social media platforms during the relevant period. They proposed obtaining forensic images or clones of the devices, along with documents reflecting usage data and device identifiers. To govern this process, Defendants provided a proposed inspection protocol, modeled after one approved by Judge Gonzalez Rogers in *eHealthinsurance Svcs., Inc. v. Healthpilot Techs. LLC*, 2021 WL 3052918 (N.D. Cal. July 20, 2021) outlining how a neutral third party would conduct the examination in a controlled and standardized manner.

C. Special Considerations for Large-Scale Litigation

Future research should examine procedural dynamics that shape large-scale and coordinated tech litigation. In particular, areas for deeper analysis include technical aspects of Bellwether testing within Judicial Council Coordinated Proceedings (JCCP), which can provide insight into how representative cases influence discovery and settlement trajectories; the distinctive features of Multidistrict Litigation (MDL) generally as they relate to coordination across jurisdictions, management of shared discovery, and the treatment of common versus individualized issues; and case management practices, including judicial approaches to scheduling, consolidation, phasing of discovery, and the resolution of discovery disputes.

D. International Discovery

Future research in this area should include delving into the discovery processes of key litigation in international jurisdictions including the E.U., U.K., Canada, and Australia. Studying the trajectory of other discovery processes is critical to understanding the opportunities and limitations of discovery in the U.S. It can provide a lens into how companies are able to preserve and share evidence in countries with more robust regulation, and best practices for improving efficiency, reducing discovery costs, and opposing objections to discovery requests. Future research should also examine the opportunities presented by 28 U.S.C. section 1782, a mechanism in US law that allows for domestic discovery proceedings to be initiated against US companies to support foreign lawsuits, investigations, and proceedings against those same companies.

APPENDIX: LIST OF CASES ANALYZED

Social Media

- *In re: social media adolescent addiction* (4:22-md-03047-YGR, MDL No. 3047)

Civil Rights

- *Huskey v. State Farm Fire & Casualty Company* (1:22-cv-07014)
- *Mobley v. Workday, Inc.* (3:23-cv-00770)

Gambling

- *Soucek v. Roblox Corporation* (3:23-cv-04146)

Gaming

- *Murphy et. al. v. Roblox* (3:23-cv-01940)

Privacy

- *Griffith v. TikTok, Inc. et al.* (5:2023-cv-00964)
- *In Re: Tiktok, Inc., Minor Privacy Litigation* (2:25-ml-03144)
- *In re: Google Location History Litigation* (5:18-cv-05062)
- *Robert Weissman v. Clearview AI, Inc.* (25-1673)

Public Health

- *In re Juul Labs, Inc., Mktg., Sales Prac. & Prods. Liab. Litig* (3:19-md-02913)