KEKER VAN NEST & PETERS

Navigating the Privacy Minefield:
Litigation Trends and Case Strategy

January 18, 2023

Presenters

Ben Berkowitz

bberkowitz@keker.com

Tom Gorman

tgorman@keker.com

Christina Lee

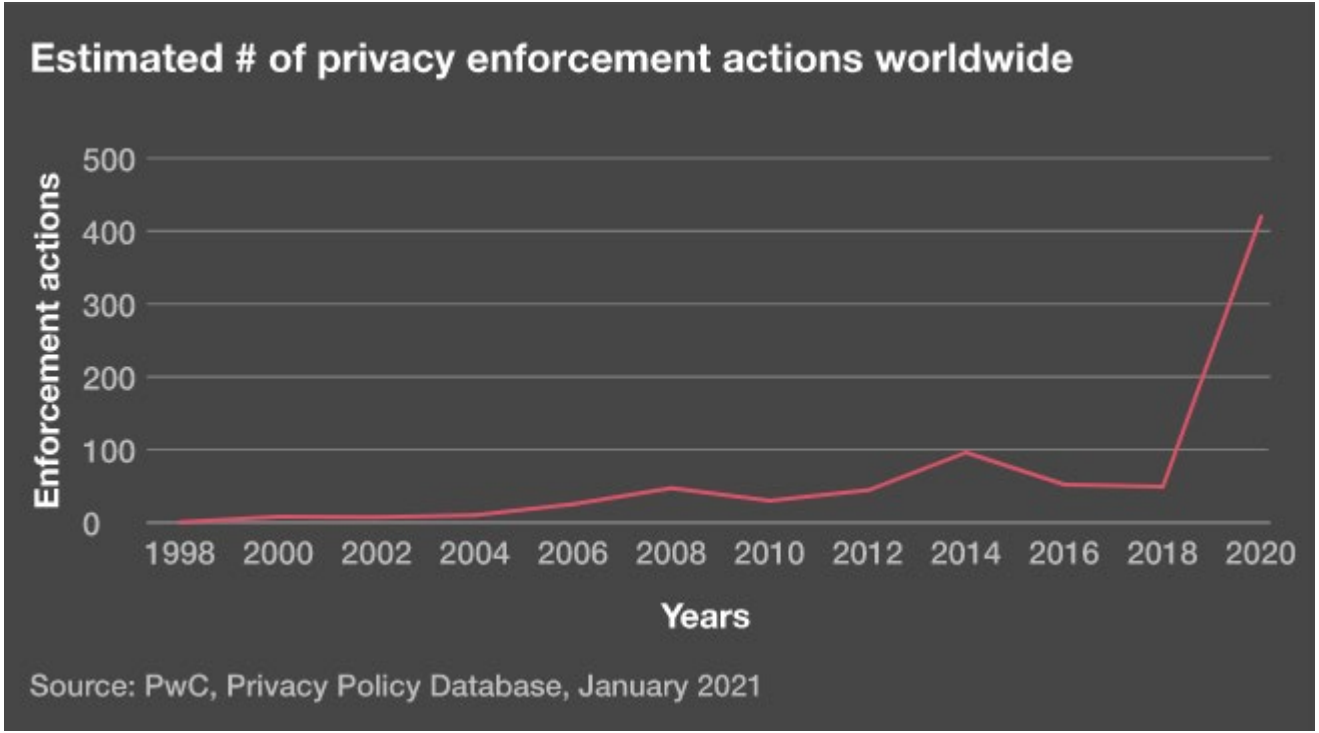
clee@keker.com

Agenda

- **Privacy Litigation Trend: Big Data in the Crosshairs**
- **Overview of Claims Asserted**
- **Key Defenses & Practical Takeaways**
- **Litigation Strategy**

Privacy Litigation Trends

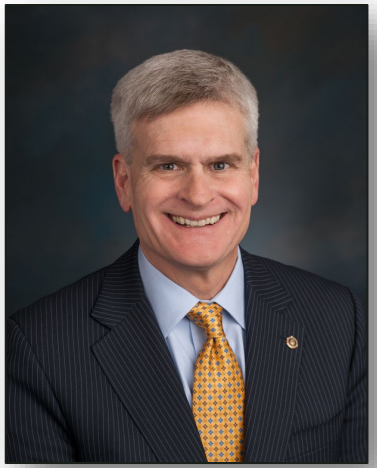
Litigation Trend: Increasing Enforcement



Source: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/seven-privacy-megatrends/rise-privacy-enforcement.html

Bipartisan Scrutiny of “Big Tech”

“[T]ech firms collect and exploit sensitive personal information -- often threatening national security, harming our emotional health, and discriminating against vulnerable groups.”



“We should have a conversation about what data is appropriate to collect, what limits should be placed on the groups that data is collected on, and restrictions on how that data is sold or transferred to other parties.”

Big Data in the Crosshairs

Rise in suits targeting Big Tech

- **Increased litigation targeting not only data *breaches*, but also *collection* and *use* of personally identifying information**

Notable Recent Class Action Settlements

- *In re: Facebook, Inc. Consumer Privacy User Profile Litigation* (N.D. Cal.) - $725m
  - Allegations of granting third parties access to user content and PII without consent
- *In re: T-Mobile Customer Data Security Breach Litigation* (W.D. Mo.) - $350m
  - Allegations of failure to adequately protect consumers' PII from data breach
- *In re: Tiktok Consumer Privacy Litigation* (N.D. Ill.) - $92m
  - Allegations of surreptitious harvesting and profiting from biometric data, geolocation information, other PII, and unpublished digital recordings
- *In re: Zoom Privacy Litigation* (N.D. Cal.) - $85m
  - Allegations of sharing PII with third parties without permission, misrepresenting encryption protocol, failure to prevent "Zoombombing"

Notable Recent Public Settlements

- Google agreed to a $391.5 million settlement with 40 states in 2022.
  - Allegations relating to the collection of location information
- The FTC imposed a $150 million civil penalty on Twitter in 2022.
  - Allegations of the use of account security data for targeted advertising to users
- Equifax agreed to pay at least $575 million as part of a settlement with the FTC, the CFPB, and 50 states in 2019.
  - Allegations arising out of a data breach
- The FTC imposed a $5 billion civil penalty on Facebook in 2019.
  - Allegations of sharing user information with third parties without consent

Big Data in the Crosshairs

- **Increased litigation targeting not only how data is collected, but also how data is *used***
- **Examples:**
  - Location information
  - Browsing activity
  - “Cookie” tracking
  - App-usage data
  - Biometric data

In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020)

- **Privacy class action alleging:**
  - *Collection*: using cookies to track users' browsing histories when they visited third-party sites after they had logged out of the platform
  - *Use*: compiling information into personal profiles sold to advertisers
- **Asserted claims:**
  - Wiretap Act, Stored Communications Act (SCA), California statutes (California Invasion of Privacy Act; Computer Data Access and Fraud Act), and California common-law claims

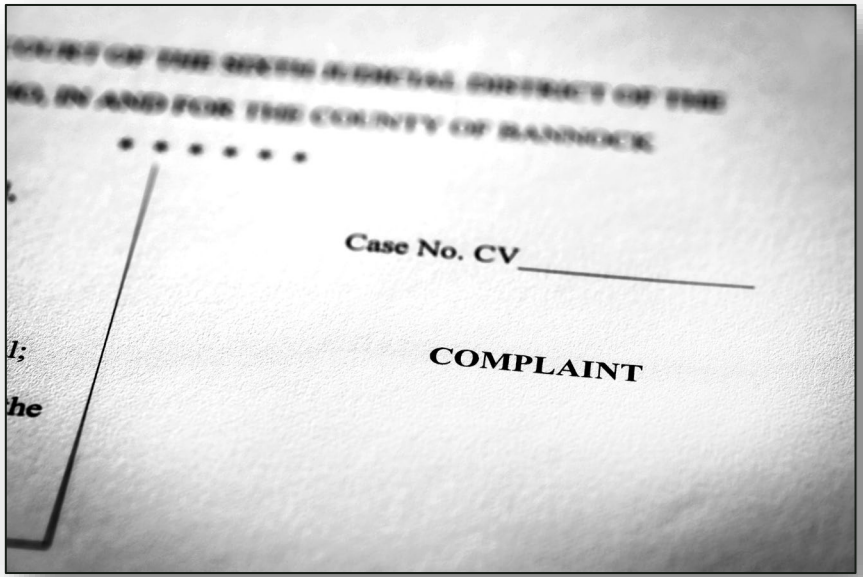
In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020)

- **Ninth Circuit reversed dismissal on 12(b) grounds**
  - *Nature of collection*:
    - Concluded that plaintiffs plausibly pleaded that a Help Center page "set an expectation that logged-out user data would not be collected," when it was in fact "collected…anyway"
  - *Sensitivity of the collected information*
    - Found that "the amount of data allegedly collected was significant," as was the use of an "enormous amount of individualized data" to "compile highly personalized profiles"
- **Post-*In re Facebook*, plaintiffs are increasingly asserting claims based on compilation of data.**

The Anatomy of a Privacy Class Action

The Anatomy of a Privacy Class Action

- **Common Causes of Action**
- **Key Defenses**
- **Class Certification**
- **Summary Judgment**



Common Causes of Action

Common Causes of Action

- **Common-Law Privacy Claims**
  - Intrusion Upon Seclusion, California Constitutional Right to Privacy
- **Statutory Privacy and Wiretapping Claims**
  - Wiretap Act, Stored Communications Act, & Computer Fraud and Abuse Act
  - California Invasion of Privacy Act (CIPA) and Consumer Privacy Act (CCPA)
- **Consumer Claims**
  - Unfair Competition Law, Consumers Legal Remedies Act, Common-Law Fraud, Breach of Contract, Unjust Enrichment

Types of Claims Asserted

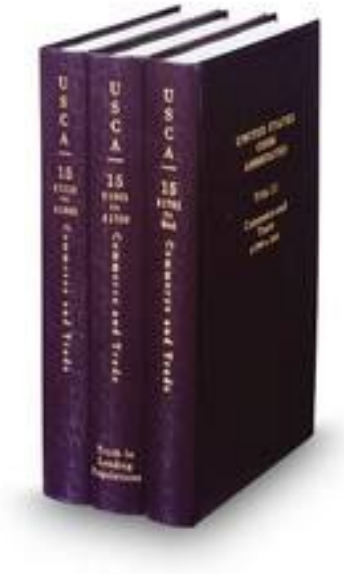
- **Common-law privacy claims:**
  - Intrusion upon seclusion / invasion of privacy
  - California Constitutional Right to Privacy
    - Article I, Section 1 of the California Constitution: "All people are by nature free and independent and have inalienable rights. Among these are…**privacy**."
  - Elements
    - Legally protected privacy interest
    - Reasonable expectation of privacy in the circumstances
    - Egregious breach of social norms / highly offensive to a reasonable person

Types of Claims Asserted

- **Common-law privacy claims:**
  - "The California Constitution sets a '**high bar**' for establishing an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014).
    - Plaintiffs must allege "*with specificity*" the data at issue to establish a legally protected privacy interest—*e.g.*, "the specific content in the emails at issue."
    - *But see In re Facebook*, 956 F.3d at 603 : The Ninth Circuit rejected the argument that plaintiffs "needed to identify specific, sensitive information" in light of the nature and sensitivity of the data collected.

Types of Claims Asserted

- **Statutory claims**
  - California Invasion of Privacy Act
  - California Consumer Privacy Act
  - Wiretap Act
  - Stored Communications Act
  - Computer Fraud and Abuse Act



Claim Spotlight: California Invasion of Privacy Act

- **CIPA is a criminal statute that provides for civil penalties.**
  - $5000 statutory damage penalty *per violation*.
- **CIPA is decades-old and addressed older wiretapping, eavesdropping, and surveillance technologies.**
  - The core provisions were enacted in 1967, with additional provisions added over time.
- **Plaintiffs have attempted to wield CIPA in privacy litigation addressing new technologies.**

Claim Spotlight: California Invasion of Privacy Act

- **CIPA claims alleging wiretapping:**
  - CIPA is California's state-law analogue to the federal Wiretap Act.
  - California Penal Code § 631 punishes a person who, "willfully and without the consent of all parties to the communication," attempts to read or learn "the **contents** or meaning of any message, report, or communication" in transit over a wire.
    - A CIPA claim requires the interception of the "contents" of an electronic communication.
    - "Record information" (*e.g.*, the origination, length, and time of a phone call) associated with the communication is unactionable.

Claim Spotlight: California Invasion of Privacy Act

- ***McCoy v. Google* (N.D. Cal.):**
  - Plaintiff asserted that the defendant violated § 631 by collecting data about how often and for how long he used third-party apps.
- **The court dismissed plaintiff's CIPA claim because it was premised on the alleged collection of "record information."**
  - Data on when and how often a smartphone user opens and runs third-party apps, and the length of time spent on the apps, amounted to "record information."
  - Plaintiff failed to allege the interception of the "contents" of any communication.

Claim Spotlight: California Invasion of Privacy Act

- ***Hammerling v. Google* (N.D. Cal.):**
  - Plaintiffs asserted that the defendant violated § 631 by collecting data about their activity on third-party apps.
- **The court dismissed plaintiffs' CIPA claim because it failed to allege that the defendant intercepted contents while "in transit" and within the state of California.**
  - Plaintiffs' allegations that the defendant collected "real-time data" were insufficient to plausibly allege interception of that data.
  - Plaintiffs failed to allege that the data was intercepted "within th[e] state" of California, as required by the statute.

Claim Spotlight: California Invasion of Privacy Act

- **CIPA claims targeting collection of geolocation information:**
  - California Penal Code § 637.7 prohibits "us[ing] an electronic tracking device to determine the location or movement of a person."
  - An "electronic tracking device" is defined as "any device attached to a vehicle or other movable thing that reveals its location by the transmission of electronic signals."

Claim Spotlight: California Invasion of Privacy Act

- ***In re Google Location History Litigation* (N.D. Cal.):**
  - Plaintiffs asserted § 637.7 claim, alleging that the defendant used their mobile devices to determine their location.
- **The court dismissed plaintiffs' CIPA claim under a plain-language reading of the statute.**
  - The defendant's *software* services did not constitute a "device." Nor did the hardware components of plaintiffs' phones, which could not track location on their own.
  - Plaintiffs failed to plead that an "electronic tracking device" was "attached" to a "vehicle or other movable thing."

Types of Claims Asserted

- **Consumer claims**
  - Fraud
  - Unfair Competition Law
  - Consumers Legal Remedies Act
  - Breach of contract
  - Quasi-contract (*e.g.*, breach of implied contract; unjust enrichment)

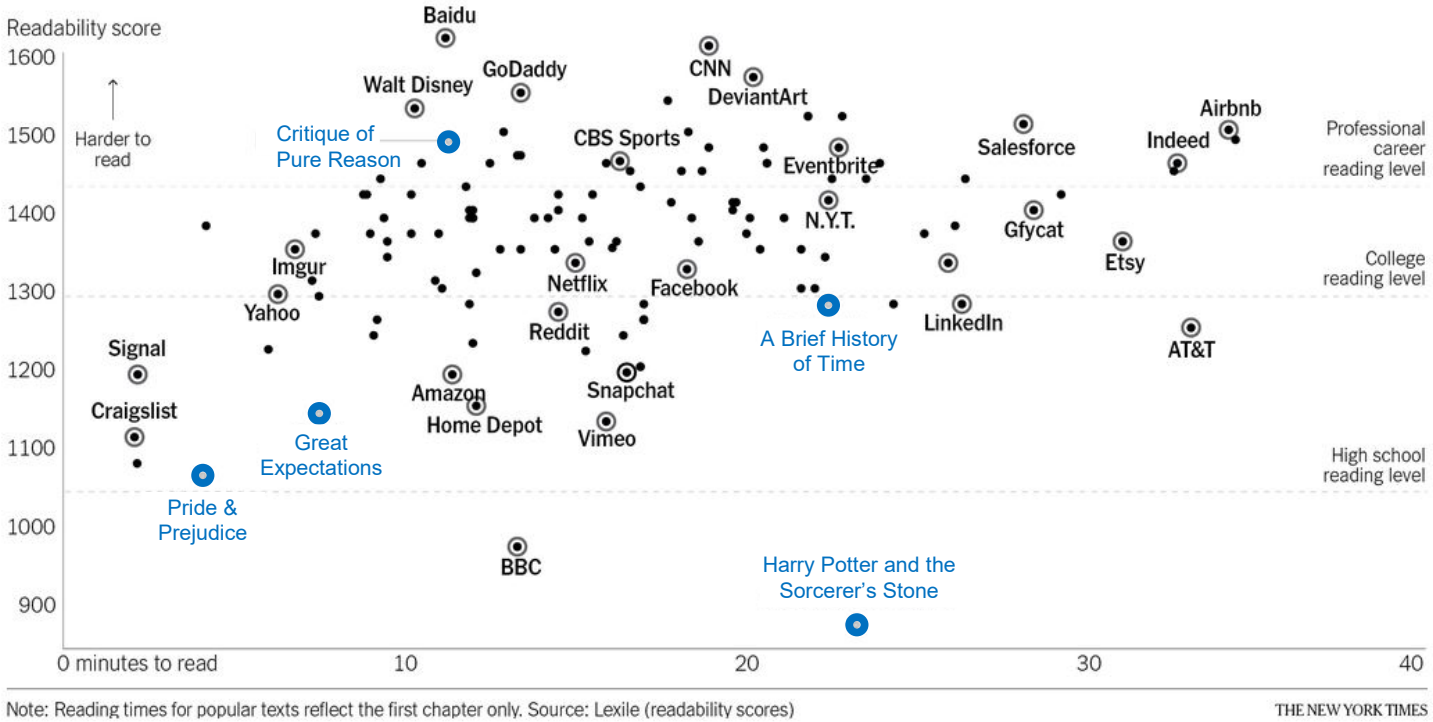
Key Defenses & Practical Takeaways

Terms of Service & Privacy Policies

Front line of defense

- **Relevant to consent and disclosure-based defenses**
- **Disclosures can be used to defeat elements of common claims (*e.g.*, expectation of privacy, reliance) at the pleadings stage and at class certification**
  - *E.g.*, *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014) (declining to certify class alleging Wiretap Act violations because of the "panoply of sources from which email users could have learned of," and thus impliedly consented to, the alleged interceptions)
- **Online contract formation**
- **Broad and clear disclosures in plain English are the most defensible**

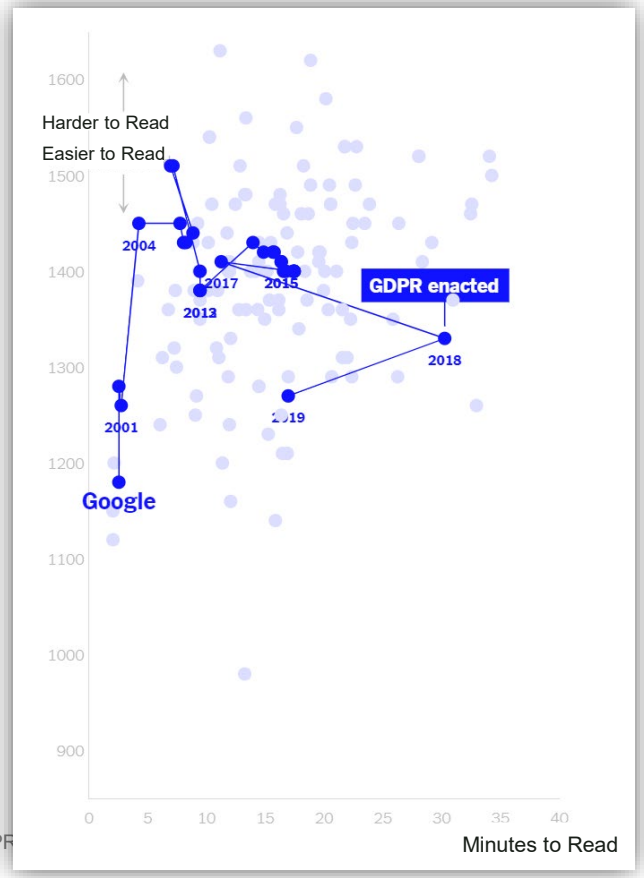
Terms of Service & Privacy Policies



"We Read 150 Privacy Policies. They Were an Incomprehensible Disaster."

--Kevin Litman-Navarro, *The New York Times*

Terms of Service & Privacy Policies



2010:

- **Location data** – Google offers location-enabled services, such as Google Maps and Latitude. If you use those services, Google may receive information about your actual location (such as GPS signals sent by a mobile device) or information that can be used to approximate a location (such as a cell ID).

2019:

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you.

Your location can be determined with varying degrees of accuracy by:

- GPS
- IP address
- Sensor data from your device
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices.

Terms of Service & Privacy Policies

A word of caution:

- **Courts have increasingly looked at statements made *outside of* Terms of Service and Privacy Policies that might give rise to a reasonable expectation of privacy**
  - Ads
  - Device pop-ups
  - Help center / support pages
    - *See, e.g.*, *In re Facebook*, 956 F.3d at 602 (finding that a Help Center page created an expectation of privacy)

Article III Standing

***TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021)**

- Follows *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016), which held that procedural violations of the Fair Credit Reporting Act, without concrete harm, cannot satisfy the injury-in-fact requirement of Article III.
- Plaintiffs must establish a material risk of future harm.
  - Misleading information in a consumer's credit file, standing alone, is not a concrete harm.
  - Plaintiffs must demonstrate, for example, a "sufficient likelihood" that the inaccurate information would be given to third parties.

Article III Standing

- Courts have been resistant to *Spokeo*-type standing arguments in the context of traditional privacy claims.
  - *Transunion* recognized "**disclosure of private information**" and "**intrusion upon seclusion**" as "intangible harms" that have been "traditionally recognized as providing a basis for lawsuits in American courts." 141 S. Ct. at 2204 (2021).
- But under the right circumstances, courts may be receptive to Article III-standing arguments.
  - *See, e.g.*, *Abdulaziz v. Twitter, Inc.*, No. 19-CV-06694-LB, 2020 WL 6947929 (N.D. Cal. Aug. 12, 2020)

Litigation Strategy

Litigation Strategy: Pleadings Stage

- **Common Rule 12(b) arguments**
  - Article III standing
  - Failure to plead sufficient details regarding the PII at issue
    - *See In re Yahoo Mail Litig.* (N.D. Cal.) (failure to plead details of emails)
  - Failure to plead required statutory elements (*e.g.*, CIPA)
    - *See In re Google Location History* (N.D. Cal.) (no "electronic tracking device")
  - Consent / Disclosure
    - Courts increasingly resistant to consent defenses at the pleadings stage
    - Alternative framing: disclosures can be used to defeat elements of common claims (*e.g.*, expectation of privacy, reliance)

Litigation Strategy: Compelling Individual Arbitration

- **Enforcing Contractual Arbitration Rights**
  - Strong procedural defense to class actions
  - BUT: Mass arbitration filings are an increasing threat
- **No Arbitration Agreement?**
  - Consider third-party agreements
  - *See, e.g.*, *Arellano v. T-Mobile USA, Inc.*, 2011 WL 1362165 (N.D. Cal. 2011)

Litigation Strategy: Key Witnesses

- **Identify Key Corporate Witnesses**
  - Who will be the Company spokesperson?
  - Explain the Company's privacy and cybersecurity policies
  - Explain the data collected, why and how it was used, and (in the case of breach) what steps were taken to safeguard it
- **Identify Experts**
  - Industry standards
  - Key technology / data architecture
  - Consumer behavior
  - Increasing use of surveys by both plaintiffs and defendants

Litigation Strategy: the Named Plaintiffs

- **Taking Discovery**
  - Conduct discovery with class certification and summary judgment in mind
    - Did the Company actually collect data from the Named Plaintiffs? Not always!
    - Did the Named Plaintiffs consent to the collection / use of their data?
    - Are the Named Plaintiffs situated differently than other Class Members?
      - *e.g.*, did the Named Plaintiffs choose to share the same data with other third-parties?
    - Take Named Plaintiff discovery early, and plan ahead for potential third-party discovery

Litigation Strategy: Class Certification

- **Variations in consent and disclosures**
  - Variations in disclosures that class members were exposed to can establish that reasonable expectation of privacy and consent are not susceptible to class-wide proof.
  - *In re Google Assistant Privacy Litigation* (N.D. Cal.):
    - "[C]ourts in this Circuit have denied class certification in cases involving claims for which reasonable expectation of privacy is a necessary element because 'the individual nature of the objective expectations inquiry' raised issues that defeated commonality or predominance."

Litigation Strategy: Class Certification

- **Marshal evidence demonstrating that the class actually saw the relevant disclosures.**
  - Courts have certified a class over objections that class members were exposed to different disclosures, in the absence of sufficient information that class members actually saw the disclosures. *See Campbell v. Facebook Inc.*, 315 F.R.D. 250, 266–67 (N.D. Cal. 2016).
- **Establish that the amount and nature of the data collected from class members varied.**
  - Under *In re Facebook*, the amount and nature of the data collected inform whether plaintiffs have a reasonable expectation of privacy.

Litigation Strategy: Summary Judgment

- **Summary judgment issues vary widely across cases and across named plaintiffs.**
- **Consider whether to bring a summary judgment motion before or after class certification**
  - Pros: early win on all or subset of claims
  - Cons: early summary judgment binds only the named plaintiffs, not the class
  - Defeating a weaker Named Plaintiff on summary judgment may only invite amendment prior to class certification.

Questions?

Thank you