

Navigating the Privacy Minefield: Litigation Trends and Case Strategy

May 22, 2024



Presenters



Ben Berkowitz

Partner

Keker, Van Nest & Peters

bberkowitz@keker.com



Danielle Pierre

Litigation Counsel

Google

daniellepierre@google.com



Tom Gorman

Partner

Keker, Van Nest & Peters

tgorman@keker.com



Christina Lee

Partner

Keker, Van Nest & Peters

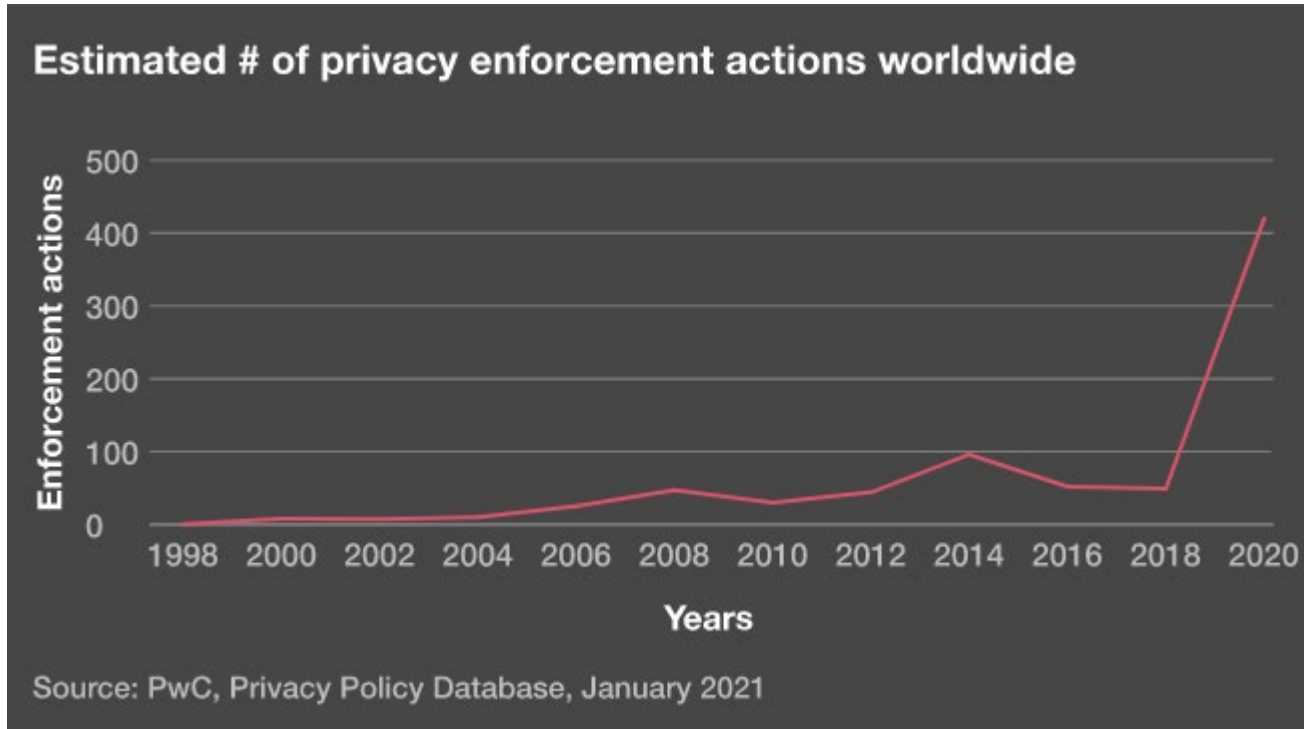
clee@keker.com

Agenda

- **U.S. Privacy Litigation Trends**
- **Overview of Claims Asserted: U.S. and California**
- **Key Defenses & Practical Takeaways**

U.S. Privacy Litigation Trends

U.S. Litigation Trend: Increasing Enforcement



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

Congressional Scrutiny of “Big Tech”

Innovation, Data, and Commerce Subcommittee Hearing: “Promoting U.S. innovation and Individual Liberty through a National Standard for Data Privacy” (March 1, 2023)



Cathy McMorris Rodgers (R-WA), House Energy and Commerce Committee Chair

“Americans have no say over whether and where their personal data is sold and shared, they have no guaranteed way to access, delete, or correct their data, and they have no ability to stop the unchecked collection of their sensitive personal information.”

“This isn’t acceptable. Data brokers and Big Tech’s days of operating in the dark should be over.”

“People should trust their data is being protected.”

Bipartisan Scrutiny of “Big Tech”



“For too long, giant tech companies have exploited consumers’ data, invaded Americans’ privacy, threatened our national security, and stomped out competition in our economy.”



“For years I have been trying to find ways to empower consumers against Big Tech. I have heard too many stories from families who feel helpless in the face of Big Tech. Stories about children being bullied to the point of committing suicide. Human trafficking. Exploitation of minors. All the while the social media platforms look the other way. ”

Proposed “American Privacy Rights Act of 2024”

- Bipartisan and bicameral draft legislation announced on April 7, 2024 by Senator Cantwell (D-WA) and Congresswoman McMorris Rodgers (R-WA)
- Aims to establish a national privacy standard at the federal level
- Provides a private right of action for violations of data privacy rights under the proposed Act; also enforceable by the FTC and State attorneys general
- Prevents companies from enforcing mandatory arbitration in cases of substantial privacy harm
- Expressly sets “data minimization” limitations on how companies can use consumer data

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



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
 - AI privacy suits



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
- *United States v. Epic Games, Inc.* (E.D. N.C.) - \$520m
 - Allegations of collecting PII from minors without parental consent in violation of the Children's Online Privacy Protection Act (COPPA)
- *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. Capital One Consumer Data Security Breach Litigation* (E.D. Va.) - \$190m
 - Allegations of failure to adequately protect consumers' PII from data breach

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
- **Post-*In re Facebook*, plaintiffs are increasingly asserting claims based on compilation of data.**

Recent Privacy Cases in the Ninth Circuit



- **The Ninth Circuit recently heard 5 privacy cases in one day in February 2024:**
 - *Hammerling v. Google, LLC* (22-17024) – Allegations that Google secretly used plaintiffs’ Android smartphones to collect data regarding their use of third-party apps
 - *Taylor v. Google, LLC* (22-16654) – Allegations of “passive” data transfers performed by Google over its Android OS
 - *Greenstein v. Noblr Reciprocal Exchange* (22-17023) – Allegations of ongoing threat of identify theft and fraud following cyberattack
 - *Baptiste v. Apple, Inc.* (2315392) – Allegations that Apple retained PII collected in connection with video streaming rentals on iTunes
 - *Minahan v. Google, LLC* (23-15775) – Allegations that Google violated NY and MN privacy statutes by retaining user’s video rental history data

Dark Patterns



Dark Patterns

What are dark patterns?

California Civil Code:

“[A] user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice...” Cal. Civ. Code 1798.140(I).

Other useful definitions:

“User interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions” (Mathur 2019 (Princeton University Study))


Dark Patterns

Fake countdown timers



Dark Patterns

Misdirection

*** Phone** 

*** Email**

We'd love to send you emails with offers and new products from New Balance Athletics, Inc. but if you do not wish to receive these updates, please tick this box. [View Privacy Policy.](#)

Please select **Yes** below if you are happy to receive email notifications of **exclusive member offers** from M8 Group companies. You will always have the option to unsubscribe from any emails you decide you would rather not receive.

YES

I do want to hear about exclusive offers & discounts

NO

I'd rather NOT hear about exclusive offers & discounts

Don't worry, we will never sell or rent your personal information, it's part of our [privacy policy](#). Also, you can update your preferences and unsubscribe from 'My Account' at any time.

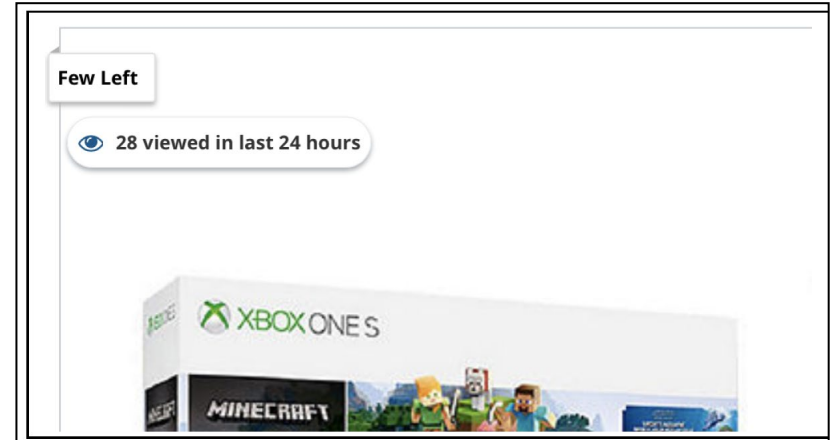
Dark Patterns

Obscured renewing subscription

<p>Shipping Rates</p> <p><input type="checkbox"/> Enjoy FREE shipping with WSJwine Advantage</p> <p>Learn More</p> <p>Add to Cart</p> <p>Item No. M09559</p>	<p>Item Description</p> <hr/> <p>Luscious Chardonnay ADD-ON Item #: M09559 - 12 btls</p> <hr/> <p>WSJwine 1 Year Advantage Delivery Membership Item #: 15245UL</p> <hr/>
---	---

Dark Patterns

- **Fake activity messages**
- **Messages indicating low stock or high demand**
- **Obstruction—making sign up easy and cancellation hard**



Dark Patterns



Commissioner Christine S. Wilson



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

“[D]ark patterns that violate the law rightly constitute a priority for the agency.” (September 15, 2022)

Dark Patterns



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

FTC enforcement action against Age of Learning, Inc.

- ABCmouse misrepresented its cancellation terms
- Made it difficult for consumers to cancel their memberships
- \$10 million paid to settle

Special Offer
38% OFF
Annual Membership!

\$59⁹⁵ for 12 Months

Payment Option
4 equal monthly installments of \$19⁷⁵
(Save 17%)

Is this a gift? [Click Here](#)

In a recent study surveying more than **5,000 parents** who use ABCmouse.com with their children, over **85%** reported a significant **positive impact** on their children's learning.

Award-Winning Curriculum!

Easy Enrollment!

1 Create Your Family Account

Email

Confirm Email

Password

Confirm Password

2 Enter Your Payment Information

VISA MASTERCARD PAYPAL Pay with Amazon

Cardholder Name

Credit Card Number

Expiration Date MM / YYYY CVV [\(What's This?\)](#)

Billing Zip/Postal Code
(@International Cards, please enter 12345)

Phone Number
(Optional, but recommended)

Easy Cancellation
If your family does not absolutely love ABCmouse, you can cancel at any time.
🔒 Your information is safe and protected.

3 I agree to the [Terms & Conditions](#)

Submit

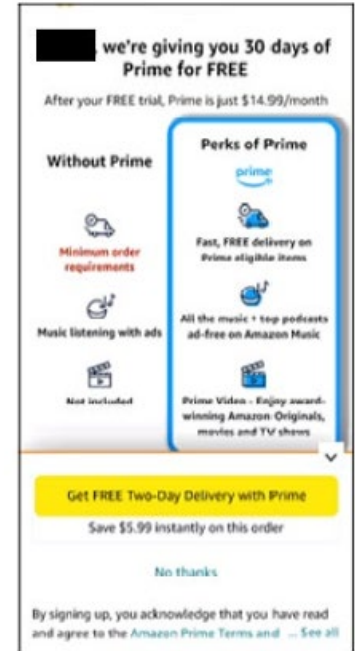
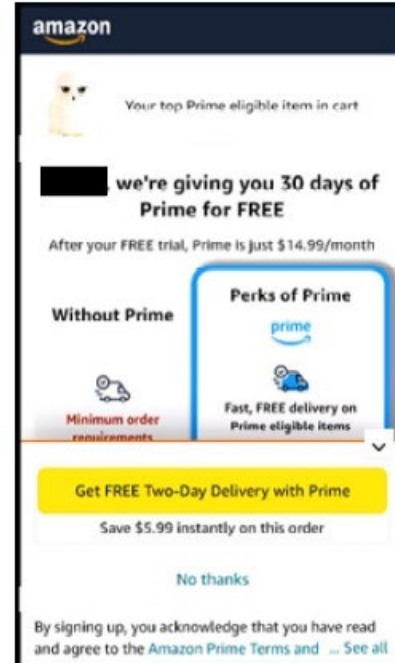
Dark Patterns



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

FTC enforcement action against Amazon.com, Inc.

- Complaint filed on June 21, 2023 in the Western District of Washington
- Allegations that Amazon enrolled consumers into its Prime program without their consent and made it difficult for them to cancel their subscriptions



Dark Patterns

Cal. Consumer Privacy Act (CCPA) regulations (Cal. Code Regs. Tit 11, Div. 1, Chp. 20, Section 999.315(h))

Ban the use of dark patterns to subvert or impair the process for consumers to opt out of the sale of personal information

Cal. Privacy Rights Act (effective January 1, 2023)

Agreement “obtained through use of dark patterns does not constitute consent” Cal. Civ. Code 1798.140(h)



Common Causes of Action: U.S. and California

Common Causes of Action: U.S. and California

- **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, Consumer Legal Remedies Act, Common-Law Fraud, Breach of Contract, Unjust Enrichment

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:**
 - Cal. 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.

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.”**
- ***Hammerling v. Google* (N.D. Cal.; affirmed by Ninth Circuit):**
 - 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 CA. The Ninth Circuit affirmed on disclosure grounds.**

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."

Claim Spotlight: California Invasion of Privacy Act

- **CIPA claims targeting eavesdropping:**
 - California Penal Code § 632(a) prohibits “us[ing] an amplifying or recording device to eavesdrop upon or record [a] confidential communication.”
 - The statute does not define “amplifying or recording device,” except to say it does not apply to devices of public utilities engaged in the business of providing communications services and facilitates, telephones in correctional facilities, or hearing aids.



Claim Spotlight: California Invasion of Privacy Act

- ***In re. Meta Pixel Healthcare Litigation* (N.D. Cal.):**
- Plaintiffs asserted § 632(a) claim, alleging that the defendant used their proprietary computer code to obtain healthcare-related information of Facebook users.
- The Court did not dismiss plaintiffs' CIPA claim, holding that the Pixel software is an "amplifying and recording device" under section 632(a).
- However, the Court dismissed the plaintiffs' constitutional privacy and unfair competition claims because they did not "identify any particular categories of information that they shared with their healthcare providers that they reasonably believe was captured by Meta."

Claim Spotlight: Increased AG Enforcement Post-CCPA

People v. Sephora (SF Superior):

- AG enforcement sweep: Allegations that Sephora sold customers' personal information without proper notice, and that after customers opted out via user-enabled global privacy controls, Sephora continued to sell their information.
- \$1.2 million penalty, revise privacy policy and opt out, provide regular reporting to AG.



People v. DoorDash (SF Superior):

- Via marketing cooperative, allegations that DoorDash sold customers' personal information without providing notice or opt out, in violation of both CCPA and CalOPPA.
- \$375,000 civil penalty, remedy marketing practices, and annual reporting to AG.



Key Defenses & Practical Takeaways

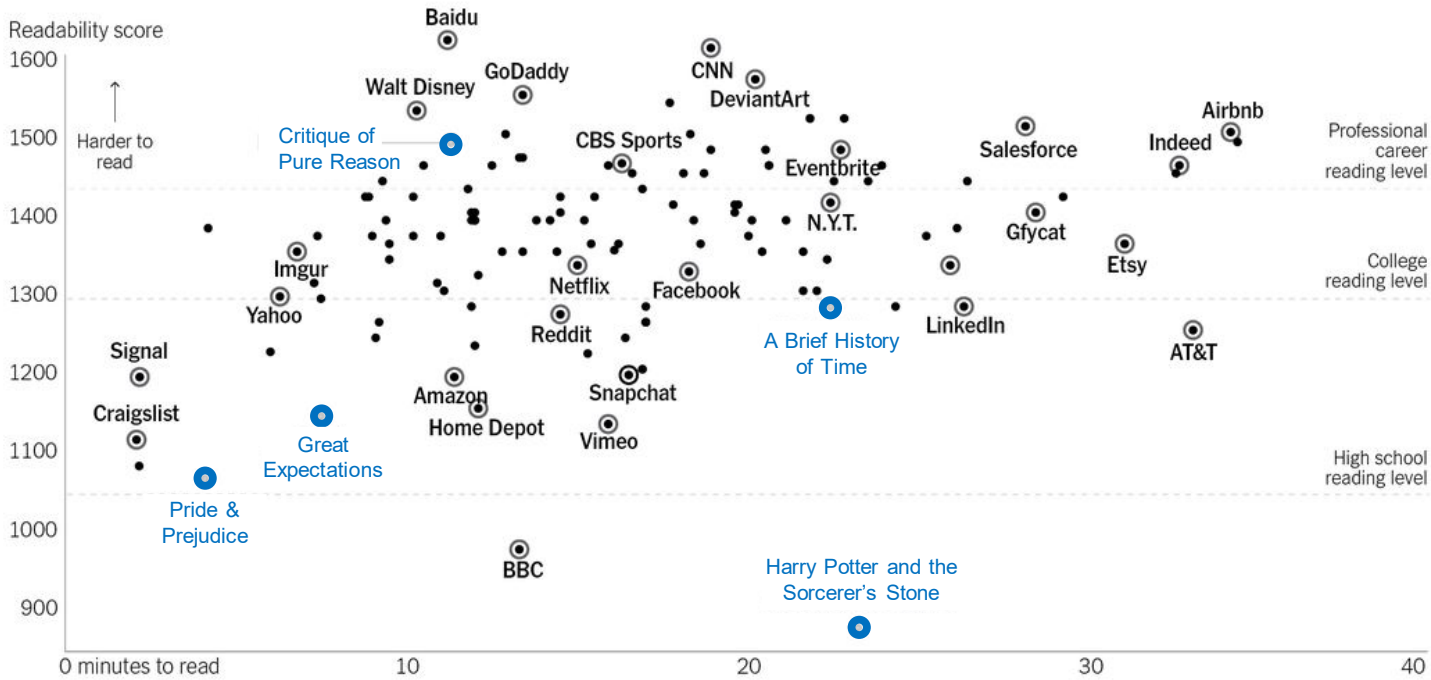
Terms of Service & Privacy Policies

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)
- **Broad and clear disclosures in plain English are the most defensible**
- **Online contract formation**



Terms of Service & Privacy Policies



Note: Reading times for popular texts reflect the first chapter only. Source: Lexile (readability scores)

THE NEW YORK TIMES

***“We Read 150
Privacy Policies.
They Were an
Incomprehensible
Disaster.”***

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

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.
- 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).
 - ***Sanchez v. L.A. Department of Transportation*** (9th Cir. 2022) – City’s collection of scooters’ real-time location data amounted to injury-in-fact sufficient to confer standing

Article III Standing

- But under the right circumstances, courts may be receptive.
 - ***Phillips v. U.S. Customs and Border Protection*** (9th Cir. 2023)
 - CBP’s unlawful collection and retention of migrants’ records alone does not constitute injury-in-fact sufficient to confer standing
 - ***Abdulaziz v. Twitter, Inc.***, (9th Cir., argued and submitted Dec. 4, 2023)
 - The defendant argues that the plaintiff did not plausibly allege that the Kingdom of Saudi Arabia’s breach of Twitter’s security in 2014 and 2015 caused his persecution and harassment by the KSA
 - Unlike in *In re Zappos.com, Inc.*, the plaintiff did not pursue claims based on a present risk of future identity theft.

Questions?

Presenters



Ben Berkowitz is an experienced trial and appellate lawyer who has a track record of winning cases for major technology companies in high-profile litigation. He has served as lead counsel for Google in multiple nationwide class action matters: In *Hammerling v. Google*, *McCoy v. Google*, and *Lundy v. Google*, he defeated a series of nationwide privacy class actions regarding Google's Android operating system. In *In re Google Location History Litigation*, he leads Google's defense of a consolidated set of nationwide privacy class actions on behalf of all Android and Apple mobile device users.



Danielle Pierre is Litigation Counsel at Google where she fights strategically to favorably resolve litigation matters and advises on legal issues, including privacy. Before joining Google, Danielle was an associate at a large law firm with a practice emphasis on privacy and consumer class actions.



Tom Gorman's practice focuses on high-stakes litigation for a variety of technology clients, including Google, Waymo, Lyft, Kitty Hawk, and Taiwan Semiconductor Manufacturing Company. He is representing Google in multiple nationwide privacy class actions regarding its Android operating system, including *In re Google Location History Litigation* and *McCoy v. Google*. For several years Tom has successfully defended challenges to Major League Baseball's exemption to U.S. antitrust laws.



Christina Lee represents plaintiffs and defendants in high-stakes civil litigation matters, including complex privacy cases. She has successfully represented Google in multiple putative class action lawsuits asserting privacy, contract, and consumer law claims regarding Google's alleged data collection practices, in each case obtaining dismissals of entire complaints or critical claims.