KEKER
VAN NEST
& PETERS

Navigating the Privacy Minefield: Litigation Trends and Case Strategy

May 21, 2025

Presenters

Ben Berkowitz
bberkowitz@keker.com

Christina Lee
clee@keker.com

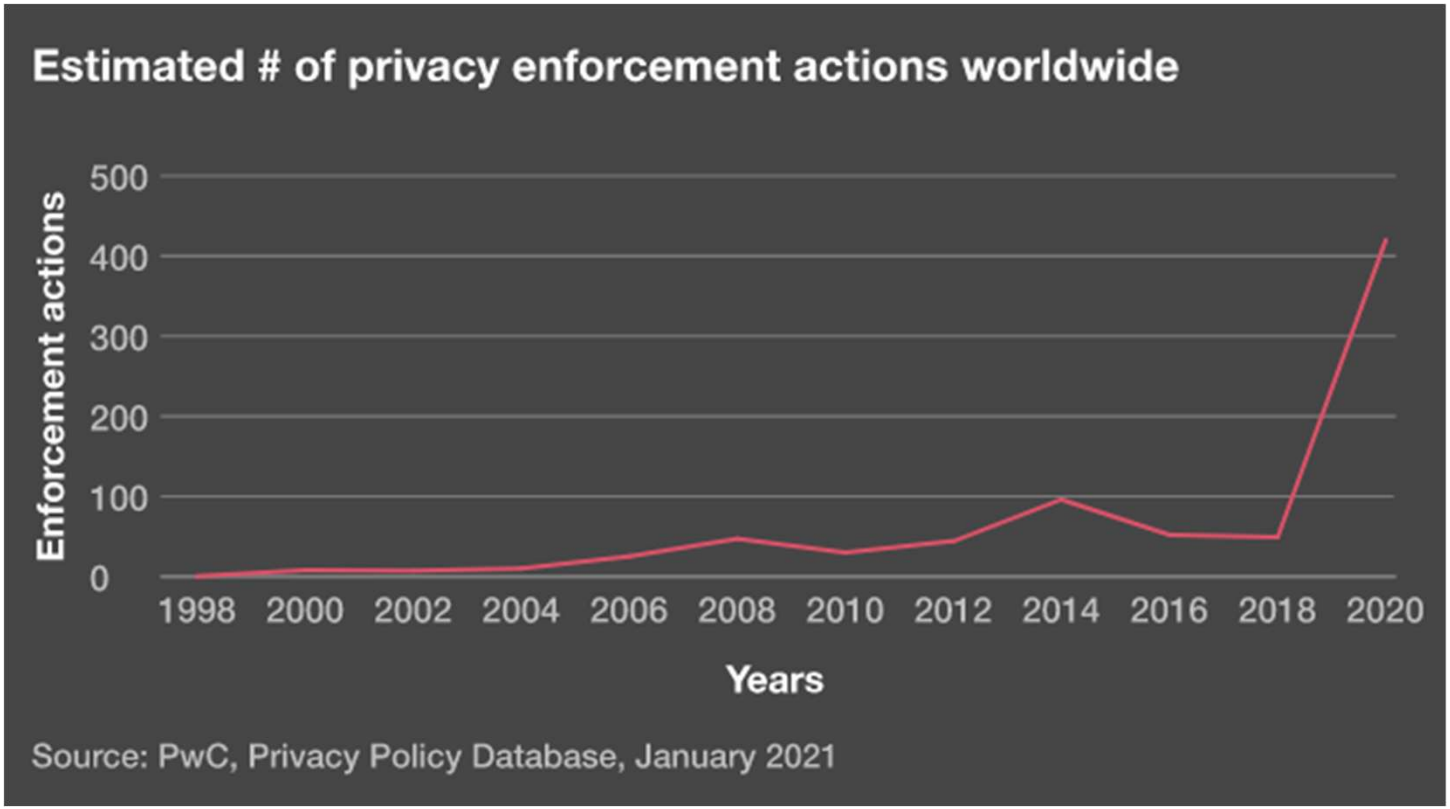
Andrew Dawson
adawson@keker.com

Agenda

- **Privacy Enforcement Trends**
- **Common Causes of Action: U.S. and California**
- **Key Defenses & Practical Takeaways**

Privacy Enforcement 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

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” – H.R. 8818

- Bipartisan and bicameral draft legislation introduced on June 25, 2024 by Congresswoman Cathy McMorris Rodgers (R-WA) and referred to the House Committee on Energy and Commerce
- 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

Privacy Regulatory Environment: Agencies

Federal Trade Commission

- Privacy / Cybersecurity Investigations
- Algorithmic bias concern; targeted AI facial recognition technology
- Children's Online Privacy Protection Act

Securities and Exchange Commission

- 2024 was the first full year of new cybersecurity disclosure rules for public companies, requiring disclosure of material cyber incidents
- Historic levels of enforcement activity continued in 2024

Case Study: *USA v. Sullivan*

- Joseph Sullivan, who served as the Chief Security Officer for Uber from 2015 to 2017.
- When Sullivan joined Uber, the company was under investigation by the Federal Trade Commission for a data breach in 2014.
- While under FTC investigation, Uber suffered another data breach. The company failed to disclose the breach to the FTC or any other state or federal regulator.
- Sullivan was found guilty of obstruction of justice and misprision of a felony for his role.

Case Background: The Uber Data Breaches

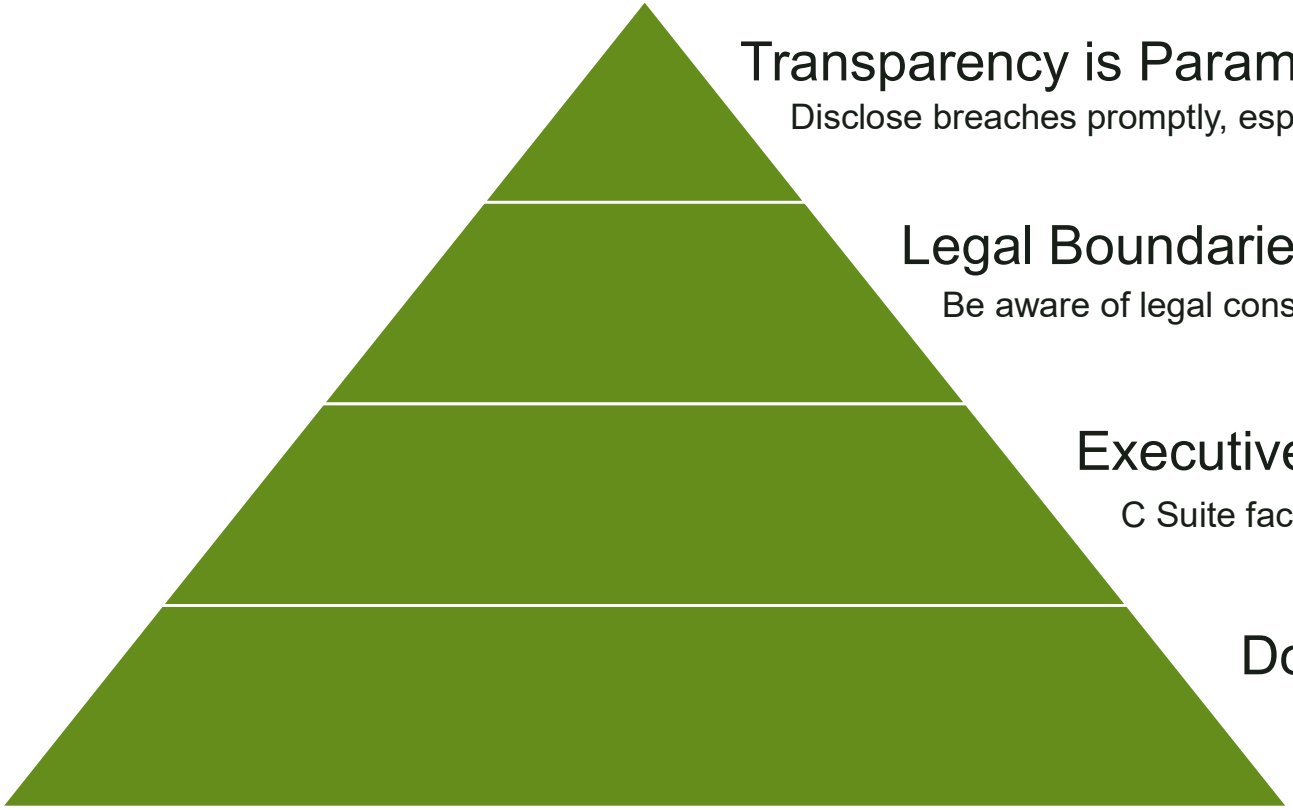
Breach
A hacker discovered an AWS key on GitHub, accessing sensitive information of tens of thousands of Uber drivers. This prompted an FTC investigation into Uber's data security practices.

Second Breach
Hackers gained access to Uber's GitHub account, found AWS keys, and downloaded unencrypted data of 600,000 individuals—similar to the 2014 breach but larger in scale. FTC not informed.

Sullivan Hired
Joseph Sullivan joined Uber as Chief Security Officer and later became Deputy General Counsel. He became heavily involved in Uber’s response to the ongoing FTC investigation.

Cover-Up Exposed
New CEO Dara Khosrowshahi discovered the truth about the breach, fired Sullivan, and publicly disclosed the incident. Federal charges followed.

Implications for In-House Counsel



Transparency is Paramount

Disclose breaches promptly, especially during investigations

Legal Boundaries

Be aware of legal considerations when engaging hackers

Executive Accountability

C Suite faces personal legal liability for cover-ups

Documentation Integrity

Accurate record-keeping is essential during security incidents

Privacy Regulatory Environment: The Rise of States

States led the charge in defining and regulating cybersecurity and privacy

- **2024**: Seven states enacted new robust privacy laws, four states' privacy laws took effect
- **2025-26**: Eleven new comprehensive privacy laws will go into effect across various states
- **By 2026**, half the US population will be covered by a comprehensive state privacy law

Across states, these are generally similar laws (ex: Children's Online Privacy Protection Act scope), with few notable differences

Notable Recent Privacy Settlements

- *State of Texas v. Google LLC* - $1.375B
  - Allegations of tracking and collecting users' geolocation, incognito search, and biometric data
- *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)
- *FTC v. Google LLC and YouTube, LLC* (D. D.C.) - $170M
  - Allegations of collecting PII from minors without parental consent in violation of the Children's Online Privacy Protection Act (COPPA)
- *United States v. Twitter, Inc.* (N.D. Cal) - $150M
  - Allegations of allowing advertisers to access PII that was purportedly collected for purposes of account security, in violation of prior FTC order.

Recent CCPA Enforcement

- **The California Privacy Protection Agency (CPPA) Board recently entered into a settlement with Honda**
  - Allegations that Honda required Californians to provide "excessive" personal information to exercise privacy rights (such as the right to opt-out of sale or sharing their data) and shared consumers' PII with ad tech companies without contract terms necessary to protect privacy
  - Settlement:
    - $632,500 fine
    - Honda required to implement a new process for Californians to assert their privacy rights, certify its compliance, train its employees, and consult a UX designer to evaluate its methods for submitting privacy requests.

Common Causes of Action: U.S. and California

Big Data in the Crosshairs

- **Increased litigation targeting not only how data is collected, but also how data is *used***
- **Examples:**
  - AI privacy suits, including chatbots
  - Location information
  - Browsing activity
  - Ad tech (pixels, tags, etc.)
  - “Cookie” tracking
  - App-usage data
  - Biometric data

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

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.

Hammerling v. Google (9th Cir. 2024)

Privacy class action alleging:

- Google tracked downloads and use of third-party mobile applications on Android operating systems without proper disclosure in its Privacy Policy

Asserted claims:

- California common-law claims; California statutes (Unfair Competition Law, Consumers Legal Remedies Act, California Invasion of Privacy Act)

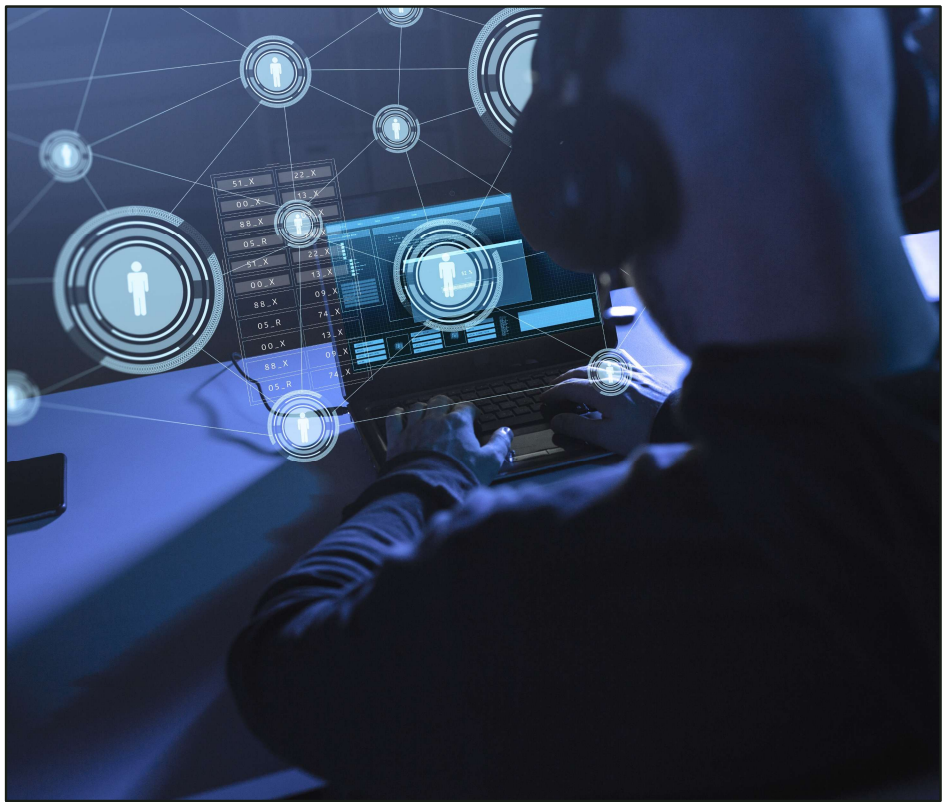
9th Circuit affirmed dismissal of all claims

- 9th Circuit found that unlike the allegations in *In re: Facebook Tracking*, Google's privacy policy "**expressly disclosed**" its intention to collect data regarding consumer activity on third-party apps

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.)**

- 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.

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."

Ad Tech Litigation: CIPA

Rise in privacy class actions against providers and users of advertising technology (pixels, ad analytics, tags, etc.)

- Typical claims: CIPA §§ 631, 632; federal Wiretap Act; constitutional and common-law privacy claims
- Theory: Ad technology implemented on an advertiser's website unlawfully "intercepts" and "eavesdrops" upon website users' communications with the advertiser
- Common targets:
  - Providers of advertising technology
  - Websites operated by advertisers, including in health-related spaces
  - Forms / surveys on websites

Ad Tech Litigation: A Case Study

***Perry-Hudson v. Twilio, Inc.* (N.D. Cal.)**

- Plaintiff asserted constitutional-privacy and CIPA §§ 631 and 632 claims against Twilio after purchasing a hair-loss product on Keeps, alleging that Keeps shared consumers' personal data with Twilio via Twilio's customer engagement software for targeted advertising.
- Two-pronged attack
  - Motion to compel arbitration based on Plaintiff's arbitration agreement with Keeps
  - Motion to dismiss focusing on Plaintiff's consent to the alleged tracking and Twilio's lack of intent to violate Plaintiff's privacy rights
- **The Court compelled the claims to arbitration**, agreeing with Twilio that it could enforce the arbitration agreement between Keeps and Plaintiff as a nonsignatory under the doctrine of equitable estoppel.

Ad Tech Litigation: Video Privacy Protection Act (VPPA)

Rise in privacy class actions against providers and users of ad tech on webpages serving video content

- Old law applied to new tech: VPPA enacted in 1988 to address the publication of Robert Bork's rental history during his Supreme Court nomination
- Imposes liability on a "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider"
- Common fact pattern:
  - Any website that serves any video content (AARP, Coach, People Magazine, online newspapers, etc.)
  - Pixel technology
  - Subscribers to the website, including simply through free online newsletters

Ad Tech Litigation: Video Privacy Protection Act (VPPA)

Who qualifies as a "consumer" under the VPPA?

- **A circuit split has emerged:**
- **CA2 and CA7**: A person need not subscribe to videos to qualify as a "consumer."
  - A person qualifies as a "consumer" any time they subscribe to goods or services from the defendant, so long as the defendant also qualifies as a "video tape service provider"
- **CA6**: A person is a "consumer" only when they subscribe to goods or services "in the nature of video cassette tapes or similar audiovisual materials."

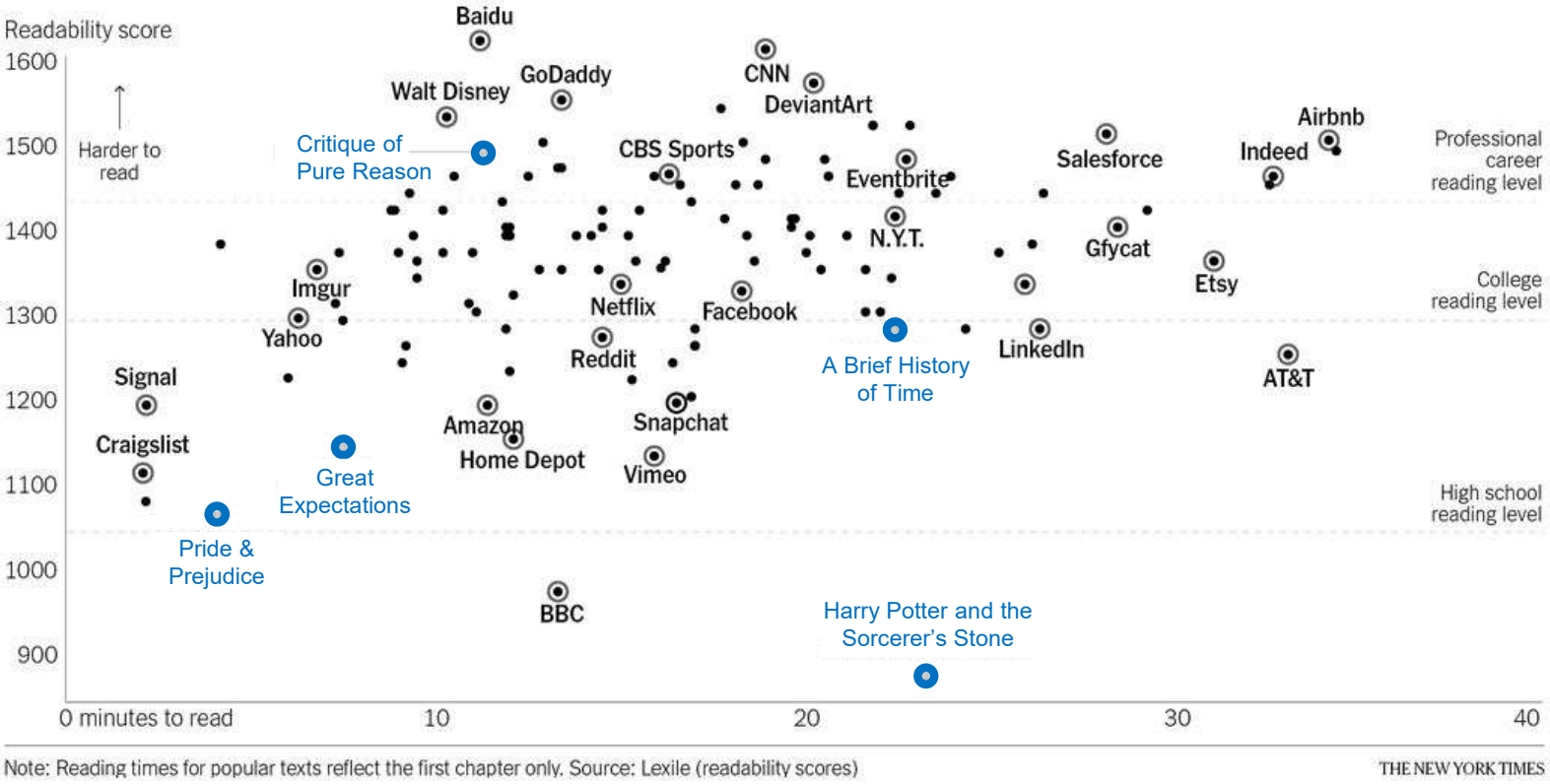
Key Defenses & Practical Takeaways

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**

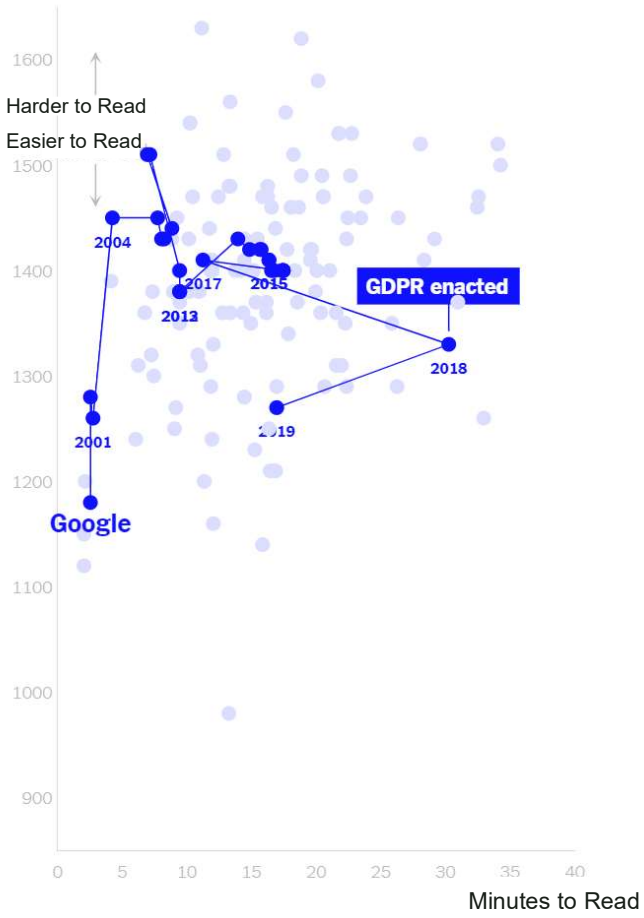
Terms of Service & Privacy Policies



"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

FTC Chairman Andrew Ferguson

"To be sure, most firms technically disclose their data practices to consumers through privacy policies. But every American knows that these **policies are long, vague, and unhelpful— probably intentionally so**. The policies also seem to change like the seasons. … And the policies are largely similar across platforms because there is not enough competition between these companies on privacy protection. **Consumers therefore have few options** if they care about participating on social media while also protecting their privacy."

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); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 624 (N.D. Cal. 2021) (denying consent defense based on disclosures in product-specific privacy notice)

Questions?

Presenters

Ben Berkowitz
Partner
bberkowitz@keker.com

Ben is an experienced trial and appellate lawyer with a track record of winning cases for major technology companies in complex and high-profile litigation. He has served as lead counsel for Google in multiple nationwide class action matters: *In Leftfield v. Google* (N.D. Cal.), he defeated a putative class action alleging trademark violations and counterfeiting related to Google's Order Online feature. In *Hammerling v. Google* (N.D. Cal.), *McCoy v. Google* (N.D. Cal.), and *Lundy v. Google* (N.D. Cal.), he defeated a series of nationwide privacy class actions regarding Google's Android operating system. In *In re Google Location History Litigation* (N.D. Cal.), he currently leads Google's defense of a consolidated set of nationwide privacy class actions on behalf of all Android and Apple mobile device users.

He also served as lead counsel for Twitter in defeating litigation involving allegations of foreign espionage by the Kingdom of Saudi Arabia in *Abdulaziz v. Twitter* (N.D. Cal.), *Al-Ahmed v. Twitter* (S.D.N.Y and N.D. Cal.), and *Al-Sadhan v. Twitter* (N.D. Cal.).

Ben also serves as lead counsel for LinkedIn and Twilio in defending several nationwide class actions alleging internet privacy violations involving pixel and other tracking technologies. Since 2015, Ben has also served as co-lead counsel nationwide for Instacart defending dozens of class and government actions.

Presenters

Christina Lee
Partner
clee@keker.com

Christina represents clients in high-stakes civil litigation matters, including complex privacy cases. She has obtained dismissals of entire complaints and critical claims through motion practice in several nationwide privacy class action cases.

She is part of the KVP team currently representing LinkedIn in multiple putative CIPA class actions. Christina has also defended Google in multiple privacy cases. This includes *McCoy v. Google* (N.D. Cal.), and *Hammerling v. Google* (N.D. Cal.), in which the firm secured dismissal on the pleadings of two successive privacy class actions, including CIPA claims, and an affirmance by the 9th Circuit. She also successfully defended Google in *In re Google Location History Litigation* (N.D. Cal.), a set of consolidated cases in which a putative class of mobile device users challenged Google's geolocation-collection practices. In that case, the firm obtained a dismissal with prejudice at the pleading stage of plaintiffs' CIPA claims.

She was also a part of the KVP team that represented Google in *Lundy v. Facebook*, a putative privacy class action that alleged that Google shared plaintiffs' geolocation information with Facebook through the Android operating system. The plaintiffs in that case voluntarily dismissed Google from the lawsuit after KVP filed a motion to dismiss on Google's behalf.

Presenters

Andrew Dawson
Partner
adawson@keker.com

Andrew has an extensive background leading trial teams and supervising complex white-collar investigations, including matters of corporate fraud, cybercrime, intellectual property, public corruption, and civil rights violations. He served nearly a decade as a federal prosecutor and leader in the U.S. Attorney's Office for the Northern District of California. He has handled numerous matters of national significance relating to intellectual property, cyber intrusions, corporate fraud, public corruption, pharmaceutical fraud, and other criminal matters.

He most recently served as chief of the district's Organized Crime Drug Enforcement Task Force Section (OCDETF), where he oversaw complex investigations relating to transnational organized crime, large-scale drug trafficking, and money laundering. Prior to this role, Andrew served as deputy chief of the Northern District's Special Prosecutions and National Security Unit, which handled national security investigations in addition to cyber intrusion, public corruption, civil rights, and other white-collar matters. He was lead trial counsel in the first ever prosecution of a corporate executive related to cybersecurity failures and associated obstruction of justice. And he worked on a high-profile prosecution arising out of a trade secret dispute between two major Silicon Valley companies.

He also served as trial counsel in a white-collar racketeering case involving $400 million in pharmaceutical fraud, handled the investigation of an infamous hack of a prominent social networking site, and secured the first-ever criminal conviction under the Lobbying Disclosure Act.