

KEKER
VAN NEST
& PETERS

+simmons
+simmons

Navigating the Privacy Minefield: Litigation Trends and Case Strategy

Association of Corporate Counsel
September 27, 2022

Presenters



Ben Berkowitz

Partner

Keker, Van Nest & Peters

bberkowitz@keker.com

415.773.6689



Tom Gorman

Partner

Keker, Van Nest & Peters

tgorman@keker.com

415.676.2292



Christina Lee

Associate

Keker, Van Nest & Peters

clee@keker.com

415.962.8844



Emily Jones

Partner, Digital Business

Simmons + Simmons, US

+44 7866 949065

emily.jones@simmons-simmons.com



Raza Rizvi

Partner, Digital Business

Simmons + Simmons, Middle East

+971 4 709 6634

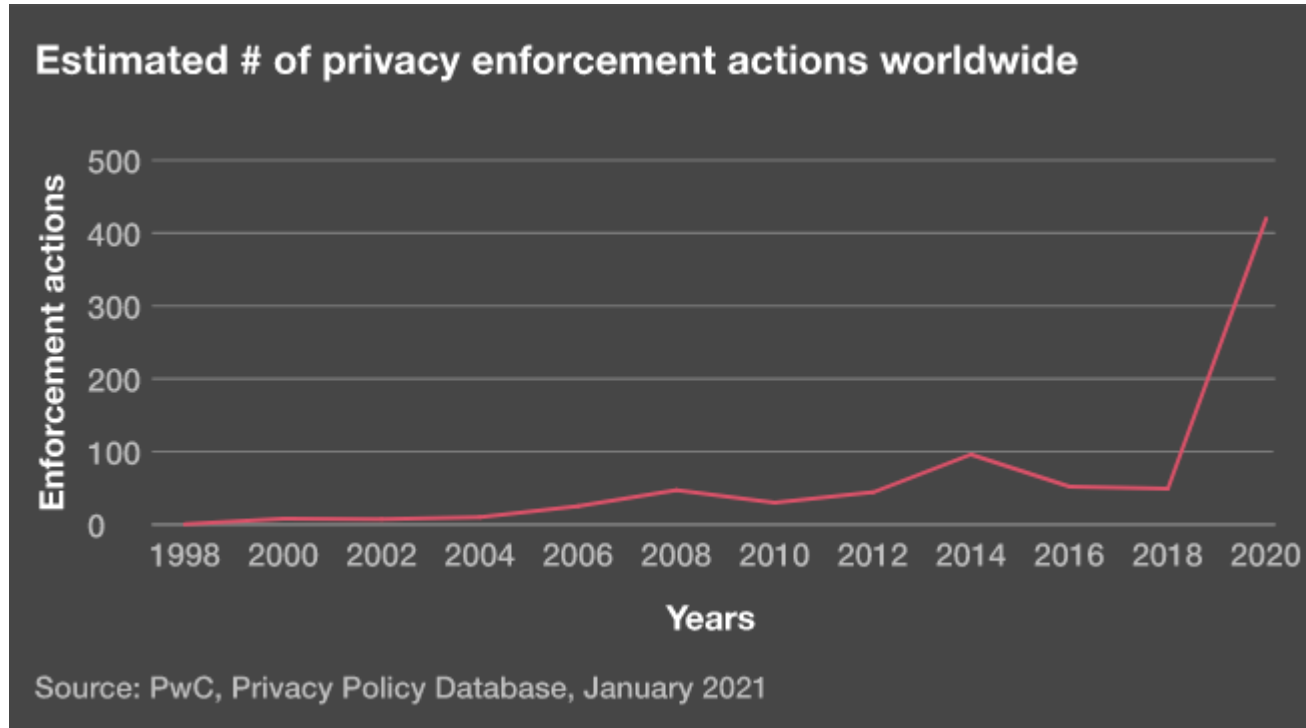
raza.rizvi@simmons-simmons.com

Agenda

- **U.S. Privacy Litigation Trend: Big Data in the Crosshairs**
- **UK/EU Enforcement Trends**
- **Cross-border Enforcement Cooperation**
- **Overview of Claims Asserted: U.S. and California**
- **Status of UK / EU Privacy Class Actions**
- **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>

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 Settlements

- *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 - Allegations of surreptitious harvesting and profiting from biometric data, geolocation information, other PII, and unpublished digital recordings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”
- *In re Plaid Inc. Privacy Litigation* (N.D. Cal.) - \$58m
 - Allegations of obtaining consumer banking data, including log-in information, and selling information to third parties

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.**

Emerging Trend: Enforcement Targeting Dark Patterns

What are dark patterns?

- “[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; Colo. SB 190 § 6-1-1303 (9)
- **Examples:**
 - Fake countdown timers
 - Misdirection
 - Obscured renewing subscription
 - Fake activity messages
 - Messages indicating low stock or high demand
 - Obstruction—making sign up easy and cancellation hard



Emerging Trend: Enforcement Targeting Dark Patterns



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS



Samuel Levine, Director, Bureau
of Consumer Protection, FTC

The FTC is stepping up enforcement regarding dark patterns.

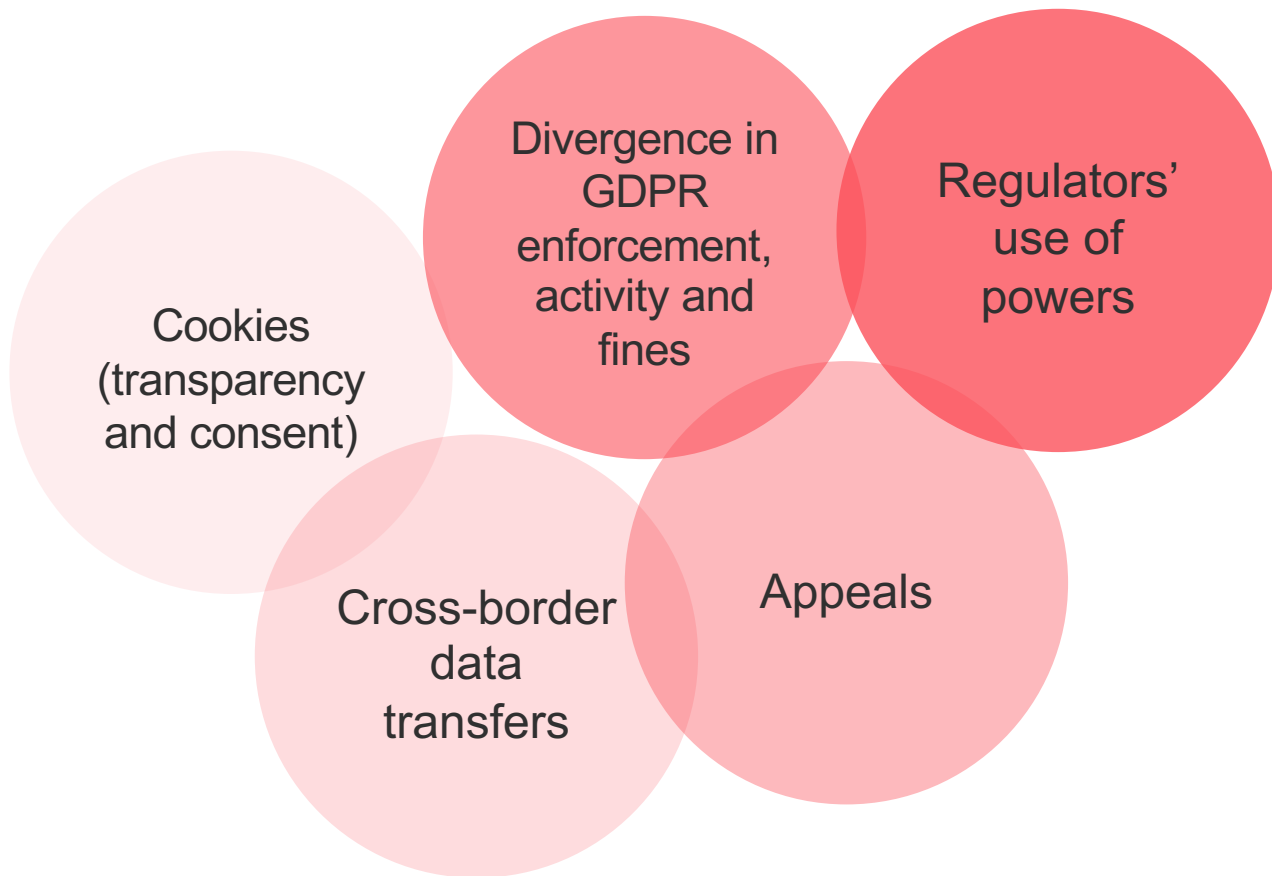
- Enforcement policy statement (Oct. 28, 2021) re: disclosures, consent, and cancellation terms
 - “Firms that deploy dark patterns and other dirty tricks should take notice.” – Samuel Levine
- Enforcement action against Age of Learning, Inc. (ABC Mouse) re: cancellation terms resulting in a \$10 million settlement

Emerging Trend: State Laws Targeting Dark Patterns

State legislators are passing laws regarding dark patterns.

- **AB 390** (October 2021)
 - Strengthens protections under California's Auto Renewal Law by ensuring that consumers can cancel automatic renewal and continuous service subscriptions online.
- **Cal. Consumer Privacy Act (CCPA) regulations** (Cal. Code Regs. Tit 11, Div. 1, Chp. 20, Section 999.315(h))
 - Bans 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** (takes effect January 1, 2023)
 - "Consent obtained through dark patterns does not constitute consent."

Enforcement trends – UK / EU (1)

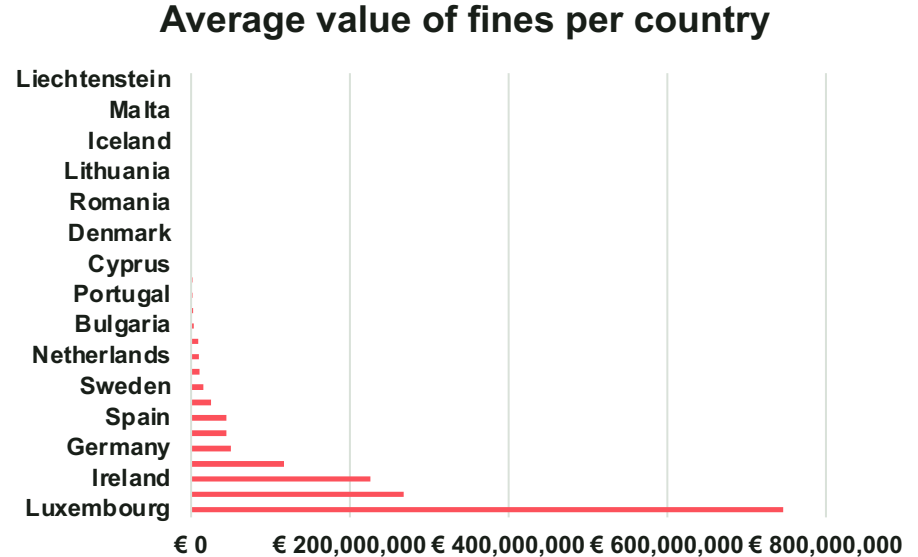
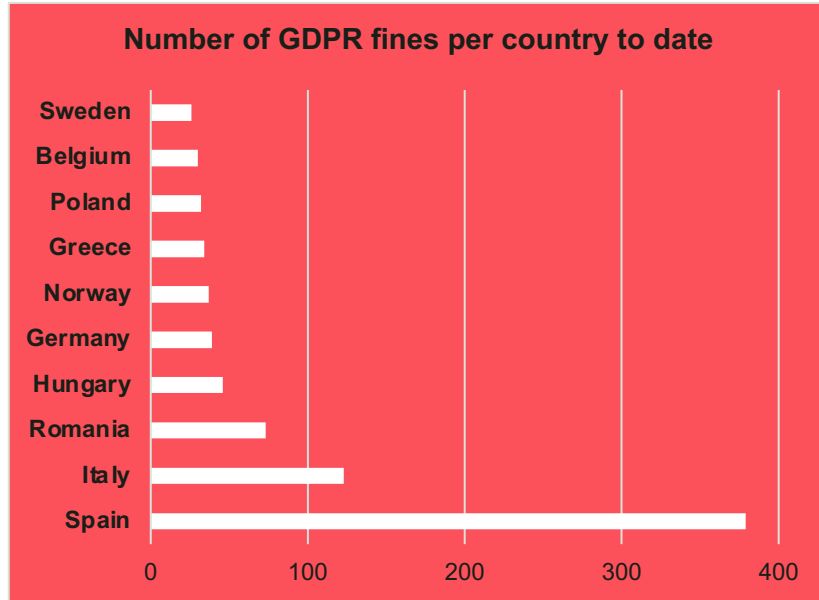


Enforcement trends – UK / EU (2)

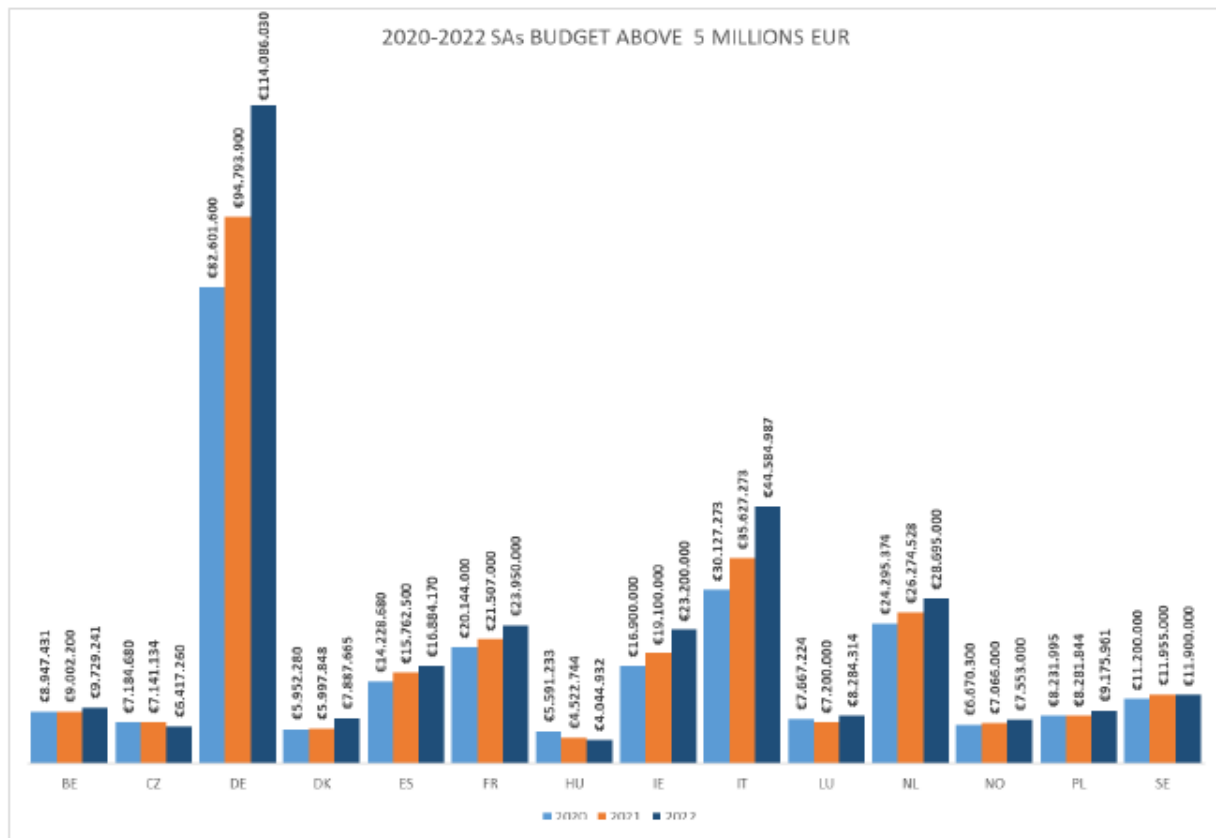
Top 10 fines across the EU

Controller / Processor	Country	Fine (€)	Breach / type of data	Date
Amazon Europe Core S.à r.l.	Luxembourg	746,000,000	Non-compliance with general data processing principles / customer data	July, 16 2021
Meta Platforms Inc (Instagram)	Ireland	405,000,000	Non-compliance with general data processing principles / children's data	September, 5 2022
WhatsApp Ireland Ltd.	Ireland	225,000,000	Insufficient fulfilment of information obligations / customer data	August, 20 2021
Google LLC	France	90,000,000	Insufficient legal basis for data processing / cookies	December, 31 2021
Facebook Ireland Ltd.	France	60,000,000	Insufficient legal basis for data processing / cookies	December, 31 2021
Google Ireland Ltd.	France	60,000,000	Insufficient legal basis for data processing / cookies	December, 31 2021
Google LLC	France	50,000,000	Insufficient legal basis for data processing / customer data	January, 21 2021
H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Germany	35,258,708	Insufficient legal basis for data processing / customer data	October, 1 2020
TIM (telecommunications operator)	Italy	27,800,000	Insufficient legal basis for data processing / customer data	January, 15 2020
Enel Energia S.p.A	Italy	26,500,000	Insufficient legal basis for data processing / customer data	January, 21 2022

Enforcement trends – UK / EU (3)

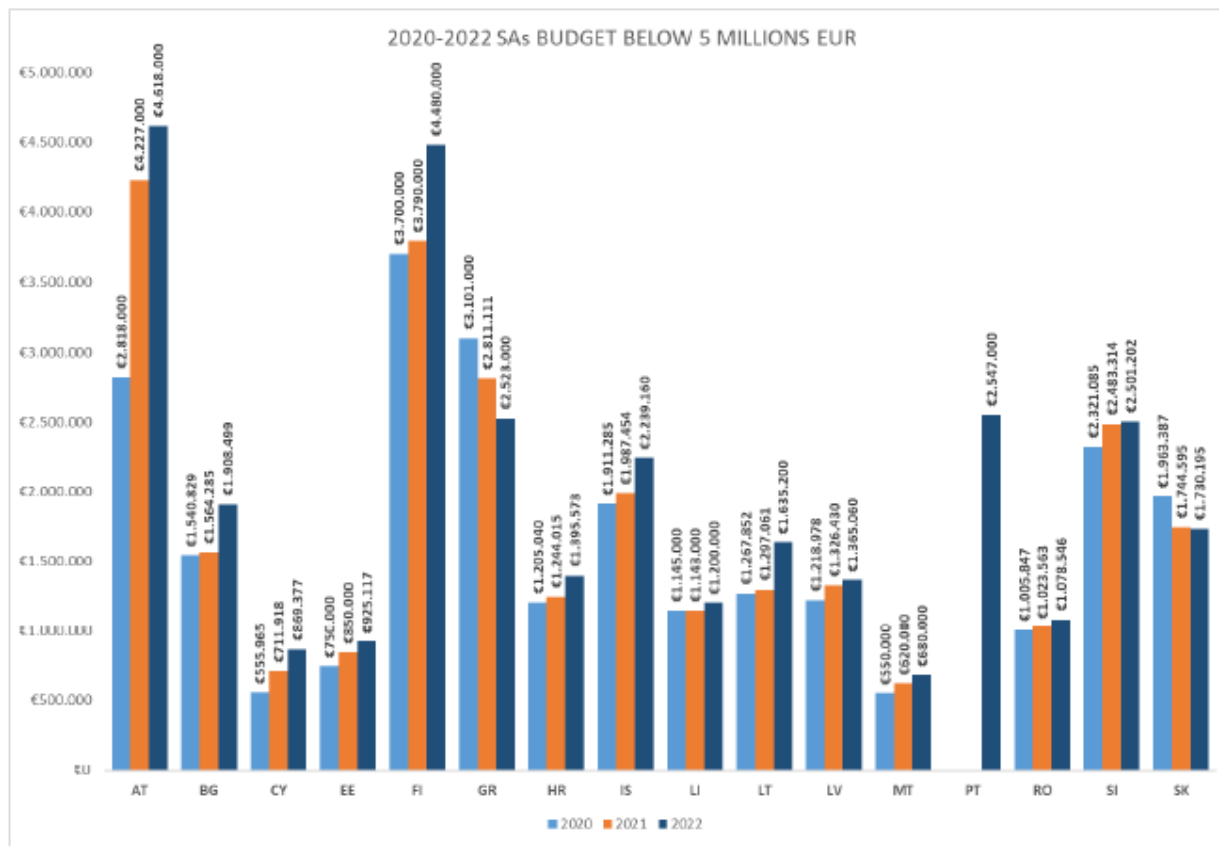


Enforcement trends – UK / EU (4)



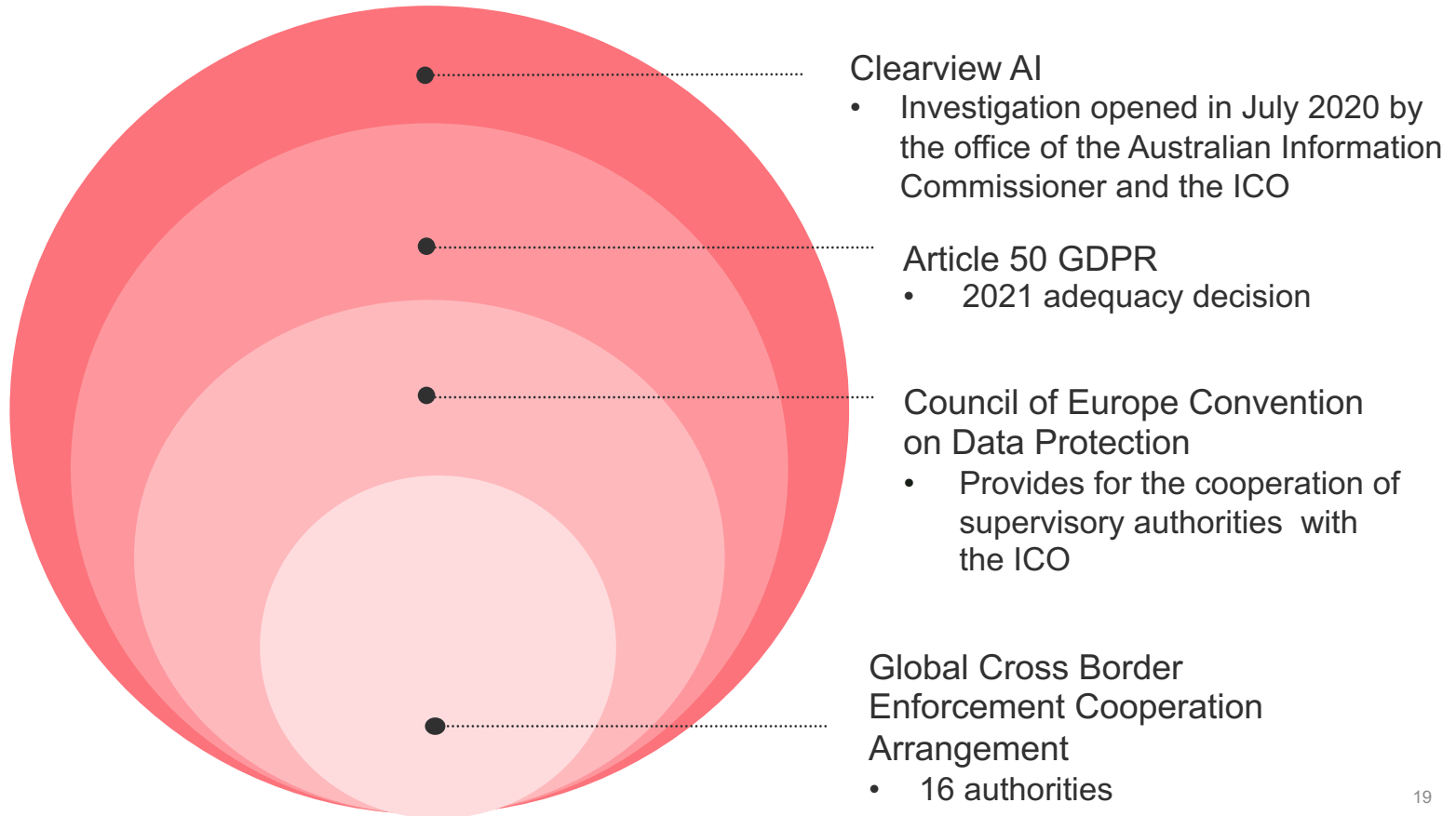
'Overview on resources made available by Member States to the Data Protection Supervisory Authorities' published by the European Data Protection Board September, 5 2022

Enforcement trends – UK / EU (5)



'Overview on resources made available by Member States to the Data Protection Supervisory Authorities' published by the European Data Protection Board September, 5 2022

Cross-border enforcement cooperation



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, Consumers 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.
- ***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.”**

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.”



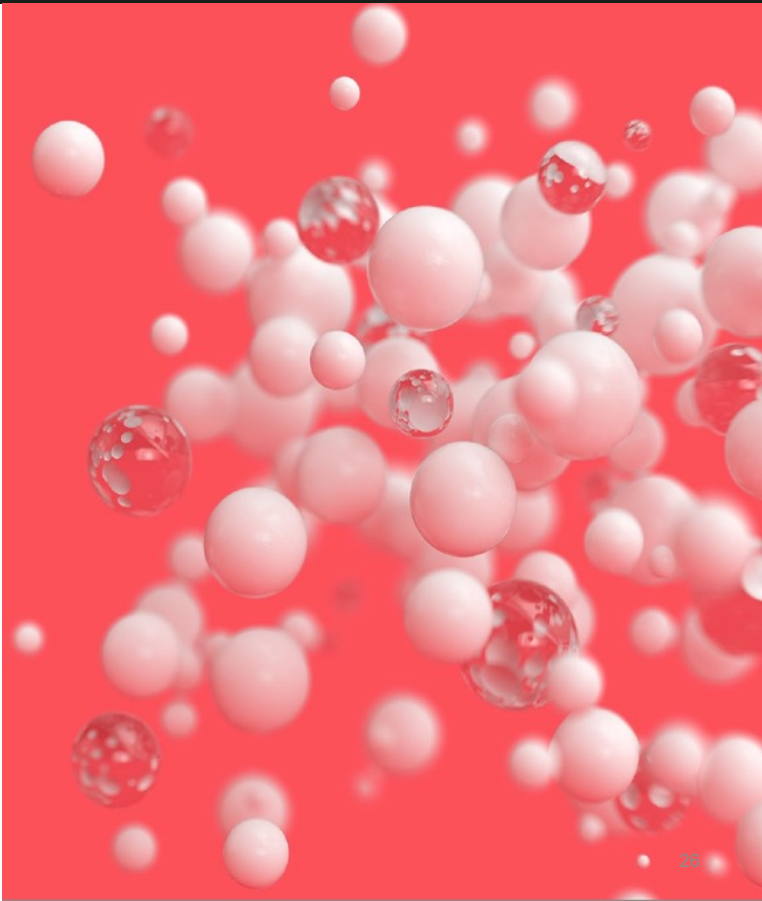
Claim Spotlight: California Invasion of Privacy Act

- ***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."

Privacy class actions – UK

Still no direct equivalent in the UK for US-style data privacy class actions

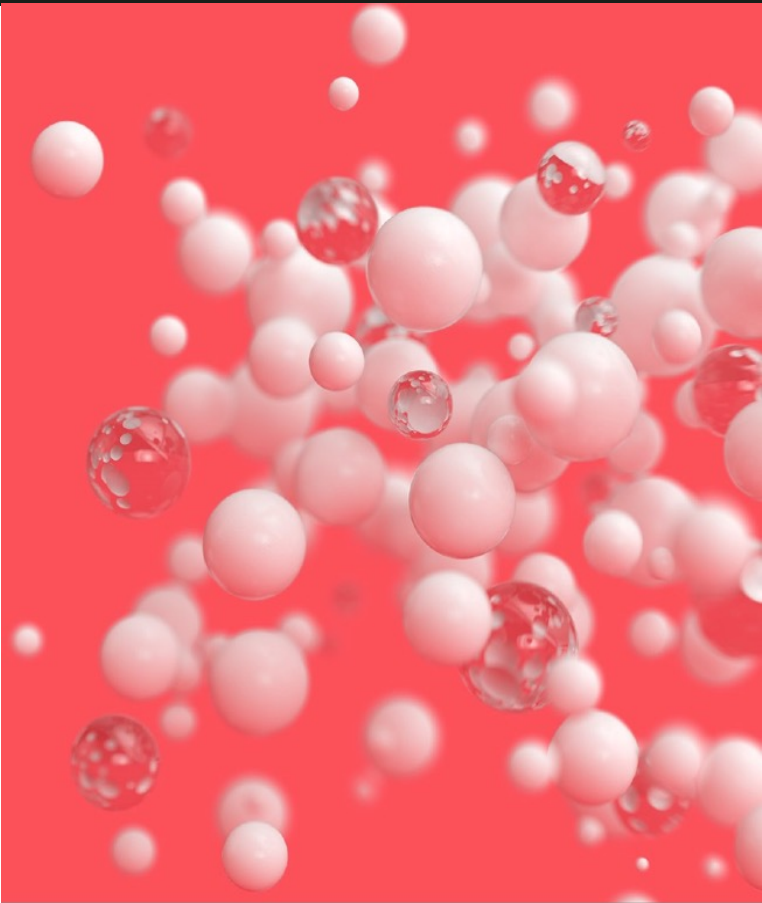
- The UK Supreme Court decision in *Lloyd v Google* stopped the sudden surge in representative actions – most have since been discontinued.
- Created difficulties for claimants in proving ‘*same interest*’, calculating measure of damages and establishing a high de minimus threshold. Data claims are now unlikely to be group actions.
- Also led to challenges to data protection actions brought through other collective mechanisms (particularly group litigation orders, previously used to bring claims against British Airways, Ticketmaster and Marriott).
- ‘*Misuse of private information*’ tort as an alternative means of redress – *Andrew Prismall v Google and DeepMind*.



Privacy class actions – EU

Not yet a direct equivalent in the EU for US-style data privacy class actions

- In April 2022, the Court of Justice of the EU (CJEU) ruled that the GDPR does not preclude national legislation enabling consumer protection associations a right to pursue data protection claims on a representative basis
- An increase in '*forum shopping*' - consumer associations looking to start a lawsuit in the jurisdiction with more favourable consumer protection laws.
- In all member states, qualified entities and consumer organisations will soon be able to use all the instruments that are included in the Representative Actions Directive, including injunctions and collective redress – including the GDPR.



Key Defenses & Practical Takeaways

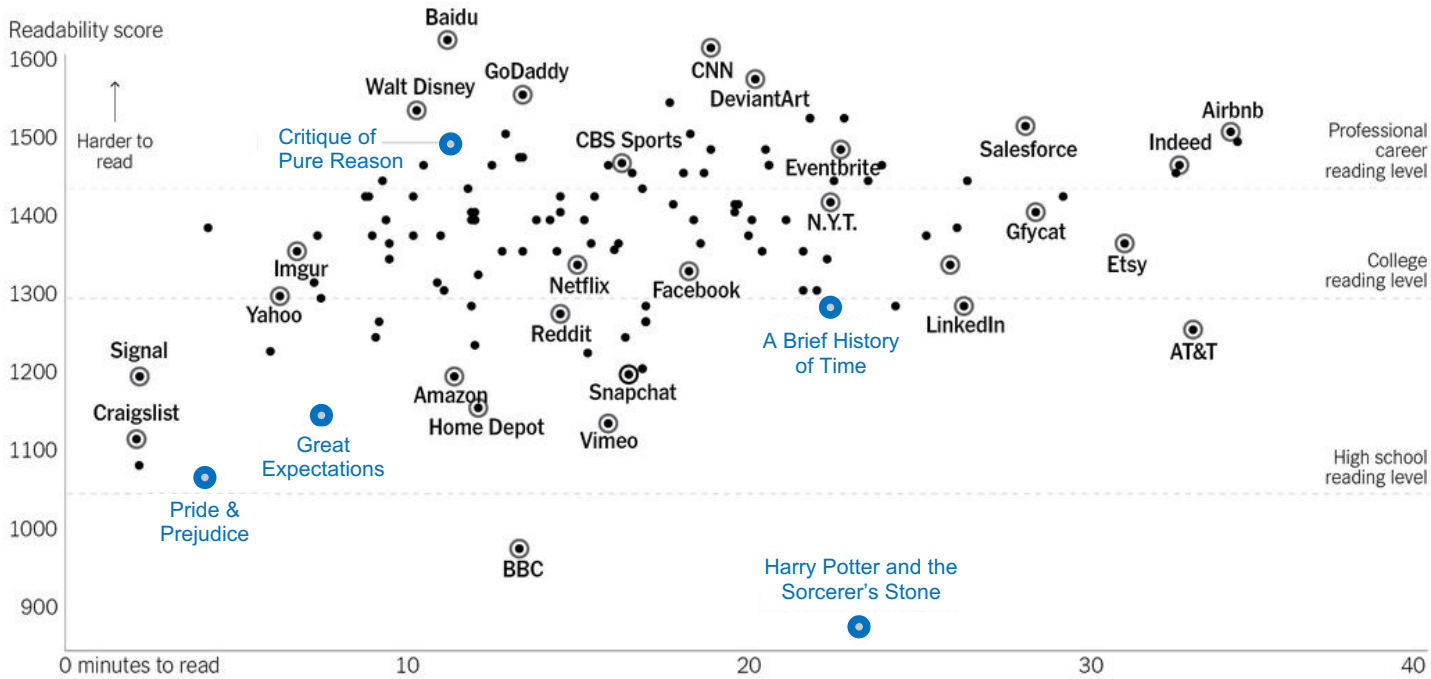
Terms of Service & Privacy Policies

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



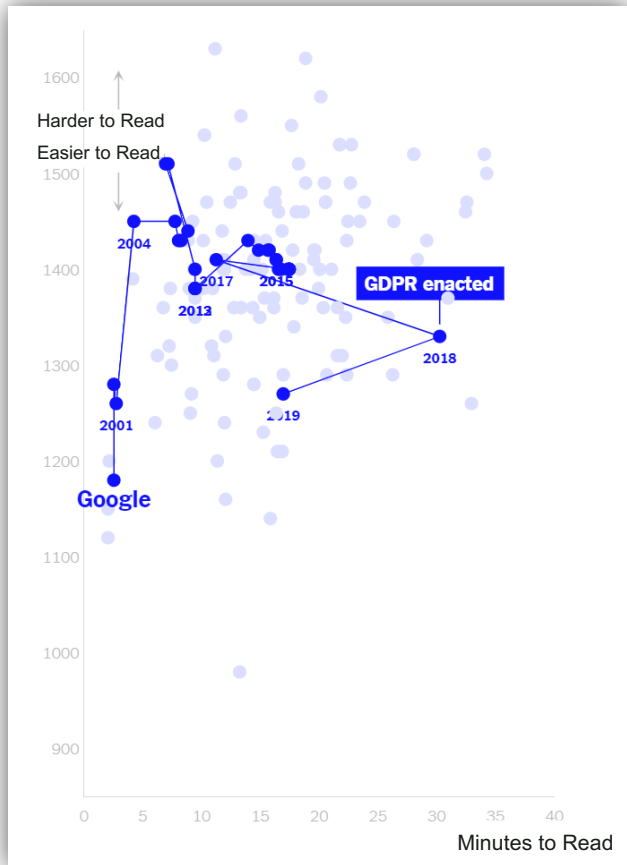
Note: Reading times for popular texts reflect the first chapter only. Source: Lexile (readability scores)

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



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.
- 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.
 - *E.g.*, *Abdulaziz v. Twitter, Inc.*, No. 19-CV-06694-LB, 2020 WL 6947929 (N.D. Cal. Aug. 12, 2020)

Practical takeaways (1)

Top tips



Review

Ensure to review the latest guidance and enforcement activity – the same principles are being breached for the same reasons time and time again



Don't delay

Uncertainty in the regulatory landscape is not a good reason to drag heels



Educate

Ensure that the relevant individuals know what to do if the worst happens – and have tested the systems and controls in place

Practical takeaways (2)

Top tips



WFH

Working remotely requires paying close attention to security – especially if you're working with personal data



Management engagement

GDPR compliance involves commitment and culture change – senior management need to be engaged



Continuous review

Carry out a data protection audit/gap analysis to identify compliance levels and any gaps that need to be addressed – set reminders to repeat the exercise

Questions?

Presenter Bios



Ben Berkowitz

Partner

bberkowitz@keker.com

415.773.6689

Ben is an experienced trial and appellate lawyer who has a track record of successfully defending major technology companies in high-profile privacy, intellectual property, and class action litigation. He currently serves as lead counsel for Google in multiple nationwide privacy class actions, including *In re Google Location History Litigation* and *Hammerling et al. v. Google*. He also led Twitter's successful defense of two recent federal lawsuits involving allegations of foreign espionage by the Kingdom of Saudi Arabia.



Tom Gorman

Partner

tgorman@keker.com

415.676.2292

Tom'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

Associate

clee@keker.com

415.962.8844

Christina represents clients in high-stakes commercial disputes, including in privacy and patent litigation. She is representing Google in several nationwide privacy class actions. She was a member of the firm's trial team that obtained a judgment of over \$80 million in a post-merger dispute that was unanimously affirmed by the Delaware Supreme Court. She previously served as a law clerk to Judge Milan D. Smith, Jr. of the U.S. Court of Appeals for the Ninth Circuit and to Judge Gonzalo P. Curiel of the U.S. District Court for the Southern District of California.

Presenter Bios



Emily Jones

Partner, Digital Business
US

+44 7866 949065

emily.jones@simmons-simmons.com

Emily is a partner at international law firm Simmons & Simmons. She is an English qualified attorney who has worked in Silicon Valley for over five years advising fast growth technology, fintech and healthcare companies on data privacy, cyber security and technology laws as they grow their businesses globally. Emily has been advising on data privacy and security issues for over 15 years and works with US companies entering new markets and launching new products and services especially involving emerging technologies, such as AI. Emily is an active member of the Simmons global data privacy team which publishes regular guidance on data privacy developments and delivers the firm's international data transfer assessment solution tool, CtrlTransfer. She is CIPP/E certified and regularly speaks at conferences on data privacy and security matters.



Raza Rizvi

Partner, Digital Business
Middle East

+971 4 709 6634

raza.rizvi@simmons-simmons.com

Raza is a partner at international law firm Simmons & Simmons and co-founded the first technology law focussed practice in the Middle East over 15 years ago. He is an English qualified Dubai-based attorney with over two decades of experience on matters concerning the commercialization, protection and regulation of data, particularly in the context of emerging technology. He has supported a wide range of international businesses on strategic projects in the Middle East and is a CIPP/E certified privacy professional, regularly advising on the policy and regulatory issues underpinning emerging data laws in the Middle East.

Thank you
