

# Potent Privacy Perspicacities

CLA Privacy Law Section Executive Committee Members:  
Sheri Porath Rockwell, Sidley Austin LLP  
Cody Venzke, ACLU  
Paul Lanois, Fieldfisher  
Brett Cook, Motorola Solutions, Inc.

September 2023

SAN DIEGO / SEPTEMBER 21- 23

# ANNUAL MEETING

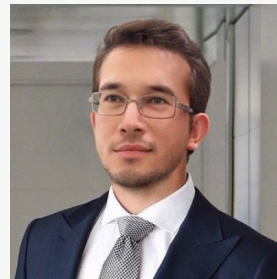
BREAKING BARRIERS

CALIFORNIA  
LAWYERS  
ASSOCIATION

#CLAAnnual

# Agenda:

- Trending Privacy Issues.....Sheri Porath Rockwell
- COPPA: How a 90s Privacy Law.....Cody Venzke  
Became the FTC’s Big Flex in 2023
- The Interplay Between.....Brett Cook  
Data Privacy and Security
- International Data Transfers.....Paul Lanois



# ANNUAL MEETING

BREAKING BARRIERS

# Trending Privacy Issues

**Sheri Porath Rockwell**

Counsel, Sidley Austin LLP

Outgoing Chair, CLA Privacy Law Section

[Sheri.rockwell@sidley.com](mailto:Sheri.rockwell@sidley.com)



SAN DIEGO / SEPTEMBER 21- 23

# ANNUAL MEETING

BREAKING BARRIERS

CALIFORNIA  
LAWYERS  
ASSOCIATION

#CLAAnnual

# Data is Everywhere + Privacy is Everywhere

DAVID NIELD GEAR JUL 16, 2023 7:00 AM

## How to Use Generative AI Tools While Still Protecting Your Privacy

Here's how to take some control of your data while using artificial intelligence tools and apps.

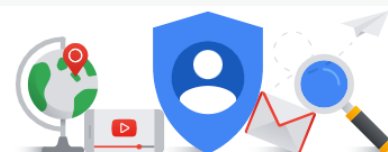
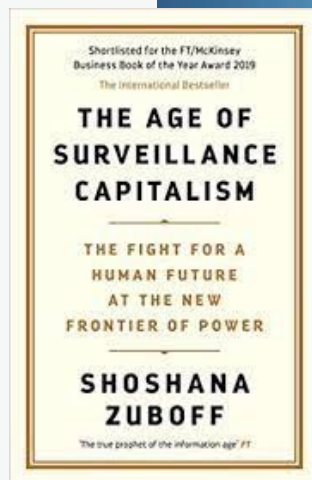


We care about your privacy

By clicking "Accept all cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Reject all cookies

Accept all cookies



GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.





# Privacy in the US – It's Exploding

- **CALIFORNIA**
  - 1<sup>st</sup> comprehensive state privacy law: California Consumer Privacy Act (CCPA)
    - Transparency
    - Access + Deletion Rights + Correction
    - Opt-out Rights
    - Statutory Damages
  - 1<sup>st</sup> (and only) state with privacy agency – California Privacy Protection Agency
- **OTHER STATES & NY CITY**
  - Post-CCPA Wave (2021-22): 4 states (VA, CO, CT, UT – Effective 2023)
  - Second Wave (2023): 7 states + 1 amendment; several pending
  - Health Privacy, Employee Privacy, Children's Privacy
- **FTC & OTHER FEDERAL AGENCIES**
  - Enforcement under FTC Act · Rulemaking (FTC, CFPB, etc.)
  - Guidance signaling enforcement priorities & expectations (FTC, EEOC)

## 2023 – The Year of Health Data Privacy

- **Paradigm-shifting laws: Washington, Nevada, Connecticut**
  - **Broad definition of “consumer health data” – more than you think**
  - **Opt-in consent for collection and separate consent for use (including digital advertising)**
  - **Know your vendors + know your online tracking technologies**
  - **Access controls**
  - **Private right of action**
- **FTC enforcement actions + guidance = digital advertising; biometrics**

## Employee Privacy Increasingly in Focus

- **California privacy law (CCPA) fully covers employment data (employees, job applicants, contractors)**
  - **Rights to access**
  - **Enhanced privacy policy**
  - **Digital advertising / sale opt-outs**
- **California AG “inquiry letters” to large employers – July 2023**
- **Automated Employment Decision Tools**
  - **EEOC – *Artificial Intelligence and Algorithmic Fairness Initiative***
  - **New York City Local Law 144 (effective July 2023)**
  - **California regulations in progress**
  - **Proposed laws**

## Key Trends & Implications for Business

- **Transparency / Be vigilant re dark patterns**
- **Purpose-based limitations**
- **Sensitive data and opt-in consent**
- **Hyper focus on digital advertising**
- **AI / algorithmic bias**
- **Vendor oversight**
- **Audits-testing + training + policies**



# COPPA: How a 90s Privacy Law Became the FTC's Big Flex in 2023

**Cody Venzke**

Senior Policy Counsel, ACLU  
Executive Committee, CLA Privacy Law  
Section

[Venzkec@gmail.com](mailto:Venzkec@gmail.com)



# COPPA: How a 90s Privacy Law Became the FTC's Big Flex in 2023

**Flex #1: General Knowledge About Your Users Is Relevant to COPPA Enforcement**

**Flex #2: COPPA Is a Modern Privacy Bill**

**Flex #3: COPPA Violations Support FTC Act Enforcement**

# Flex #1: General Knowledge About Your Users Is Relevant to COPPA Enforcement

COPPA applies (1) to online services that are directed to children or (2) to a particular user the services *knows* is a child.

**COPPA REGS:** “In determining whether a Web site or online service, or a portion thereof, is **directed to children**, the Commission will consider . . . competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.”

*FTC v. Google & YouTube (Sept. 2019)*

- **Partner Pitches:** “YouTube is today’s leader in reaching children age 6-11 against top TV channels.”
- **Rating Systems:** Categorized content into age groups and included categories for children under 13 years old.
- **Child-Directed *Portions*:** Curated channels manually and automatically and had knowledge of their content.

# Flex #1: General Knowledge About Your Users Is Relevant to COPPA Enforcement

*U.S v. Epic Games (Dec. 2022)*

- **Partner Pitches:** “[M]any Fortnite players are kids.”
- **Marketing:** Licensed toys and children’s clothing.
- **Surveys:** Survey sent to Epic showed 53% of U.S. children aged 10-12 played Fortnite weekly; internal social media data showed a third of players were 13-17.
- **Customer Support:** “Many” customer requests and reports identified players as under 13, some of which specifically highlighted concerns with on-by-default voice chat.
- **News Reports:** Articles and posts chronicling popularity among children, including the popularity of “Fortnite dances.”
- **Customer Interactions:** Sent Fortnite “swag” to celebrities’ children and incorporated feedback from children.

*“Epic knows that children play Fortnite.”*



***Statutes written decades ago don't specify how gaming ecosystems should operate. The laws have not changed, but their application has evolved and long-standing industry practices are no longer enough.***

*- Epic Statement (Dec. 19, 2022)*



***Developers who create a teen-rated or mature-rated game can no longer assume that it won't be deemed to be directed to children . . . .  
Younger players who are interested in higher-rated games can find ways to access them.  
Developers should proactively create age-appropriate ways for players to enjoy their games.***

*- Epic Statement (Dec. 19, 2022)*



## Flex #2: COPPA Is a Modern Privacy Bill

### COPPA

Online services must provide notice and obtain “verifiable parental consent.”

#### *U.S. v. Amazon (May 2023)*

- Failure to provide “truthful” notice
- Default settings to retain children’s data indefinitely violated COPPA
- “Retaining children’s voice recording for longer than necessary to fulfil their purpose”

#### *U.S. v. Edmodo (May 2023)*

- School consent is limited to the “educational content” and does not extend to “non-educational commercial purposes.”
- “[T]he COPPA Rule also requires that operators retain children’s personal information only as long as is reasonably necessary to fulfill the purpose for which it was collected.”

## Flex #3: COPPA “Violations” Support Broader FTC Enforcement

### *U.S. v. Amazon.com, Inc. (May 2023)*

- Misrepresented users’ ability to delete children’s voice records
- UDAP + COPPA claims

### *In the Matter of Epic Games (Dec. 2019)*

- Complaint refers to “parents” (15x), “kids” (10x), and “children” (3x)
- Dark patterns in purchases and “friction for friction’s sake” in refunds as a UDAP claim – no COPPA claim

### *In the Matter of Facebook, Inc. (July 2023)*

- Order to show cause why existing consent decree should not be modified
- Messenger for Kids allowed contact with “unapproved contacts” despite representations in notice to parents
- Proposed Modified Order
  - Use of children *and teens’* personal information limited to provided service – no advertising or monetization of PI
  - Permit users to delete PI collected as a child or teen; must obtain affirmative consent to retain that data within 6 months of 18th birthday



***The FTC's latest complaint against Meta is a political stunt. It's a clear attempt to usurp the authority of Congress to set industry-wide standards and instead single out one American company while allowing Chinese companies like TikTok to operate without constraint on American soil.***

*- Facebook Statement (May 3, 2023)*

# The Interplay Between Data Privacy and Security

## **Brett Cook**

Counsel, Motorola Solutions, Inc.  
Executive Committee, CLA Privacy Law  
Section

[Brett.d.cook@gmail.com](mailto:Brett.d.cook@gmail.com)



SAN DIEGO / SEPTEMBER 21- 23

# ANNUAL MEETING

BREAKING BARRIERS

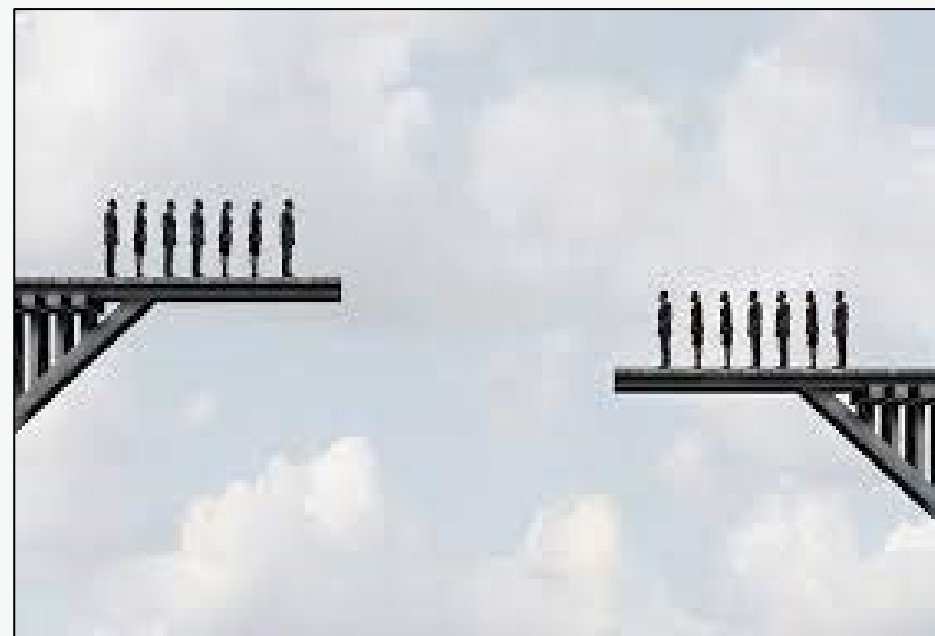
CALIFORNIA  
LAWYERS  
ASSOCIATION

#CLAAnnual

# You Can't Have One Without the Other

**Privacy** → How you treat personal data

**Cybersecurity** → How you secure the Confidentiality, Integrity and Availability of data and the information systems on which the data transits and is processed



“

*Passwords are like underwear. Don't let people see it, change it very often, and you shouldn't share it with strangers.*

*-Chris Pirillo*





## Cybersecurity Key Stats 2022

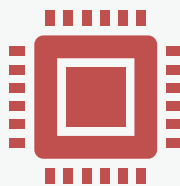
- 493.33 million ransomware attacks were detected by organizations worldwide
- Personal data breaches were the second highest cyber crime reported to FBI (Phishing was #1)
- The global average data breach cost was \$4.35 million
- The average cost of breaches resulting from stolen or compromised credentials amounted to \$4.50 million
- The healthcare industry has been the costliest for breaches for 12 consecutive years, with an average data breach cost reaching \$10.10 million

*50+ Cybersecurity Statistics for 2023 You Need to Know – Where, Who & What is Targeted.*  
Techopedia, July 18, 2023

## MOVEit Data Security Incident



The *MOVEit* transfer solution enables enterprises to transfer files between various stakeholders, including business partners and customers.



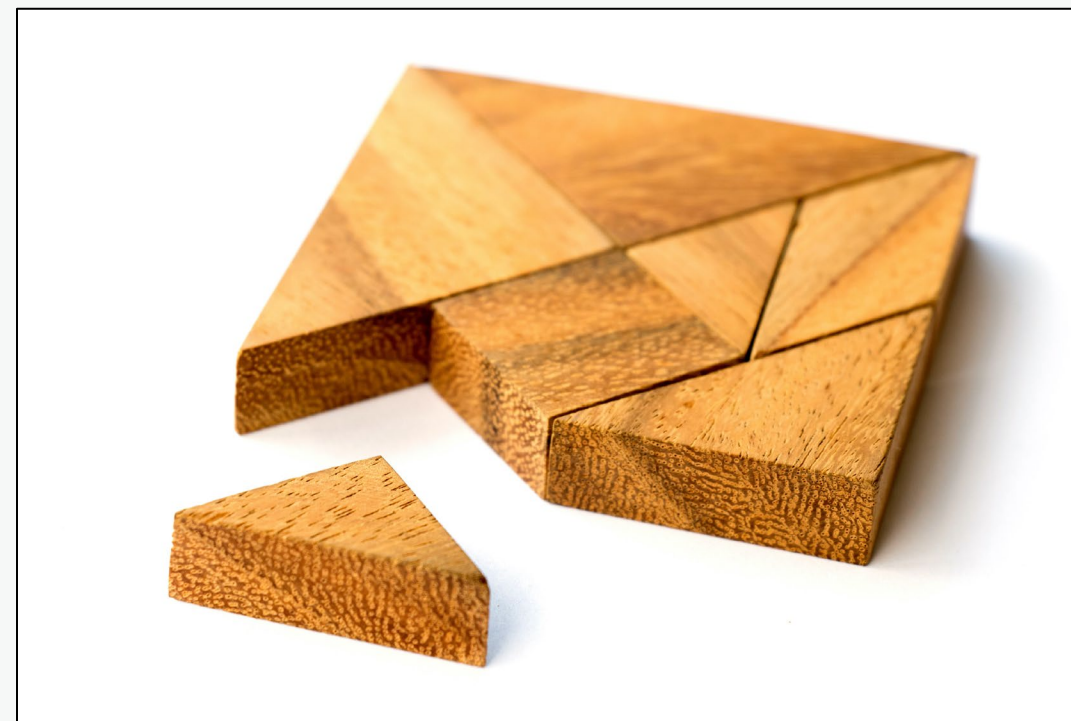
In May 2023, vulnerabilities were discovered in its file transfer web application that could allow an unauthenticated attacker to take over systems and steal data.



More than 1,700 software companies and 3.5 million users worldwide rely on its services. As of June 2023, more than 16 million people are known to have had their information accessed by hackers exploiting the vulnerabilities.

# Critical Capabilities of Data Security Programs

- Find ,Classify and Map Data Across Your Environments
- Track Dark, Shadow or Unknown Data
- Identify Potential Access & Exposure Risks
- Create Alerts for High-Risk Vulnerabilities and Critical Data



# Incident Reporting Requires Privacy & Security Collaboration

Reporting requirements vary based on data subject residence, sectoral requirements, etc.

Examples:

- CA: Must notify residents whose unencrypted personal information, as defined, was reasonably believed to have been acquired by an unauthorized person without unreasonable delay
- HIPAA: Covered Entities must notify individuals and HHS of the loss, theft or disclosures of unsecured PHI without unreasonable delay or within 60 days of discovery
- New SEC data breach disclosure regulations



# International Data Transfers

**Paul Lanois**

Director, Fieldfisher  
Executive Committee, CLA Privacy Law  
Section

[Paul.lanois@fieldfisher.com](mailto:Paul.lanois@fieldfisher.com)



SAN DIEGO / SEPTEMBER 21- 23

# ANNUAL MEETING

BREAKING BARRIERS

CALIFORNIA  
LAWYERS  
ASSOCIATION

#CLAAnnual

## Recap on international data transfers

Chapter V of the GDPR prohibits the transfer of personal data outside the EU (or UK) unless the transfer:

- Is to an adequate country
- Is subject to an appropriate safeguard (e.g. the SCCs)





## Schrems II

### Schrems II case – July 2020

- This case was led by privacy activist Max Schrems who sought to challenge the protection of data being transferred outside the EEA.
- Focus was on transfers to the U.S. and the EU-U.S. Privacy Shield but the SCCs were also impacted.
- Judgment found that the old EU SCCs did not offer adequate protection from access by government authorities in third countries.
- Transfer Impact Assessments



## EU-US Data Privacy Framework

- The European Commission has greenlit the EU-U.S. Data Privacy Framework – entered into force on 11 July.
- The Framework allows entities in Europe to transfer personal data to the US without the need for SCCs or BCRs.
- Substantial differences from Privacy Shield, namely because it provides for a new judicial redress mechanism that will enable EU citizens to seek judicial redress simply and at no cost



# Q&A