ACC Association of Corporate Counsel CHICAGO

BLANKROME

Privacy and Artificial Intelligence Litigation: Anticipating Trends to Minimize Exposure

Presented by:

Daniel Saeedi, Rachel Schaller
Gabrielle Ganze & Amanda Noonan
Blank Rome LLP

Ronak Shah
Molson Coors Beverage Company

March 20, 2025

Introductions

Daniel Saeedi
Partner

Rachel Schaller
Partner

Gabrielle Ganze
Associate

Amanda Noonan
Associate

Ronak Shah
Assistant General Counsel
Molson Coors

BLANKROME

Your Presenters

The Blank Rome Chicago Technology, AI and Privacy Team

- The Blank Rome privacy team covers the US in all areas of privacy and technology
- The Chicago Team's focus is litigation. We are:
  - Trial Lawyers and Experienced in Class Action Litigation
  - Privacy Trained and Certified
  - Several Wins in Novel Areas of Tech/Privacy Law
  - Trusted for B2B Disputes in Technology
  - Strong Understanding of Technology and Forensics

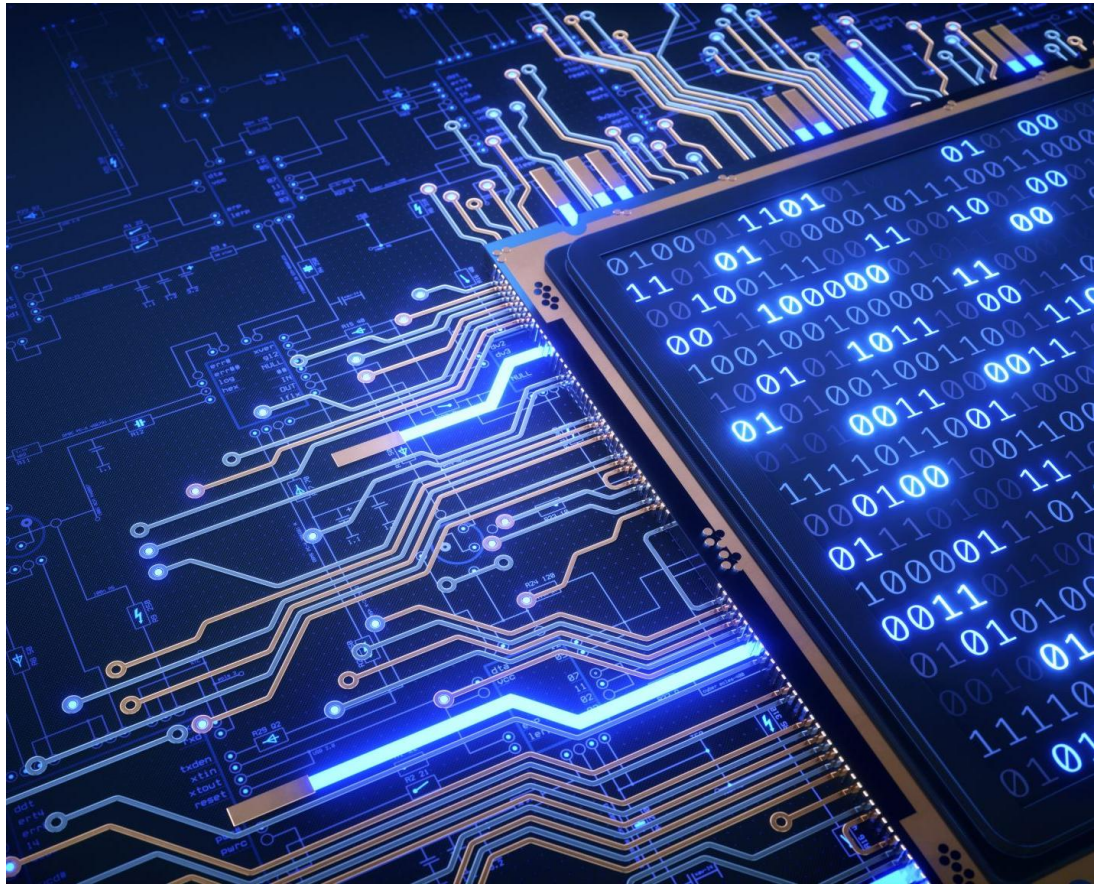
Ronak Shah

- Assistant General Counsel - Privacy, Molson Coors
- Spearheads the development and implementation of Molson Coors' global privacy and data protection strategy
- Co-chair of the Molson Coors' AI Steering Committee

BLANKROME

Presentation Overview

- Protecting Artificial Intelligence Know How and Interacting with Organizations regarding Technology
- New AI Laws and What is On the Horizon
- Biometrics, Genetics and Neural Data
- Online Tracking Litigation
- Children's Privacy



BLANKROME

AI and History

Industrial Age

Machine Age

Radio and Television Age

Nuclear Age

Space Age

Internet and Software Age

The Intelligence Age

BLANKROME

Examples of Artificial Intelligence

- ***Performing Tasks*** - Automated-decision making
- ***Predicting*** - Algorithms and machine learning
- ***Creating*** - Generative AI
- Examples:
  - Website chatbots that analyze language and respond to questions
  - Digital assistants like Siri or Alexa
  - Personalized marketing based on analyzing data
  - Software that analyzes medical imaging to identify diagnoses
  - Facial recognition for distracted driving or analyzing emotion
  - AI robotics in manufacturing

BLANKROME

Protecting Artificial Intelligence Know How

- AI is most often through patent and trade secrets mechanisms
- Protecting AI through patents has its challenges
  - Not easy to describe
  - Case law is still unsettled
  - Certain aspects of AI are not patentable on their own

Trade Secrets Law provides greater flexibility – no registration needed, the protections can last longer, more aspects can be protected, and the process for protection is automatic provided the elements are met

BLANKROME

Protecting Artificial Intelligence Know How

- **<u>What is a Trade Secret? Three Things</u>**

- **First** – It falls under one or more of the statutory protectable categories of business-related information – for AI that means:
  - Technical information, including patterns, formulas, methods, processes, programs, codes, etc.

- **Second** – It derives value from not being known – **(secret)**

- **Third** – It is the subject of *reasonable measures to keep the information secret* – **(adequate safeguards)**

BLANKROME

How are your AI programs, codes and related know-how safeguarded?

Contractual Safeguards – NDAs, Employment Agreements, Third-Party Agreements with Protections (*combatting AI espionage*)

Technical Safeguards – Need to know access, password protection, multi-factor authentication, encryption, access logs, tracking of devices and activities

Physical/HR Safeguards – Policies, Training, Clean Rooms, Physical Restrictions

BLANKROME

Interacting with Other Organizations regarding Technology

Prepare for 3 key phases when sharing AI know-how with other organizations:

1. ***Courtship*** – the processes by which two entities set up the sharing scenario
   - *Identify what will be jointly developed or modified* ***and who owns it!!!***

2. ***Relationship*** – the actual sharing of AI know-how for purposes of the shared initiative or goal
   - Monitor the process, correct failures, and ***update the parties' understandings***

3. ***Shipwreck*** – the process by which the entities wind down the sharing relationship or even become contentious regarding the know-how
   - Return or destroy shared materials and enforce rights when necessary

BLANKROME

SAFEGUARDING COMPUTER SYSTEMS – THE KEY LAWS

Federal Defend Trade Secrets Act – prevents unauthorized access, disclosure or use of trade secrets with improper means

Computer Fraud and Abuse Act – prevents unauthorized access to computer systems that cause damages or loss

Stored Communications Act – prohibits unauthorized interception of communications stored on a protected system

Electronic Communications Privacy Act – prohibits unauthorized eavesdropping of communications made in transit

State Laws and Common Law Invasion of Privacy

Copyright Act of 1976 – foundation of U.S. Copyright Law that has gradually expanded the types of original works protected

Digital Millennium Copyright Act (DMCA) – amended copyright law to address digital age and allows for notice-and-takedown requests to websites

BLANKROME

New AI Laws and What is On the Horizon

AI TRANSPARENCY AND OTHER AI LAWS

LAWS REGULATING AI IN EMPLOYMENT

BLANKROME

AI Transparency and Other Laws

- **California**
  - GenAI: Training Data Transparency, AB 2013 (Effective January 1, 2026)
  - California AI Transparency Act, SB 942 (Effective January 1, 2026)
  - **15 other new AI California Laws:** Entertainment, Elections, Misinformation and Deepfakes, Healthcare, and Education
- **Colorado -** Artificial Intelligence Act
  - Effective Feb. 1, 2026
- **Utah** - Artificial Intelligence Policy Act
  - Effective May 1, 2024
- **Tennessee** - Ensuring Likeness, Voice, and Image Security (ELVIS) Act
  - Effective July 1, 2024

BLANKROME

AI Employment Laws

- **New York City Bias Audit Law**
- **Colorado Artificial Intelligence Act**
- **Amendment to the Illinois Human Rights Act**
- **Federal EEOC Guidance (Now Rescinded)**
    - ***"The requested page cannot be found."***

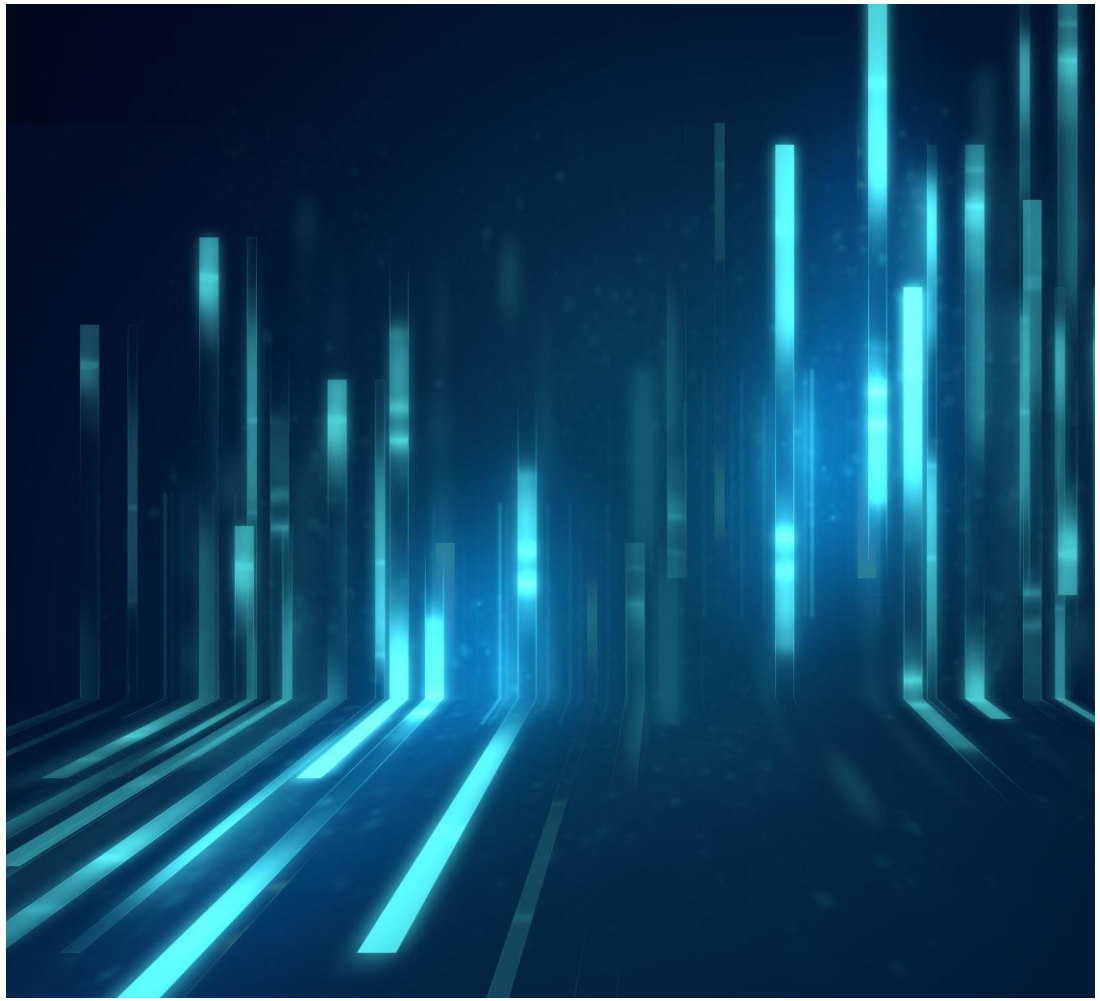
BLANKROME

New York City Local Law 144 (AEDT Bias Audit Law)

- Passed in 2021, became enforceable in July 2023
- **Automated Employment Decision Tool (AEDT):** a computation process derived from machine learning, statistical modelling, data analytics, or artificial intelligence
- 3 key requirements for AEDTs:
  - **Audits -** Mandates independent bias of AEDTs used by employers to evaluate employees or prospective employees
  - **Notification** – to employee/prospective that employer will be using AEDT
  - **Transparency** – results of the bias audit and data collected in AEDT
- **Penalties:** up to $500 for the first violation and each additional violation occurring on the same day, up to $1500 for subsequent violations

BLANKROME

Colorado Artificial Intelligence Act (CAIA)



- **Effective date:** Feb. 1, 2026
- **Requires:** documentation, disclosures, notifications, and reasonable care in high-risk AI systems
- **Applies to:** developers (including substantial modifiers) and deployers of a high-risk AI system
- **"High-risk":** makes decision that has a material effect on education, employment, housing, insurance, or financial, health care services, or legal services
- **Enforcement:** exclusively by the Colorado Attorney General
- **Penalties:** up to $20,000/violation

BLANKROME

Amendment to Illinois Human Rights Act

- **Effective date:** January 1, 2026
- **Violations:**
  - (1) an employer uses artificial intelligence that has the effect of subjecting employees to discrimination based on a protected class; or
  - (2) an employer fail to provide notice to any employee that they are using artificial intelligence
- ***What is AI under the Act?*** Generative and traditional predictive AI
- **Private Right of Action:** Plaintiffs can file suit in the Circuit Court
- **Extended SOL:** Deadline to file with IDHR extended to 2 years

BLANKROME

What Employment Activities May Involve AI?

Pre-Hire Screening	Employment Monitoring	Employment Decisions
• Recruitment – Advertisements and Chatbots • Hiring decisions – Resume Scanning and Scoring • Video Interviews and Scoring	• Software tracking: activities, performance/productivity, and location • Wearables in the Workplace	• Promotions and pay increases • Layoffs and terminations

BLANKROME

Statutory Privacy

Recent Developments in the Following:

- Biometrics Litigation
- Genetics Litigation
- Neural Data Regulation
- Online Tracking Litigation

BLANKROME

Biometrics and BIPA

Key BIPA Developments

- **What is or is not biometric information?** – The *Zellmer* Decision
- **How does the new BIPA Amendment work?** – Everyone is losing on retroactivity except us!
- **Key Technologies at Issue** – identification, optics, movement recognition, AI as applied to physical measurements

Don't forget other states and municipalities with biometrics laws!

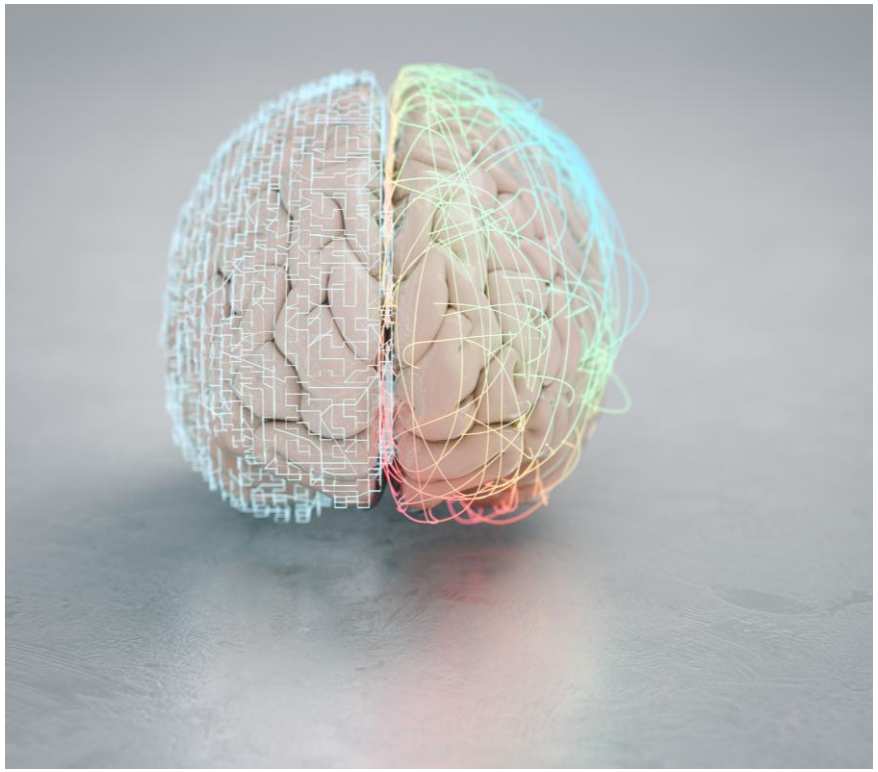
- Texas AG, Meta and the $***1.4 Billion*** Settlement

Colorado – amendment to Colorado Privacy Act (Effective July 1, 2025)

- **Requires:** Consent from employees and prospective employee (including contractors)
- **Enforcement:** Colorado Attorney General and Colorado District Attorneys
- **Penalties:** $20,000 per violation

BLANKROME

Neural Data Regulation



- ***What is neural data?*** data collected from the brain and nervous system, often through devices that can detect electrical signals
- ***As of 2023, the Global market for neurotech was growing at a compound annual rate of 12% and is expected to reach $21 billion by 2026 (Harvard Business Review)***
- ***Who is using it?***
  - Scientists, medical researchers, and now Neuralink (brain implants)
  - Technology companies like Meta, Apple, and ***any company*** selling/providing wearable devices
  - Employers via watches, headphones, earbuds, hard hats, caps, and VR headsets
- ***Who is regulating it and how?***
  - **California:** Amended "personal sensitive data" under the CCPA
  - **Colorado:** Amended "sensitive data" under the Colorado Privacy Act

BLANKROME

Genetic Information and GIPA

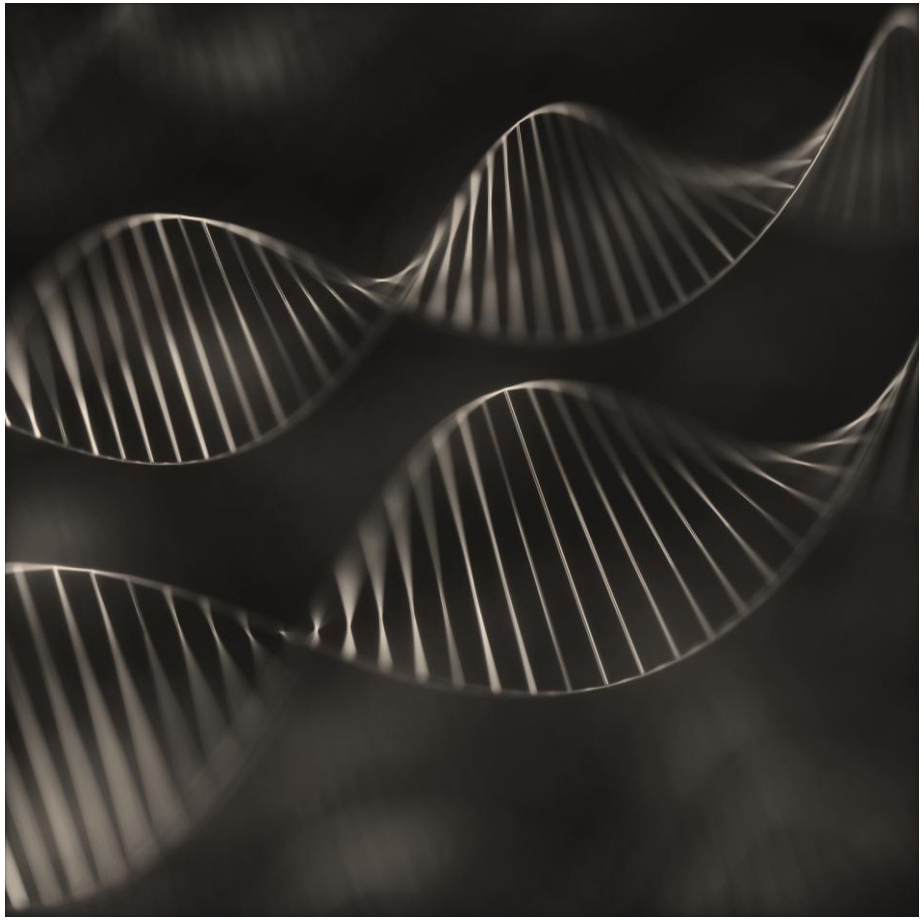
- **<u>Illinois – Genetic Information Privacy Act ("GIPA")</u>**

- ***Litigation Uptick*** – Fast growing trend of litigation under GIPA, a statute similar to BIPA in that it has large statutory penalties and a private right of action.

- ***Requirement*** - GIPA specifically prohibits Illinois employer's from "directly or indirectly" "soliciting, requiring, or requesting" an employee's genetic information as a condition of employment, preemployment application, licensure, or labor organization membership.

- ***Application -*** As family medical history is a component of genetic information, employers that require medical screenings, which may ask for family medical history, are at risk for GIPA claims.

- ***How Courts are Handling GIPA – POORLY!***



BLANKROME

What is online tracking?

1,641 online tracking lawsuits have been filed in 28 states since June 2022. Of those public filings, 1,361 were filed in California alone – 83% of all claims (*even more in private arbitration*)

A collection of information regarding users and their interactions with a website, including:

- Website analytic tools (i.e. Google Analytics, Tag Manager)
- Cookies, Pixels (Meta, TikTok and Twitter/X Pixels)
- Chatbots, Search bars
- Session Replay

How are online tracking technologies regulated?

- No laws providing private right of action specific to online tracking
- BUT, there are:
  - Comprehensive data privacy laws (which provide for AG enforcement, no private right of action)
  - Industry-specific laws (GLBA, HIPPA)
  - Laws aimed at specific groups (COPPA)

BLANKROME

Online Tracking Litigation Theories

State law statutory and common law theories have been tested in two-party consent states

- Claims fail in one-party consent states because the website operator gives the third-party consent to track

Statutes in several other two-party consent states have been leveraged in online tracking litigation:

- California Information Privacy Act (CIPA)
  - Wire tapping
  - Pen registers
- Illinois Eavesdropping Statute
- Other State laws being tested: Massachusetts Wiretap Act of 1968; Maryland Wiretapping and Electronic Surveillance Act; Arizona's Telephone, Utility, and Communications Service Records Act (TUCSRA) of 2006; Pennsylvania Wiretapping and Electronic Surveillance Control Act; Florida Security of Communications Act (FSCA)

Standing issues even in two-party consent states

BLANKROME

Illinois Trends in Online Tracking Litigation

- **Over 30 lawsuits filed in ND IL in 2024, at least 7 filed so far in 2025**
- **Illinois statutory claims**
  - Illinois Eavesdropping Statute (most claims fail; communications must be oral)
  - Illinois Consumer Fraud and Deceptive Practices Act (more success; based on representations)
- **Illinois common law claims**
  - Negligence, invasion of privacy, breach of implied contract and unjust enrichment
  - “Duty to prevent the disclosure of their private health information" via website tracking tools.
- Typically, must show the collection of highly sensitive information, leading plaintiffs to attack certain industries
  - Healthcare
  - Financial services

BLANKROME

Federal Claims Being Asserted in Illinois

- **Video Privacy Protection Act (VPPA) Litigation**
  - Increasing number of lawsuits have been filed
  - Claim businesses are illegally collecting and sharing video viewing history and PII with tracking pixels
  - In Illinois, lawsuit filed against Shout! Factor, Chess.com, Themis Bar Review

- **Electronic Communications Privacy Act, Consumer Fraud and Abuse Act and Stored Communications Act**
  - Some claims have survived dismissal depending if highly sensitive information collected (i.e., survive standing challenge)

BLANKROME

Children's Online Privacy Protection Act (COPPA)

- ***Does COPPA apply to your website?*** COPPA requires (1) verifiable parental consent and (2) a clear privacy policy handling children's data

- **New FTC Regulations:** In January 2025, the FTC approved:
  - Opt-in consent for targeted advertising and other disclosures to third parties
  - Limits on data retention

- **New State Regulations:** Expanding COPPA (NH, NJ, MD, NY, TX), Age-Appropriate Design Code Acts (CA, CT, MD) and Social Media Laws (CA, CT, FL, GA, LA, MD, NY, TN, UT)
- Bipartisan support for protecting children's data

BLANKROME

Online Tracking Technology Best practices

Privacy Policies

Cookie Banners

- Mitigates risk of private litigation under wiretapping and similar laws
- Prevents unauthorized data collection

Internal audits

Data minimization

Collecting only essential tracking data reduces risk of compliance issues

Avoiding dark patterns

Cookie Managers

- Becoming an essential legal compliance tool in US
- Several state laws (CA, CO, CT, MT, OR, TX, UT, VA, DE, IA, NH, NE, NJ, TN, MD, and MN) require a mechanism to opt out of cookies and other trackers

BLANKROME

Annual Privacy Policy Review

Arbitration Clauses

Class and mass killing procedures

Choice of law

Technology addressed

Have you addressed data collection?

Have you addressed new technologies?

New or renewed technology contracts

Legal Oversight

Review based on new laws

Adequate data protection procedures

BLANKROME

Questions/Comments

Daniel R. Saeedi

312-776-2517

Daniel.Saeedi@blankrome.com

Rachel L. Schaller

312-776-2518

Rachel.Schaller@blankrome.com

Stay Up-to Date! Blank Rome's National Privacy, Security, & Data Protection also publishes a monthly digital newsletter, "The BR Privacy & Security Download" on state, local, and federal regulations, U.S. litigation, U.S. enforcement, and internal laws and regulations

BLANKROME