Beyond the button:
Consent as a regulatory entry point

Tuesday, 28 April
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST

Welcomes and Introductions

Joanne Furtsch

VP, Knowledge & Global DPO

TrustArc

Val Ilchenko

General Counsel & Chief Privacy Officer

TrustArc

Scott Lashway

Member / Co-Chair, Privacy & Cybersecurity Practice

Mintz

TrustArc WEBINAR

LEGAL DISCLAIMER

The information provided during this webinar does not, and is not intended to, constitute legal advice.

Instead, all information, content, and materials presented during this webinar are for general informational purposes only.

Discussion Topics

1. What really is Consent?
2. Consent as a System: End-to-End Governance
3. Where Organizations Fail: Operational Breakdown
4. The Regulatory Shift: From UI to Enforcement
5. Practical Playbook: Moving to Defensible Compliance
6. Q&A

Poll Question #1

What best describes your reason for attending today's session?

1. To understand recent regulatory expectations around consent and opt-out
2. To identify operational gaps in our consent management process
3. To learn best practices and practical improvement steps
4. To benchmark our approach against industry standards
5. General interest in privacy and compliance topics

Poll Question #2

Is your organization currently using a Consent Management Platform (CMP)?

1. Yes - a fully implemented CMP across all systems
2. Yes - partially implemented or in pilot phase
3. Not yet, but planning to implement one
4. No, we manage consent manually or through custom tools
5. Not sure

What Really Is Consent?

Common terms

- Types of Tracking: Cookies, tags, pixels, serverside, etc.
- Types of consent/requests: data subject rights, UOOM do-not-sell/do-not-share, opt-out and opt-in, two-party vs. one-party (for wiretap/CIPA claims)

Common technologies

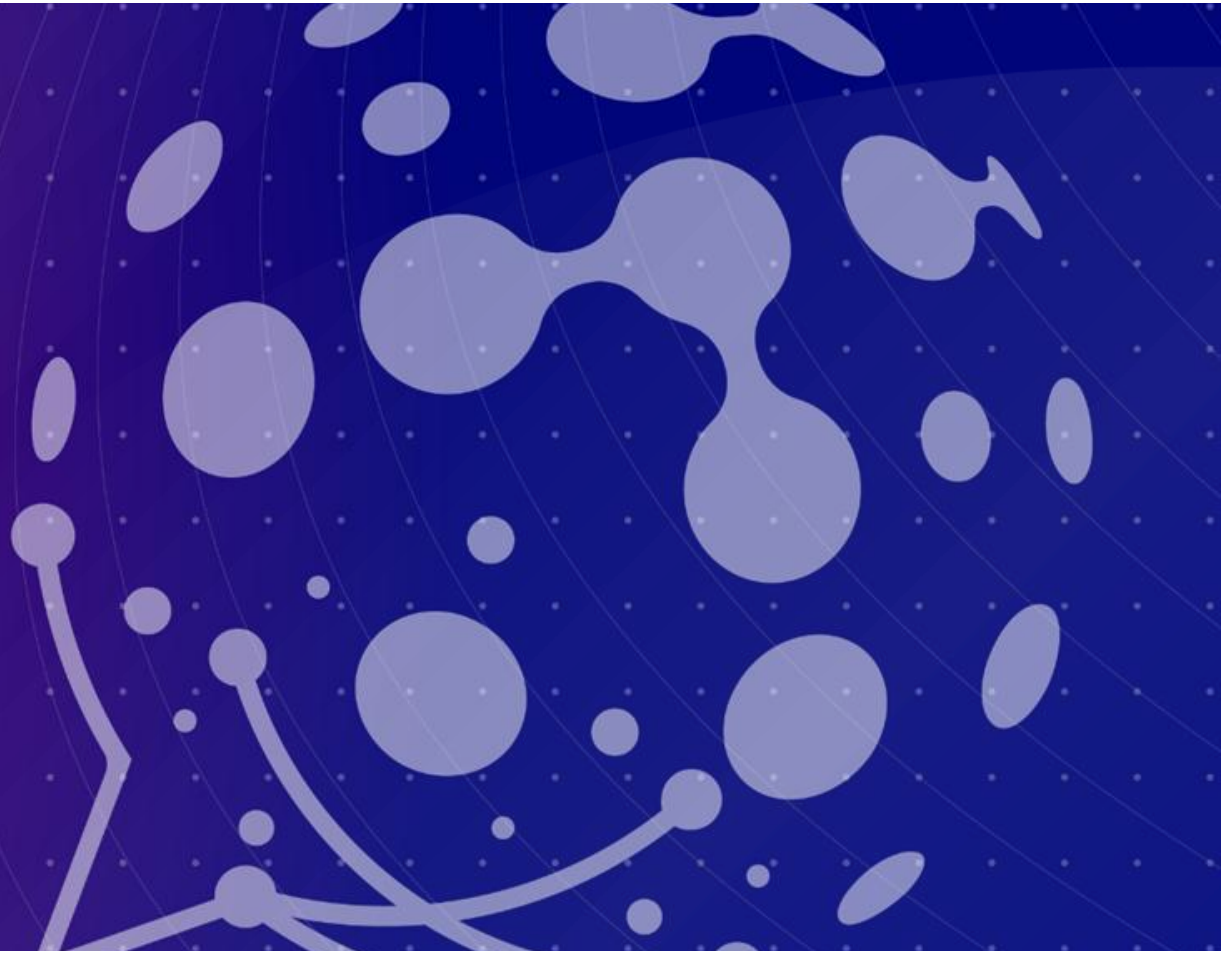
- Tag managers (GTM, Adobe Launch), cookie banners/CMPs, “Do Not Sell or Share” links, GPC, DSAR/DNSS portals

Why has it been so challenging?

- Fragmented regulations across jurisdictions (GDPR opt-in vs. US state opt-out)
- Overlapping technology stacks with no single system of record
- Gap between what the banner promises and what actually happens downstream

TrustArc WEBINAR

Consent as a System: End-to-End Governance



Consent as a System

Not a tool — an end-to-end process

Requires alignment

- **Legal:** Contracts, DPAs, “service provider agreements,” privacy notices, banner/DSAR notices, and regulatory obligations that define what you’ve promised
- **Technical:** CMP configuration, enabling UOOM/GPC, tag management, cookie classification, signal propagation to downstream systems
- **Operations:** Vendor oversight, internal workflows, DSAR/DNSS fulfillment processes, and ongoing monitoring

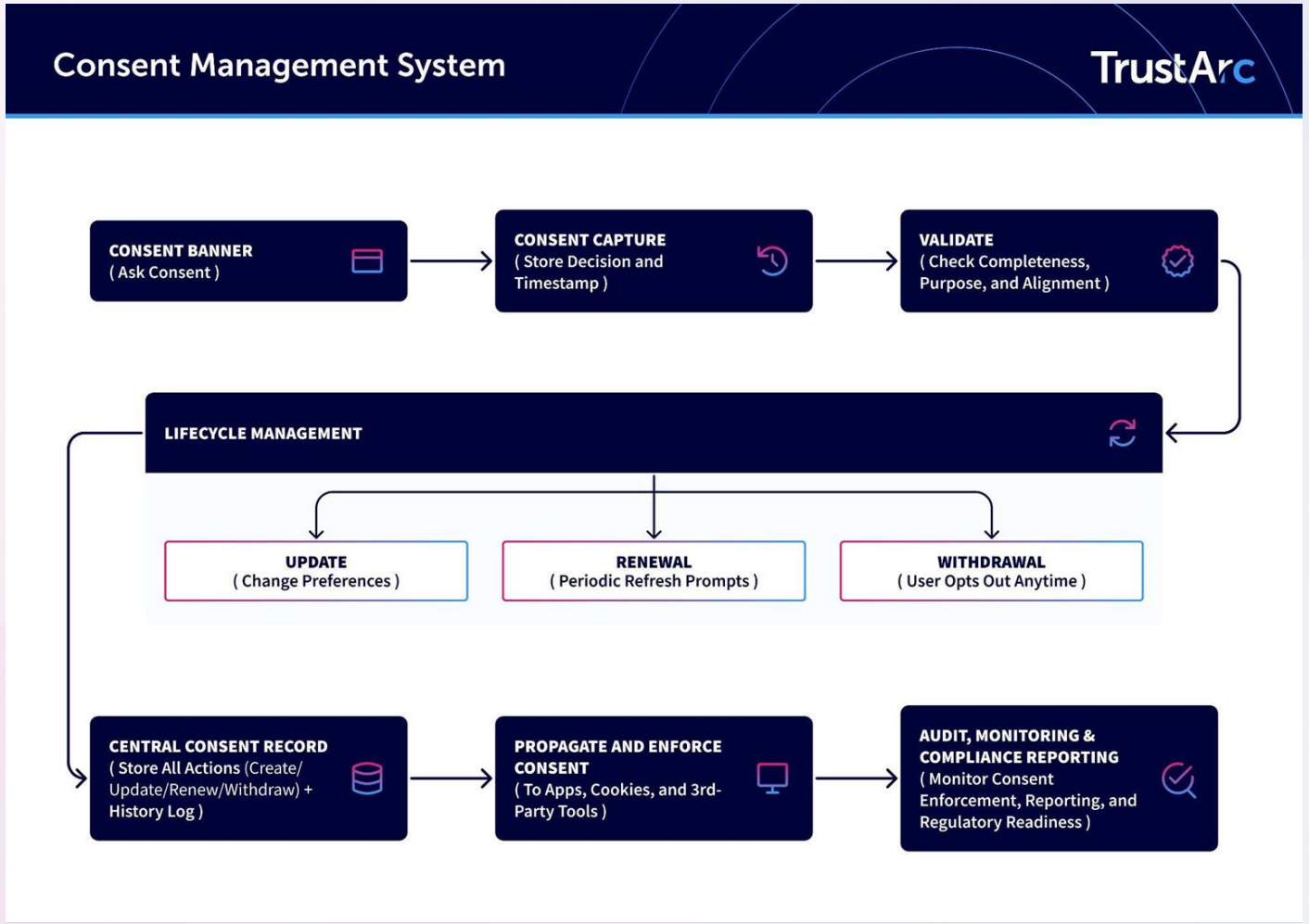
Beyond the banner: what regulators actually look for

- Contracts with vendors that match your stated data practices and meet regulatory requirements
- Data maps showing you know what data you have, how preferences flow from capture to enforcement, etc.
- Evidence that opt-outs are honored — not just recorded
- Minimization of information collected to honor requests
- “Operational compliance” programs (e.g., employee awareness + training programs and protocols)

End-to-End Flow (Where Risk Lives)

Capture → Store → Propagate → Enforce → Monitor

! Risk accumulates at each step.



What “Good” Looks Like

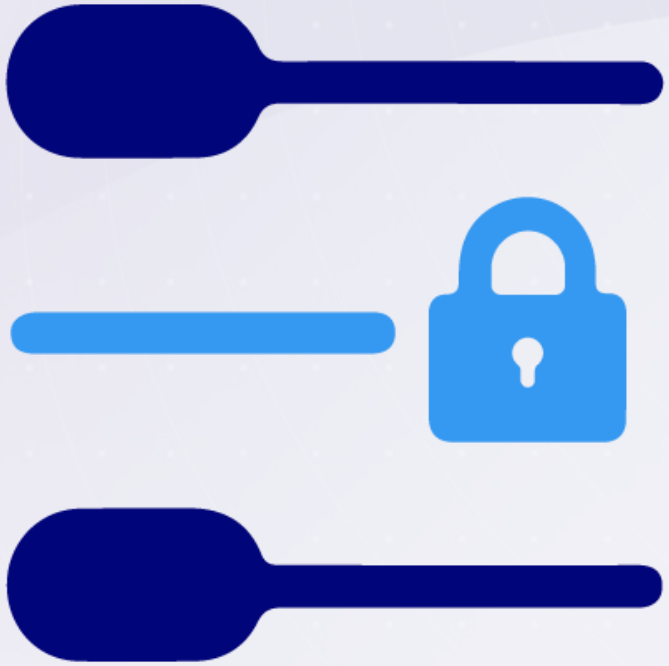
- **Consistent enforcement** — opt-out preferences honored across systems
- **Vendor alignment** — contractual obligations match technical reality; DPAs, service provider agreements and data sharing agreements enforced downstream
- **Continuous testing** — validate that opt-outs and consent withdrawals actually suppress data flows, not just update a preference record
- **Clear documentation** — proof, such as timestamped consent records, preference propagation logs, etc.
- **Defined ownership** — a single accountable team (not “marketing thinks privacy owns it”) with clear escalation paths

The Shift: Consent as a Control Point

- Consent isn't just a UX feature; it is a regulatory control mechanism

Focus has shifted: **Presence → Functionality → Proof**

- Cookie banners, DNSS links, and DSAR portals are all now entry points regulators use to launch broader investigations
- Regulators follow consent downstream — from the banner to data flows, vendor sharing, and governance controls
- The difference between looking defensible and being defensible: can you prove your controls work under scrutiny?



Poll Question #3

Who is primarily responsible for managing trackers and ensuring your CMP is functioning properly?

1. Privacy or compliance team
2. Marketing team
3. IT or web operations team
4. Shared responsibility across departments
5. Not clearly defined / unsure

TrustArc WEBINAR

Where Organizations Fail: Operational Breakdown

Where Organizations Fail

Layer 1: Capture

- Misconfigurations & GPC gaps
  Banner fires after tags load; GPC signals detected but not honored

Layer 2: Propagation

- Data silos & lag
  Preference captured but never reaches CRM, email, or ad platforms

Layer 3: Enforcement

- Vendors & rogue trackers
  Third-party pixels added outside governance; unchecked SDK sharing

Regulators follow this same sequence when investigating.

The Illusion of Compliance

What we think we have.

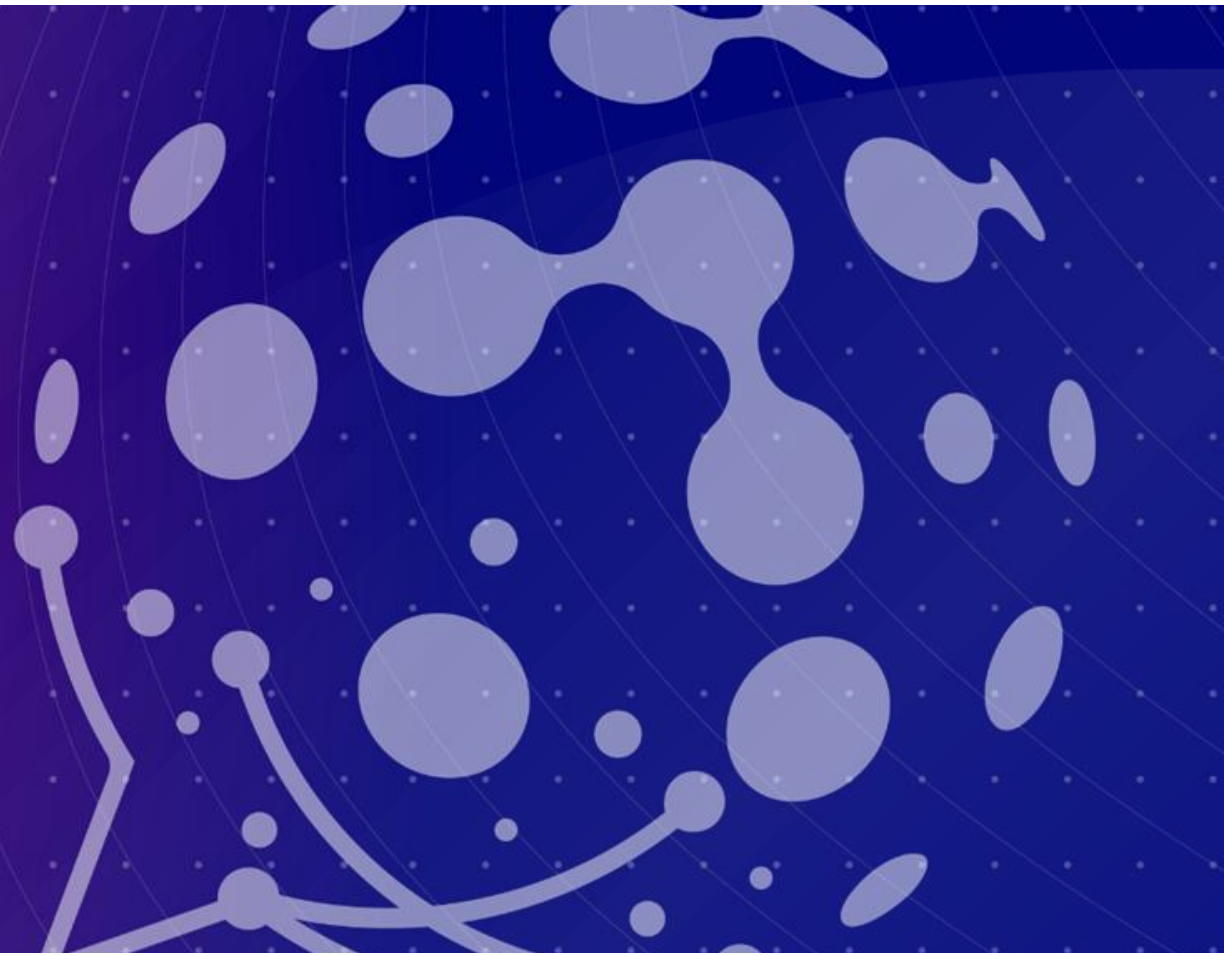
- **“We have the link”**
  Privacy policy link published on website
- **“We deployed a CMP”**
  Consent management platform is live

X The reality.

- **No valdiation**
  No checks to confirm consent flows actually work or capture valid signals
- **No monitoring**
  No ongoing oversight to detect drift, failures, or new trackers added post-deployment
- **No auditability**
  No timestamped proof of consent — making legal defense or regulatory response impossible

TrustArc WEBINAR

The Regulatory Shift: From UI to Enforcement



Consent as the “Tip of the Spear”

- **CalPrivacy and other regulators are focused on dark patterns, choice architecture, and decision making**

  CalPrivacy is testing if consent is obtained through “dark patterns” or if it is easy to understand and execute, offers symmetry in choice, avoids confusing language or interactive elements, and avoids choice architecture that impairs or interferes with the consumer’s ability to make a choice.

  “A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice.” Cal. Code Regs. tit. 11, § 7004(c)

- **The purpose is to ensure a specific type of consent with four elements**
  - Freely given
  - Specific
  - Informed
  - Unambiguous

Issues obtaining those elements of consent reveal operational gaps.

How the Regulators Test “Consent”

- **How is the request for consent or any choice presented?**

  What choice or consent request is presented?

  Is the choice or consent request presented reasonably, **according to the regulator**?

  How easy is it for a user to make a choice or give or reject consent?

- **How does a website respond to consent or choice decisions by users?**

  If a user makes a choice or declines consent, how does the website respond?

- **E.g., if a user selects “Do Not Sell or Share My Personal Information”…**

  Does the website turn off pixels/tag that could be a sale or share of personal information?

  Is the user’s decision **applied outside of the immediate website** and pixels/tags?

  Is the user’s decision **applied over time** on subsequent visits to the website?

When a regulator asks, how do you prove you presented the choice and how you operationalized it?

The Critical Question

"Is the choice or consent decision given effect?"

- Do you and the user **agree** on what the user's choice or consent decision means?
- Tested based upon two things: (1) the disclosure language surrounding the choice and consent request ***and*** (2) the effect of the choice or decision

What does "All" mean in a choice between "Accept All" or "Reject All"?

- This can be a moving target based upon user expectations: **clear language is your best defense**
- This requires building back-end systems that fulfill the choice or decision
- Compliance does not end with what is displayed after a user clicks

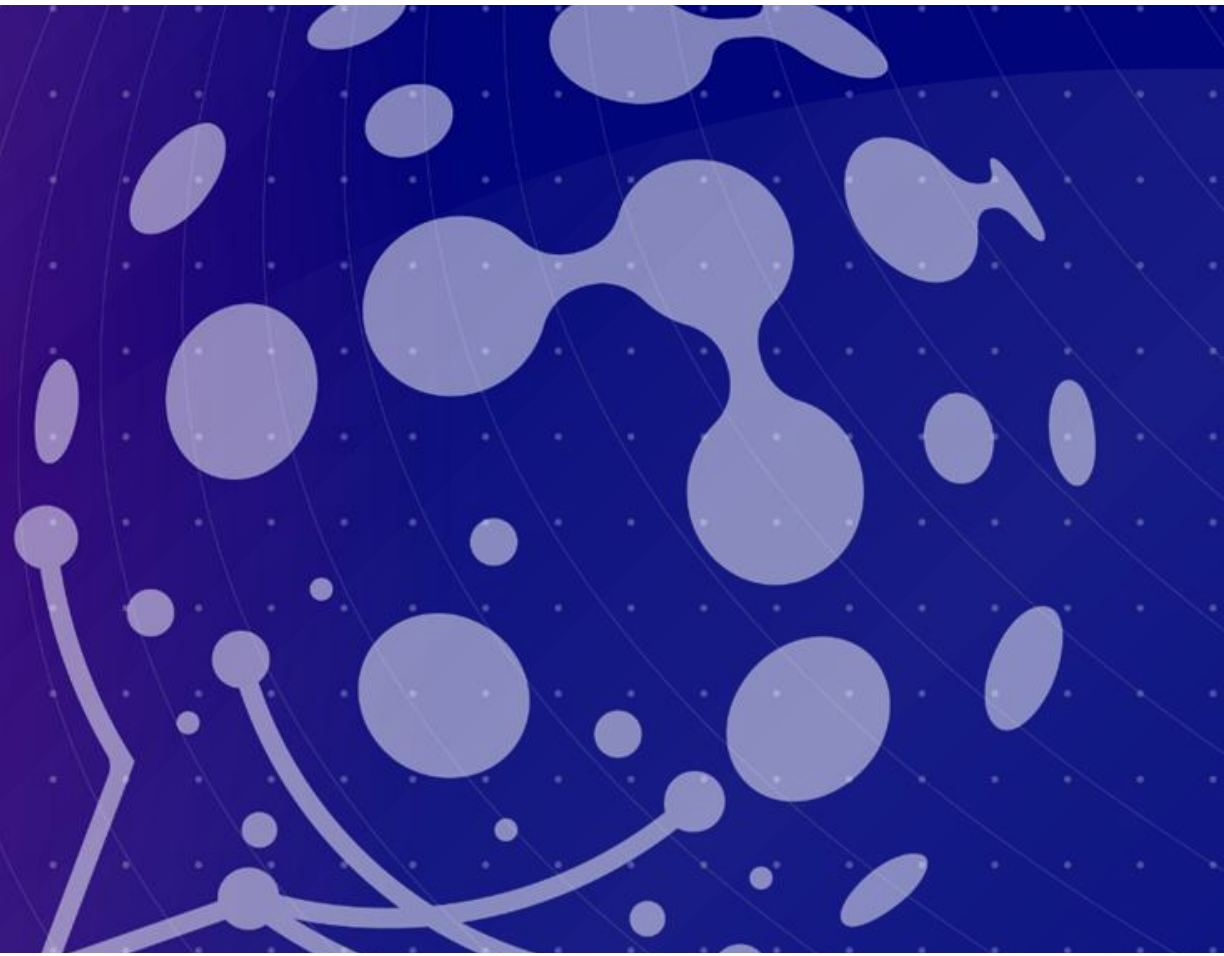
All tested by what happens after the click

Why Regulators Care Now

- **Regulatory competition** between the California AG and CalPrivacy and between California and other states with comprehensive privacy laws
- **Regulating by enforcement** establishes specific things not to do
- Most state comprehensive privacy laws are enforced by the (elected) state attorney general, and **privacy gets attention**
- Fits with new **data broker** regulations and **public awareness of data sales** through media coverage of new technologies
- Regulators testing **real-world behavior**, not only design
- Translates across industries and sectors

TrustArc WEBINAR

Practical Playbook: Moving to Defensible Compliance



From Compliance to Defensibility

- Compliance = surface-level
- Defensibility = evidence under scrutiny

If you can’t prove it, you don’t control it.

Practical Steps to Improve

- Map consent across systems
- Validate propagation & enforcement
- Implement monitoring
- Strengthen vendor oversight

Key Takeaways

Consent is a **frontline enforcement trigger**

- Cookie banners, GPC/UOOM opt-out links, DSAR, DNSS portals are where regulators start — not where they stop AND… these can create wiretap/CIPA litigation
- Operational discipline, visibility, and integrity across the full data lifecycle is what separates compliant from defensible and requires a holistic approach
- Documentation AND technical compliance is your defense — if you can't produce it under scrutiny, it doesn't count

→ What to prioritize in the next 90 days?

1. Audit and verify proper configuration of your consent mechanisms end-to-end: cookie banners, GPC/UOOm, DNSS links, DSAR portals
2. Map how preferences propagate across all downstream systems and vendors
3. Implement monitoring to detect drift, new trackers, and enforcement gaps
4. Build a documentation trail with timestamped proof you can produce under scrutiny
5. Understand + account for common enforcement patterns

Thank You!

Get a free complimentary review of your cookie consent implementation now!

trustarc.com/demo-request/consent-consumer-rights-review/

Questions and Answers

Joanne Furtsch

VP, Knowledge & Global DPO

TrustArc

Val Ilchenko

General Counsel & Chief Privacy Officer

TrustArc

Scott Lashway

Member / Co-Chair, Privacy & Cybersecurity Practice

Mintz

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ8UhH

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: **livewebconteam@iapp.org**