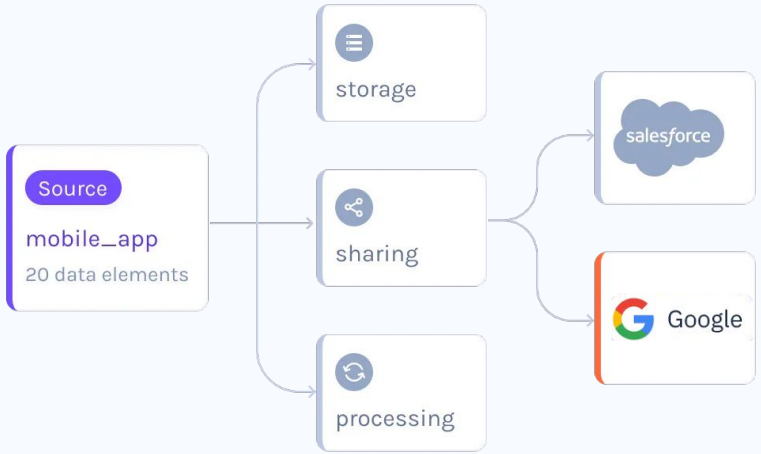
privado

Holistic mobile app privacy risk prevention: Dynamic and static app scanning

Thursday January 23, 2025



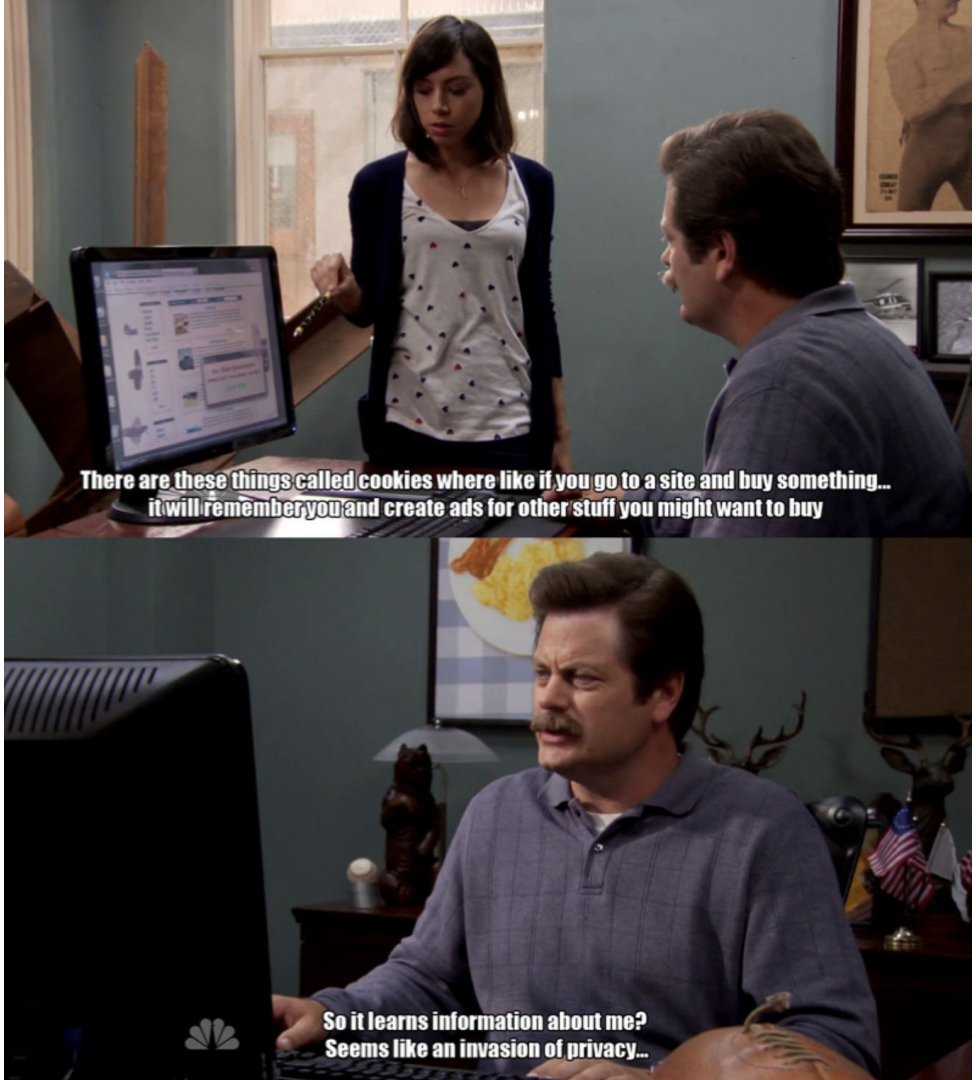
Today’s Speaker

Vaibhav Antil

CEO, Privado, CIPM

Agenda

- The State of Website Privacy Report Preview
- Mobile App Regulation & Enforcement Trends in US & EU
- Recent Privacy Fines for Mobile Apps
- Privado Solution Overview


There are these things called cookies where like if you go to a site and buy something...
it will remember you and create ads for other stuff you might want to buy
So it learns information about me?
Seems like an invasion of privacy...

THE STATE OF WEBSITE PRIVACY

2024

Insights on privacy compliance trends, risks, and best practices for websites.

privado

Our research shows most top websites have privacy compliance risks

United States

76% of the most visited websites in the US do not honor CPRA opt-out signals

69 Non-compliant websites average 69 CPRA consent compliance risks

Europe

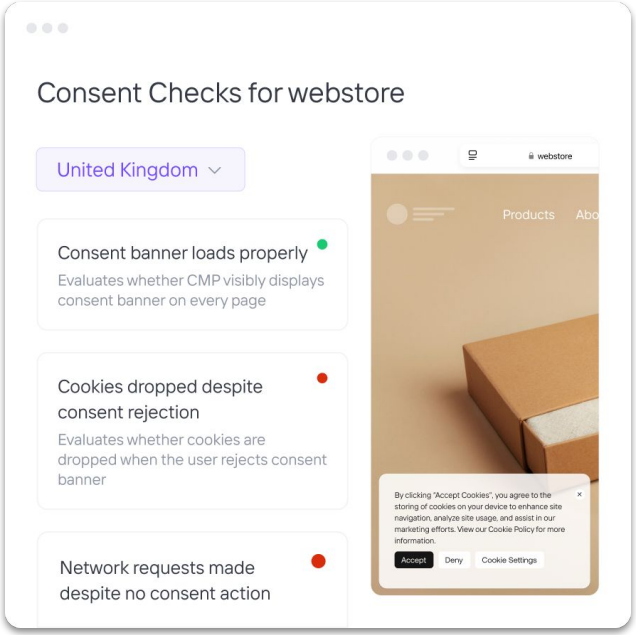
74% of the most visited websites in Europe do not honor GDPR opt-in consent

23 Non-compliant websites average 23 GDPR consent compliance risks

Source: *Privado State of Website Privacy 2024*

Prevent CMP misconfigurations with dynamic website scanning

- Dynamically scan websites to test that CMPs limit cookies and network requests according to consent
- Run scans in all locations
- Identify all 3rd party pixels and cookies
- Set workflows to run scans that flag risks when websites are updated



US and EU privacy regulators are rapidly increasing scrutiny of mobile apps

Regulation or Guidance	Enforcement Start Date	Applicable Restriction
Various rules from the FTC (Federal Trade Commission)	2021	Published guidance in 2021 and 2022 targeting mobile apps; Users must opt-in before sensitive health, financial, or location data can be shared
CIPA (California Invasion of Privacy Act)	2023 web / app fines began	Prohibits unauthorized wiretapping or recording of electronic communications without the consent of all parties.
CPRA (California Privacy Rights Act)	March 2024	Must give users option to opt-out of sharing or selling personal data
COPPA (Children's Online Privacy Protection Rule)	Early 2025	Adds requirements to further protect data for children under 13. Must list all 3rd parties receiving children’s data in parental disclosures
CNIL Mobile App Privacy Guidance	Spring 2025	Specifies new requirements mobile apps must follow to comply with GDPR, targeting SDK governance, data sharing, & insufficient consent

January 16, 2025 COPPA Update: **List every third-party recipient, or else**

Key New Requirements

- Parental disclosures must list all 3rd parties receiving children's personal data
- Obtain new parental consent when a material change is made to data sharing
- Any sharing of children's personal data with an undisclosed 3rd party will now constitute a COPPA violation

Preparing for CNIL Mobile App Sweep: **Know your SDKs**

CNIL Requirement 6.3

» App publishers and developers are responsible for using third parties in a compliant manner

» Identify data processed by each SDK

» Ensure SDKs honor consent

Preparation Checklist

1. Maintain live SDK inventory
2. Identify data flows from SDKs
3. Audit contracts with SDKs
4. Implement SDK review process

January 21, 2025 CNIL announcement: “In the coming months, the CNIL will pay particular attention to the compliance of SDK providers”

Preparing for CNIL Mobile App Sweep: **Limit permission requests**

CNIL Requirement 5.5

- Request permission for the least amount of data as possible
- Offer users alternatives to providing data access
- Process data collected locally when possible

Preparation Checklist

1. Maintain live inventory of data collected via permissions
2. Identify data flows to third parties
3. Ensure data processing aligns with privacy policies

Recent US Mobile App Privacy Fines

Company	Date	Regulation	Fine	Violation	Sharing Mechanism
Flo Health	January 2021	FTC	Undisclosed	Shared personal health data without proper consent and in violation of their privacy policy	Mobile app SDKs
Easy Healthcare (Premom app)	May 2023		$100K		Mobile app SDKs
Cerebral	April 2024		$7M		Mobile app SDKs and web pixels
Tilting Point (SpongeBob app)	June 2024	CPRA & COPPA	$500K	Shared children's data without proper consent and in violation of privacy policy	Mobile app SDKs
Twilio (Segment CDP SDK)	August 2024	CIPA	TBD	3rd party collected excessive and sensitive personal data without consent	Mobile app SDKs

Top Mobile App Privacy Risks

1st Party Collection Risks

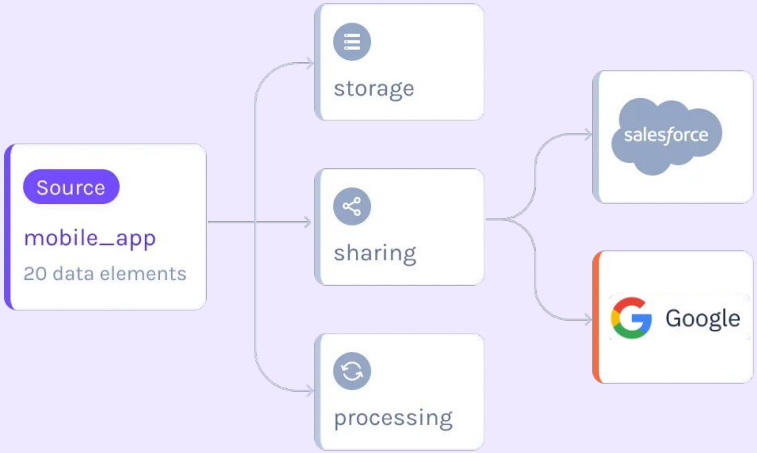
- Overcollection
- Persistent identifiers
- Children’s data

3rd Party Sharing Risks

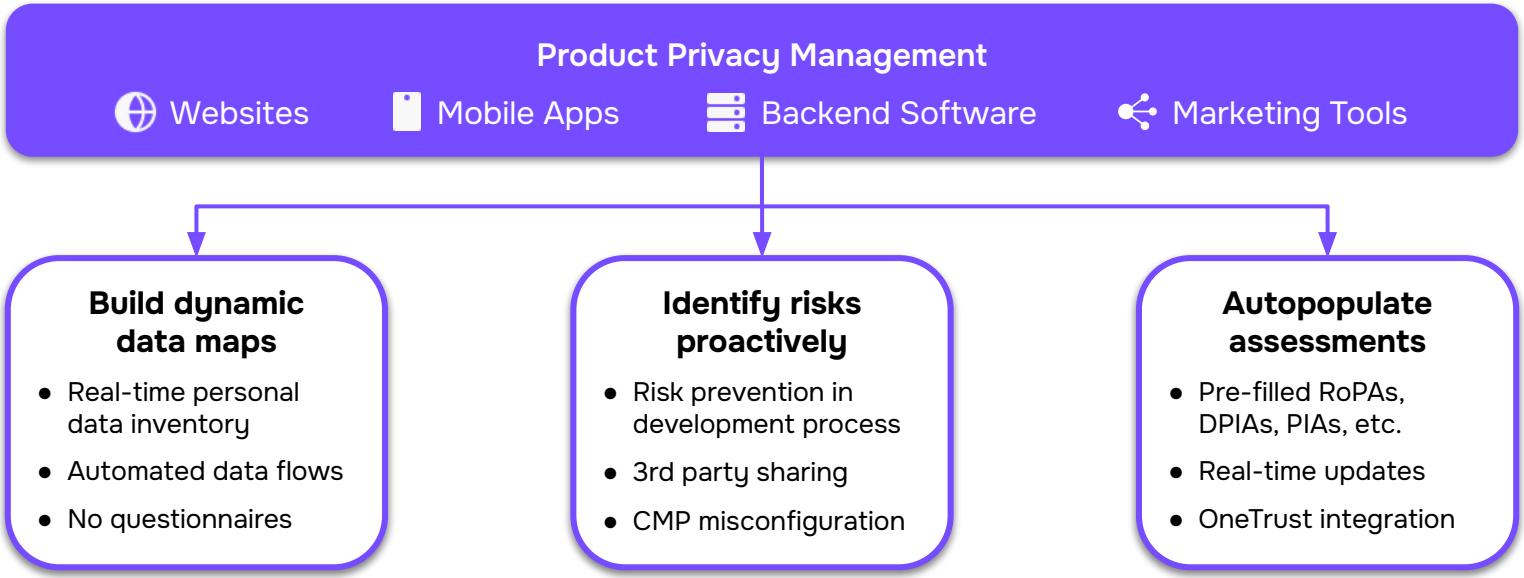
- Insufficient consent
- Sensitive data sharing
- Children’s data sharing
- 4th party publisher risks

privado

Solution Overview:
Holistic privacy risk prevention



Privado monitors risk at the source

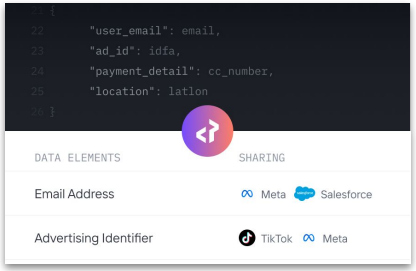


Unlock full data visibility and continuous privacy governance

Scan mobile apps inside and out for holistic privacy risk prevention

Static Code Scanning

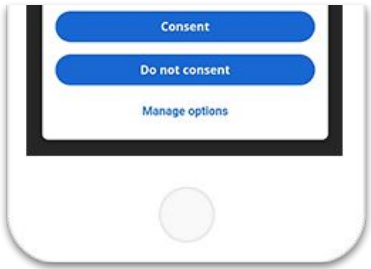
Map all data flows & flag risks early



- ✔ Build complete inventory of data elements and flows third parties
- ✔ Automate RoPAs, PIAs, DPIAs
- ✔ Flag risks in the dev process

Dynamic App Scanning

Test data flows based on consent

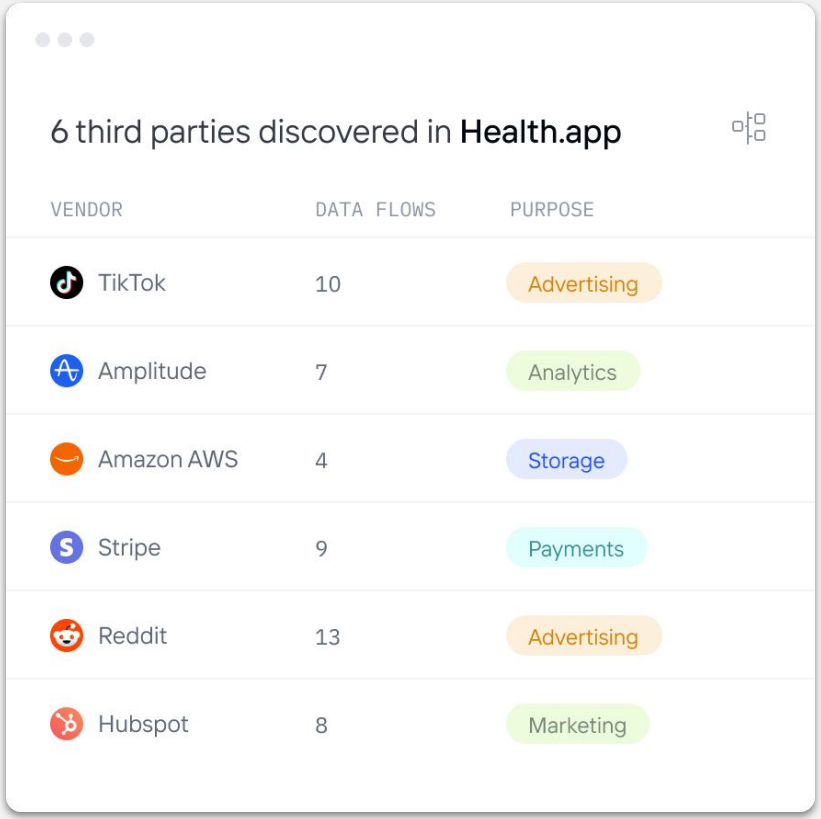


- ✔ Monitor permissions and data flows based on user activity
- ✔ Test consent banner visibility
- ✔ Flag SDKs not honoring consent

Visibility

Monitor all 3rd party activity in mobile apps

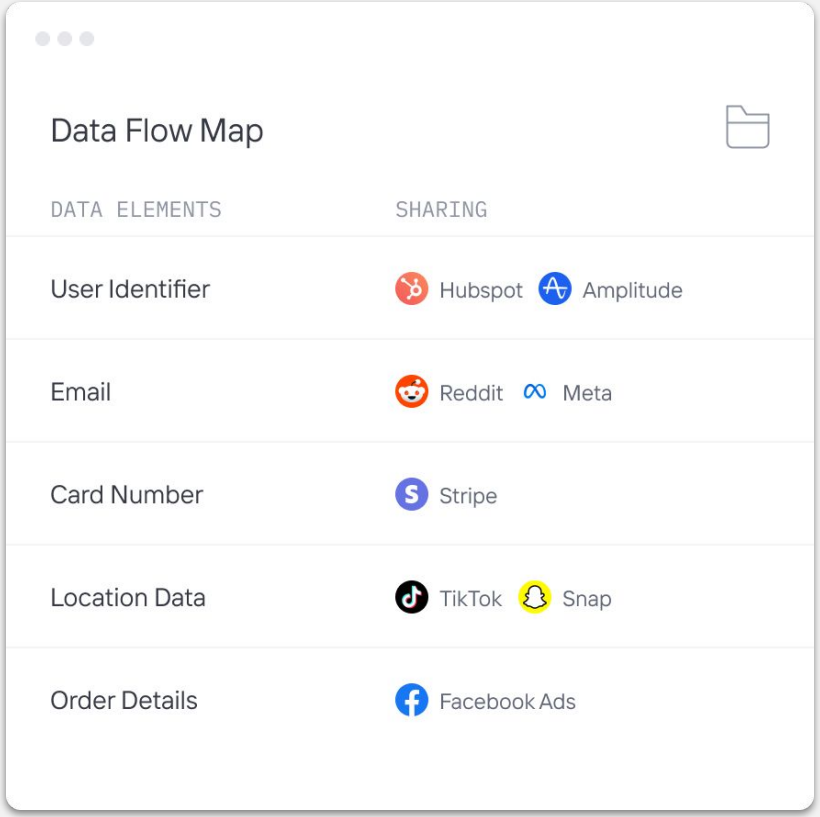
- Discover all user permissions and third-party SDKs in each app
- See which consent actions trigger which SDKs
- Identify each 3rd party call to see data shared and enable quick remediation
- Get full visibility by simulating user journey pre and post login



Data Sharing Risk Discovery

Prevent accidental data sharing

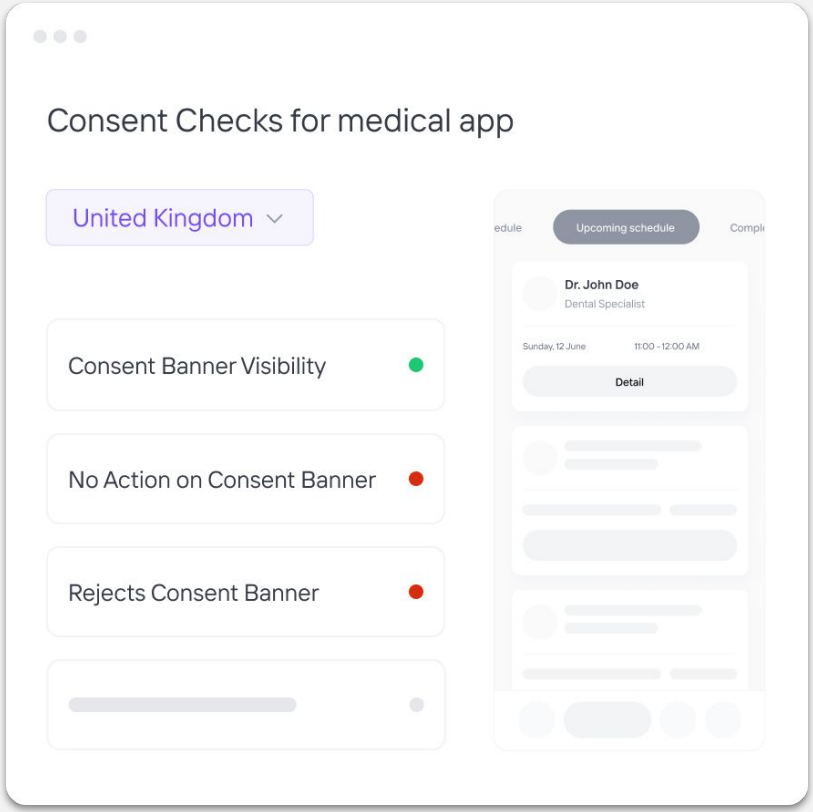
- Build data flow maps tracking data sent to 3rd parties
- Flag cross-border data flows
- Uncover sensitive data leaks and data sharing without consent



Consent Risk Discovery

Ensure banners and CMPs comply with all requirements

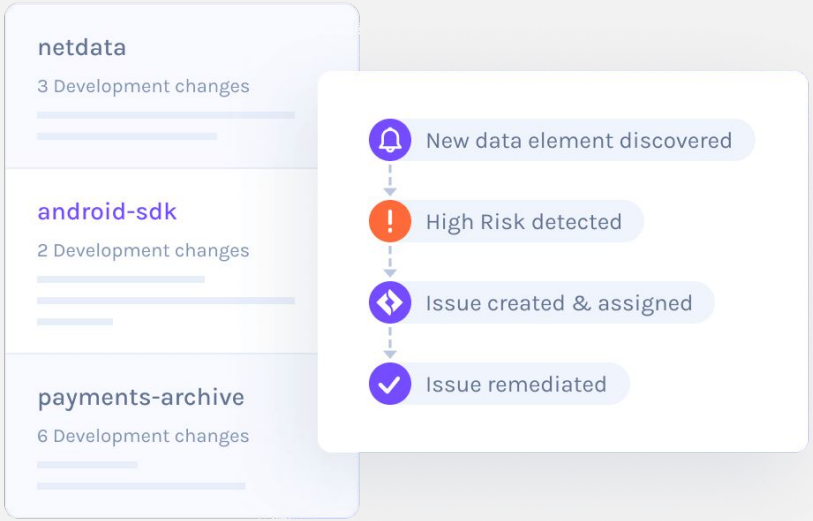
- Run 40+ checks for compliance with GDPR, CPRA, IAB's TCF, PIPEDA, and more
- Check that consent banners load properly in every app
- Flag privacy dark patterns



Risk Prevention

Implement programmatic SDK governance

- Continuously audit apps for compliance with your privacy policies
- Scan app's code to detect new data, SDKs, and risks after each app update
- Prevent risks by triggering reviews before unapproved SDKs or data flows go live



Demo

Questions

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://iapp.questionpro.com/t/ACtQeZ43Tj

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 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 will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting 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
or to obtain a copy of the slide presentation
please contact: **livewebconteam@iapp.org**