



A holistic approach to data privacy for the AI era

Thursday, 10 April

08:00–09:00 PST

11:00–12:00 EST

17:00–18:00 CET



Welcome and Introductions

Panelists



Nimrod Vax
Co-Founder and Chief
Product Officer
BigID



David Ray
CIPP/US, CIPM, CIPT
Chief Privacy Officer
BigID

Agenda

1. **Global View of AI Legislative Developments**
2. **Similarities between GDPR and EU AI Act**
3. **CCPA & Automated Decision Making**
4. **Operational Similarities between Privacy & AI**
5. **Fireside Chat with Nimrod Vax**
6. **Join BigID at the IAPP GPS in April!**

Where do we stand in 2025



US:
AI Executive Order

Canada:
AI & Data Act, June
2022 - reduce risks and
increase transparency

China:
Draft AI Regulation

European Union:
Comprehensive AI Act
AI Liability Directive

Singapore:
AI Verify - toolkit to
ensure compliance with AI
ethics

Brazil:
Comprehensive AI Bill

Jurisdictions in focus

Argentina	China	Israel	Singapore
Australia	Colombia	Japan	South Korea
Bangladesh	Egypt	Mauritius	Taiwan
Brazil	EU	New Zealand	United Arab Emirates
Canada	India	Peru	U.K.
Chile	Indonesia	Saudi Arabia	U.S.

Key AI Laws / Frameworks to be aware of as a privacy professional:

1. **EU AI Act** - set the tone for AI laws by establishing a risk-based framework that prioritizes transparency, accountability, and ethical AI development. Its alignment with the GDPR underscores the importance of integrating privacy protections into AI systems.
2. **Australian Government 2023 AI Framework** - stricter regulation of automated decision making and profiling. Emphasizes privacy by design and compliance with existing privacy laws.
3. **Multiple Californian AI Laws**, including laws requiring transparency of datasets used to train models and mandating disclosures of AI-created content used for certain defined purposes.
4. **Colorado Artificial Intelligence Act** - aims to protect individuals from risks associated with algorithmic discrimination and requires AI assessments
5. **New York City Local Law 144** - requires employers who use AI for hiring to subject AI systems to bias audits regularly.

The GDPR and EU AI Act share a common foundation in the following:

1. **Risk-Based Approach:** Both use a risk-tiered framework. GDPR focuses on high-risk processing, while the EU AI Act categorizes AI systems based on risk levels.
2. **Fundamental Rights Protection:** Both aim to safeguard fundamental rights, privacy and data protection of individuals in the EU.
3. **Transparency Requirements:** GDPR mandates transparency in data processing, while the EU AI Act requires transparency in AI system operations.
4. **Accountability and Governance:** Both result in organizations having to implement compliance programs, conduct assessments and ensure appropriate oversight.

- Adds the right to opt-out of Automated Decision Making Technology (ADMT).
- Scope includes businesses that:
 - Make significant decisions using ADMT.
 - Use ADMT for extensive profiling.
- Opt-out via cookie banner alone is not considered compliant.
- A consumer may not be asked to opt-in for one year following an opt-out.
- Notice and consent must occur “pre-use”, ideally at the point of collection.
- A new access right to learn about why and how ADMT is used (generally) and how it was used to make a decision about this consumer (specifically).

1. Inventory / Data Mapping

- Organizations need to be able to identify AI systems, what data was used for training those systems, and what personal information the AI systems use.
- Not all AI is generative, and all uses of AI should be documented.
- Definition of an AI system: **Models + data + use.**

2. Data Minimization

- As required under privacy laws, companies must limit the collection of personal information by AI to what is truly necessary for its intended purpose.
- Personal information used by AI should be kept only as long as needed.
- Stale data in AI not only creates security and privacy risk, but also affects the quality of AI results.

3. Data Subject Rights

- In some cases, individuals have (or will have) the right to access how AI was used to make decisions that affect them.
- Other rights, such as correction and deletion also apply to personal information used for AI.

4. **AI Assessments**

- Similar to privacy laws, assessments of AI systems must be conducted for privacy, security, and bias risks prior to deployment.

5. **Consent**

- Individuals must be able to opt-out of automated decision making in many jurisdictions.
- Automated decision making = decision making without human intervention.

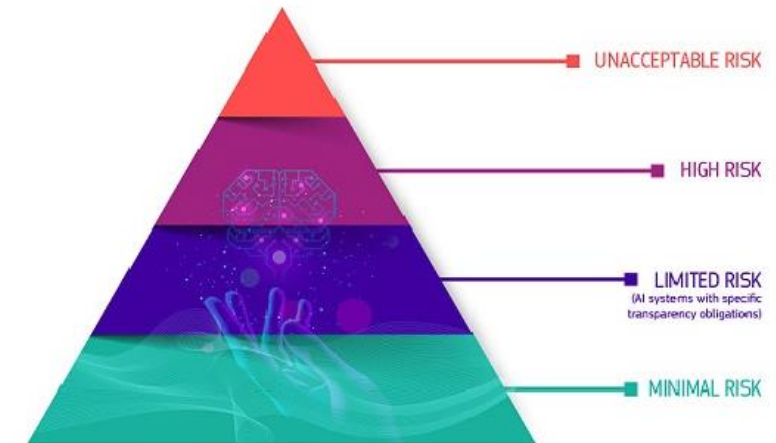
6. **Security Controls**

- Strong technical and organizational controls need to be implemented to protect data processed by AI systems.
- Prompt injection and other new attack vectors increase the risk of inadvertent exposure.

7. **Contractual Requirements**

- Vendor and customer agreements
- Notification requirements and optionality

1. **AI Governance Committee** made up of cross-functional stakeholders
2. Leverage general **frameworks** to define program controls:
 - NIST AI Risk Management Framework (AI RMF)
 - ISO 42001 Standard (Artificial Intelligence Management System)
3. Defining permitted and restricted use cases, aligned with a recognized **risk-tiering** framework.
 - a. For example, the EU AI Act defines 4 risk classifications: minimal, limited, high, and unacceptable (see image)
4. Operational tasks, including defining implementing **controls**; creating **policies**, standards and training; and completing AI **assessments** prior to launches



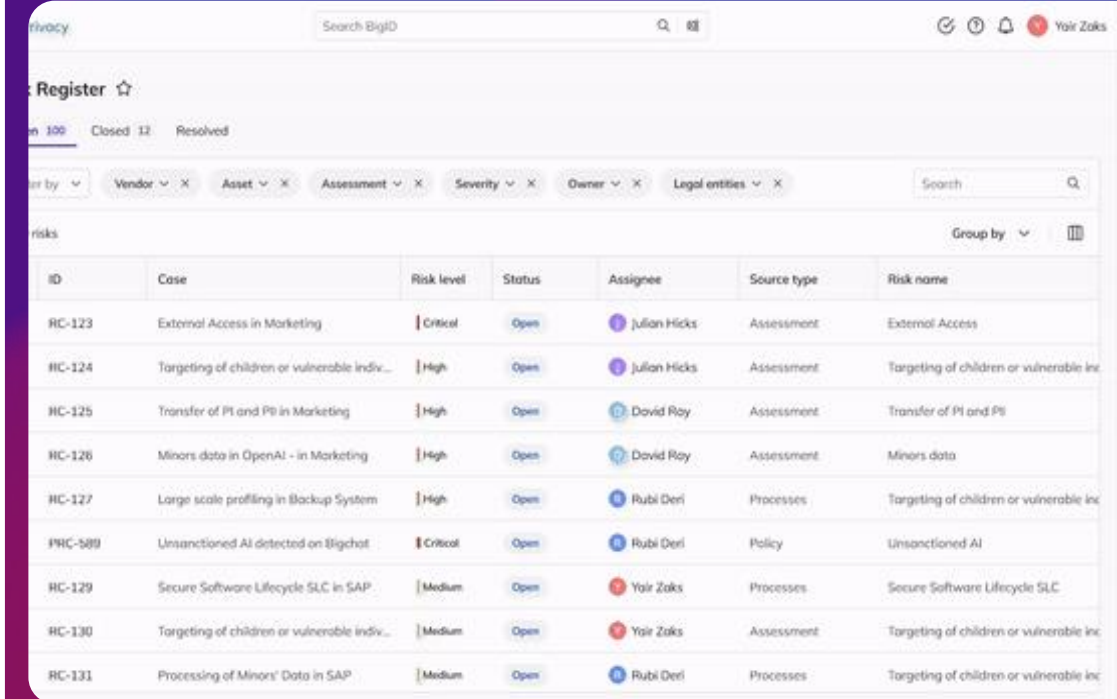
Data as a Foundation

Privacy and AI governance both start with data as their foundation.

Need to know your data

Robust AI governance programs should contain the following activities:

- Inventory of all AI and non-AI assets
- Risk management practices, which include an ability to identify, assess and track risks in a risk register
- Data maps
- Remediation processes
- Governance (expanded on in the following slide)



The screenshot displays the BigID privacy risk register interface. At the top, there is a search bar labeled "Search BigID" and a user profile for "Yair Zaks". Below the search bar, there are tabs for "Open 100", "Closed 12", and "Resolved". A filter bar allows users to filter by "Vendor", "Asset", "Assessment", "Severity", "Owner", and "Legal entities". A "Group by" dropdown is also present. The main table lists risks with the following columns: ID, Case, Risk level, Status, Assignee, Source type, and Risk name. The table contains 10 rows of data.

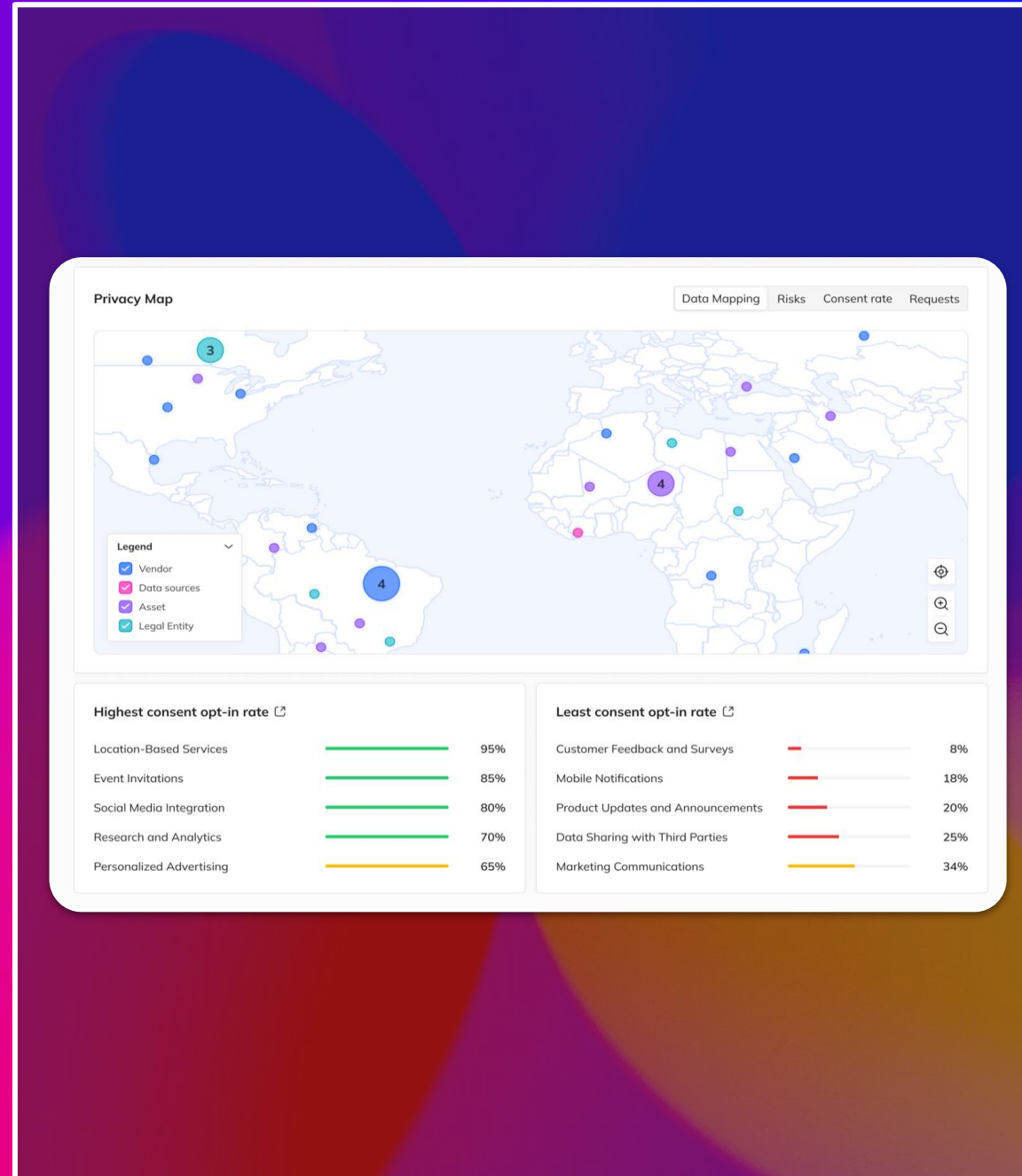
ID	Case	Risk level	Status	Assignee	Source type	Risk name
HC-123	External Access in Marketing	Critical	Open	Julian Hicks	Assessment	External Access
HC-124	Targeting of children or vulnerable indiv...	High	Open	Julian Hicks	Assessment	Targeting of children or vulnerable inc
HC-125	Transfer of PI and PP in Marketing	High	Open	David Roy	Assessment	Transfer of PI and PP
HC-126	Minors data in OpenAI - in Marketing	High	Open	David Roy	Assessment	Minors data
HC-127	Large scale profiling in Backup System	High	Open	Rubi Deri	Processes	Targeting of children or vulnerable inc
PRC-589	Unsanctioned AI detected on Bigchat	Critical	Open	Rubi Deri	Policy	Unsanctioned AI
HC-129	Secure Software Lifecycle SLC in SAP	Medium	Open	Yair Zaks	Processes	Secure Software Lifecycle SLC
HC-130	Targeting of children or vulnerable indiv...	Medium	Open	Yair Zaks	Assessment	Targeting of children or vulnerable inc
HC-131	Processing of Minors' Data in SAP	Medium	Open	Rubi Deri	Processes	Targeting of children or vulnerable inc



Breaking Down the Silos Between Privacy & Security

Privacy and security teams must work together for AI governance:

- **AI Governance Committee:** A cross-functional team should collaborate to ensure that use of AI aligns with privacy, security, data governance and other compliance and ethical standards.
- **Embedding AI governance into existing privacy and security programs:** Rather than treating AI as a separate compliance issue, integrating AI oversight into existing governance structures (e.g., assessments and risk management) enhances accountability and efficiency.
- **Aligning data risk with AI use risk:** AI adds a new layer that isn't specifically privacy or security, but relates to how the data is used and whether it's permissible and/or requires further steps based on AI laws.



Data Driven Privacy & AI Risk Assessment

Automate risk Assessments in privacy, AI, data sharing etc

- Power risk assessments with discovered data dynamically
- Supplement with customizable survey questionnaire
- AI assisted to aid DPO & CPO

The screenshot displays the 'AI Impact Assessment' interface, which is part of the 'Assessments / AI Impact Assessment' section. The interface is divided into several sections:

- Header:** 'Assessments / AI Impact Assessment' and 'AI Impact Assessment Under review'. It includes a progress bar with 90% completion, 24 items, and 16 items completed. A 'Complete' button is visible.
- Navigation:** 'Overview', 'Assessment' (selected), 'Risk overview 0', and 'Activity Log'.
- 1.f - Assets being assessed for AI usage:** A section titled 'Select all assets that are involved' with a dropdown menu showing 'Okta' and 'Slack communication service'.
- 1.g - Processing activities being assessed for AI usage:** A section titled 'Select all processing activities involved' with a dropdown menu showing 'Slack AI process'.
- 1.h - Vendors being assessed for AI usage:** A section titled 'Select all vendors involved' with a dropdown menu showing 'Slack'.
- 1.c - What are the Asset's PII's?** A section titled 'Specify the PII's collected in this asset' with a dropdown menu showing 'Email' and 'Phone number'.
- Suggestions for 1.c:** A sidebar on the right titled 'Suggestions for 1.c' with a close button. It contains three suggestions: 'Email Bank account Phone number' (with a blue dot next to 'Bank account'), 'Streamlined "PIIs" from AWS' (with a link to 'AWS'), and 'Based on AWS assessment 2023'. Each suggestion has an 'Add answer' button.

Provide employees & consumers AI preference self-service

- GDPR & CCPA compliant DSR requests with Identity verification
- Capture privacy and AI consent around data usage
- Manage & track customer & employee requests
- Integrate into your ticketing systems

The screenshot displays the 'Requests' management interface. At the top, there are tabs for 'Open Requests 19', 'My Requests 1', and 'Closed Requests 9'. Below these are filter buttons for 'Site', 'Brand', 'Regulation', 'Stage', 'Compliance Progress', 'Type', and 'Status: Open'. A search bar is located on the right. The main table lists 19 requests with columns for Request ID, Requester ID, Compliance Pr..., Type, Stage, Profile, Regulation, Regulatory P..., Actual Days, Due in (Days), and Owner. The table shows various request statuses like 'On Time' and 'Overdue' across different regulations like GDPR and CPRA.

Request ID	Requester ID	Compliance Pr...	Type	Stage	Profile	Regulation	Regulatory P...	Actual Days	Due in (Days)	Owner
2400320856	poolof@bigid.com	On Time	Preferences	Confirm	Consumer	Non-regulated	30	1	29	Select...
7670059523	pfomon85@gmail.com	On Time	View	Confirm	Customer	GDPR	30	1	29	Select...
4433498868	dannyw+aywodefai@bigid.com	On Time	View	Review	Consumer	CPRA	45	2	43	Select...
2786701336	andreas@bigid.com	Overdue	View	Collect	Consumer	GDPR	30	58	-28	Select...
5471398841	bjt@bizstart.com	Overdue	View	Collect	Consumer	Non-regulated	30	59	-29	Select...
9782499374	dona.corkery@outlook.com	Overdue	View	Review	Current Employee	Non-regulated	30	81	-51	Select...
4381331427	leeanne.q									
4506783114	ozzie.schr									
9038447212	valeri.kos									
3504788391	brigitte.hc									
2579891634	clayton.re									
3850527500	sharon.b									

Below the table, there is a 'Workflow Customization' section with a 'Delete request workflow' button. A workflow diagram shows steps: Confirm, Verify, Collect, Review, Approve, Update, Complete. The 'Approve' step is currently selected. Below this is an 'Emails' section titled 'Close Request (Manual - Request Termination)' with a table for configuring reasons and emails for manually closing requests.

Names	Triggers	Last Update	Enabled
Individual abort	Request closed manually	-	⋮
Other	Request closed manually	-	⋮
Testing	Request closed manually	-	⋮

At the bottom, there is an 'API Triggers' section with a table for setting events to trigger an API call.

Action Names	Type	When Triggered	Last Update	Enabled
No API calls added				

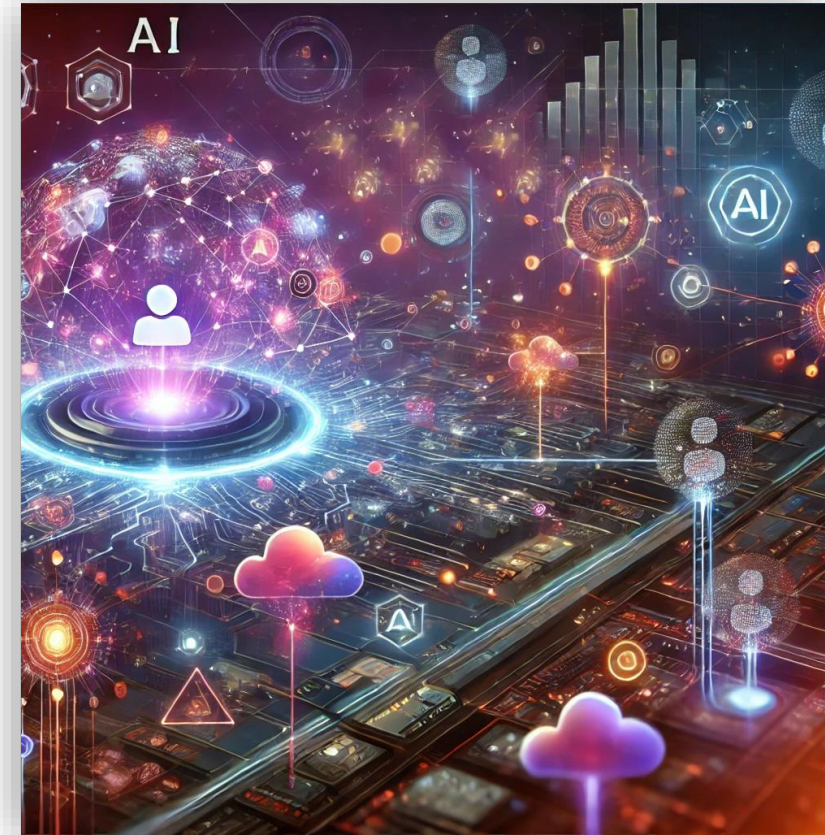
Fireside Chat: An Industry Veteran's Perspective

What's Next? 2025 AI Predictions

1. **A shift to the states for AI regulation in the US.**
2. **New / shifting roles (e.g., Chief AI Officer, Chief Trust Officer).**
3. **More or less global regulatory alignment?**
4. **Expanding privacy rules.**
5. **Increased focus on AI certifications (e.g., NIST RMF, ISO 42001)**
6. **Agentic AI privacy operations**

Augment the privacy operations team to multiply effectiveness while maintaining a person in the loop:

- Connect to your data infrastructure
- Identify AI and Privacy risks
- Initiate Risk Assessments
- Semantically index your Privacy and Data Policies
- Suggest the appropriate AI/PIA template
- Suggest responses to assessment questionnaire
- Assign questions with suggested answers to owners
- Follow up and report on progress
- Continuous compliance



Generated by ChatGPT



Universal Consent for Privacy in Prompts

Implement universal consent across AI Agents and Bots







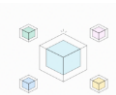











- Automatically identify sharing of personal information in chats and AI applications
- Prompt the user for consent - if needed
- sync across Web & mobile

The screenshot displays the 'Consent Management' interface in the BigID Privacy application. It features a table with 12 updates, showing user consent status for various topics and collection points. The table includes columns for User ID, Identifier, Topic, Collection point, New Value, Updated Progress, and Target Systems. The interface also includes a search bar, filter options, and a sidebar with navigation icons.

D	User ID	Identifier	Topic	Collection point	New Value	Updated Progress	Target Systems
	10102	nmichaeli+5@bigid.com	Special Offers	1	Opt In	100%	HubSpot
	10102	nmichaeli+5@bigid.com	Product Updates	1	Opt In	100%	Bizstart Int
	10100	example@bigid.com	Special Offers	1	Opt In	0%	HubSpot
	10100	example@bigid.com	Product Updates	1	Opt In	50%	Bizstart Int
	10101	example+1@bigid.com	Special Offers	1	Opt In	0%	HubSpot
	10101	example+1@bigid.com	Product Updates	1	Opt In	50%	Bizstart Int
	10100	example@bigid.com	Special Offers	1	Opt In	0%	HubSpot
	10100	example@bigid.com	Product Updates	1	Opt In	50%	Bizstart Int
	10100	example@bigid.com	Special Offers	1	Opt In	0%	HubSpot
	10100	example@bigid.com	Product Updates	1	Opt In	0%	Mailchimp
	10100	example@bigid.com	Special Offers	1	Opt In	0%	HubSpot
	10100	example@bigid.com	Product Updates	1	Opt In	0%	Mailchimp

About BigID

BigID's Integrated Privacy & Compliance Suite

 <p>Scan 100s of Data Sources</p>	 <p>AI Powered PII Classification</p>	 <p>Map PII Data By Legal Entity</p>	 <p>Data Driven Assessments</p>	 <p>Simplified RoPA & Flow</p>	 <p>Vendor Management</p>
 <p>DSR Automation</p>	 <p>Custom Data Subject Profiles</p>	 <p>Privacy Pref Portal</p>	 <p>Cookie Management</p>	 <p>Universal Consent</p>	 <p>Privacy Exec Dashboarding</p>
 <p>Regulatory Risk Register</p>	 <p>Compliance Dashboard</p>	 <p>Fix Compliance Violations</p>	 <p>DLM & Data Retention</p>	 <p>Retention Minimization</p>	 <p>Access Control & Governance</p>

BigID Is a Privacy and AI Leader:

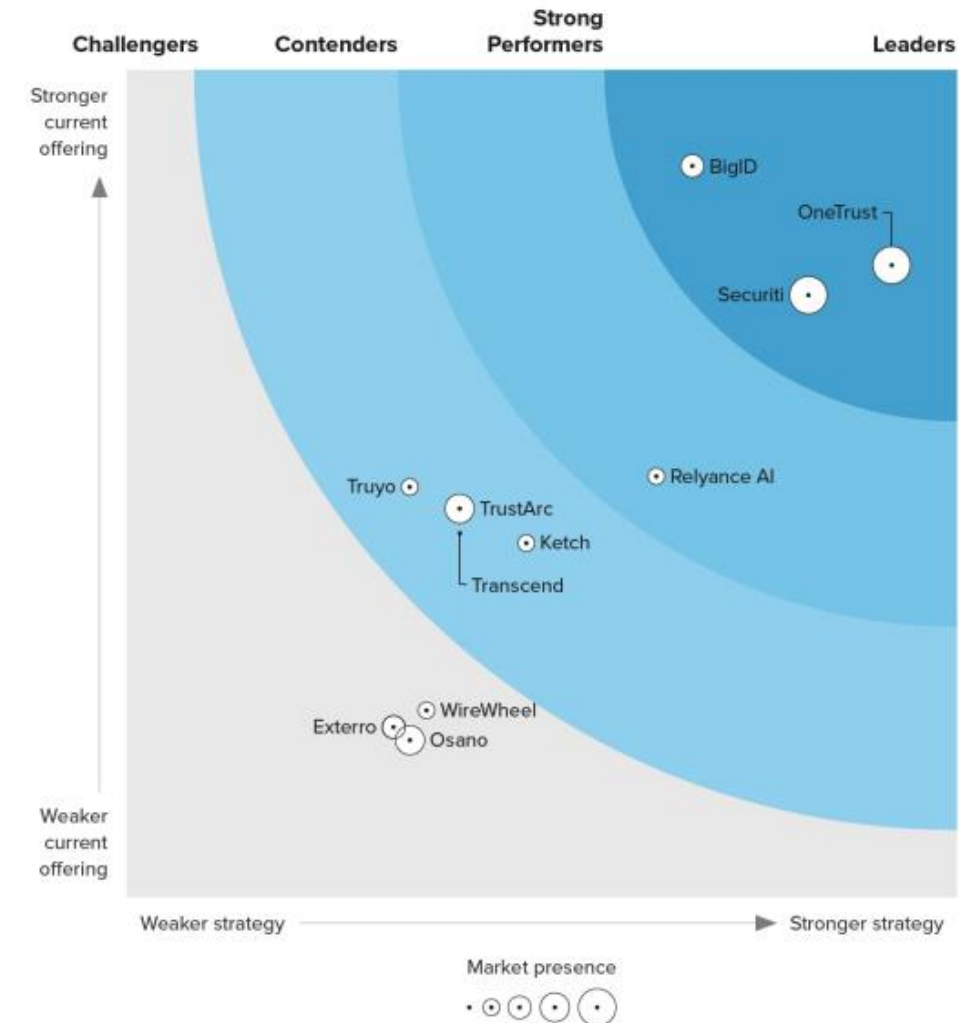
- Leader in Forrester Privacy Wave
- Leader in IDC Privacy Analysis
- Leader in GigaOM Privacy
- Only Privacy Suite with Data Minimization
- Newest & most Modern privacy suite
- Bridges Privacy with Security
- Bridges Privacy with Data & AI

Visit us at **IAPP Global Privacy Summit** booth #30

Figure 1

Forrester Wave™: Privacy Management Software, Q4 2023

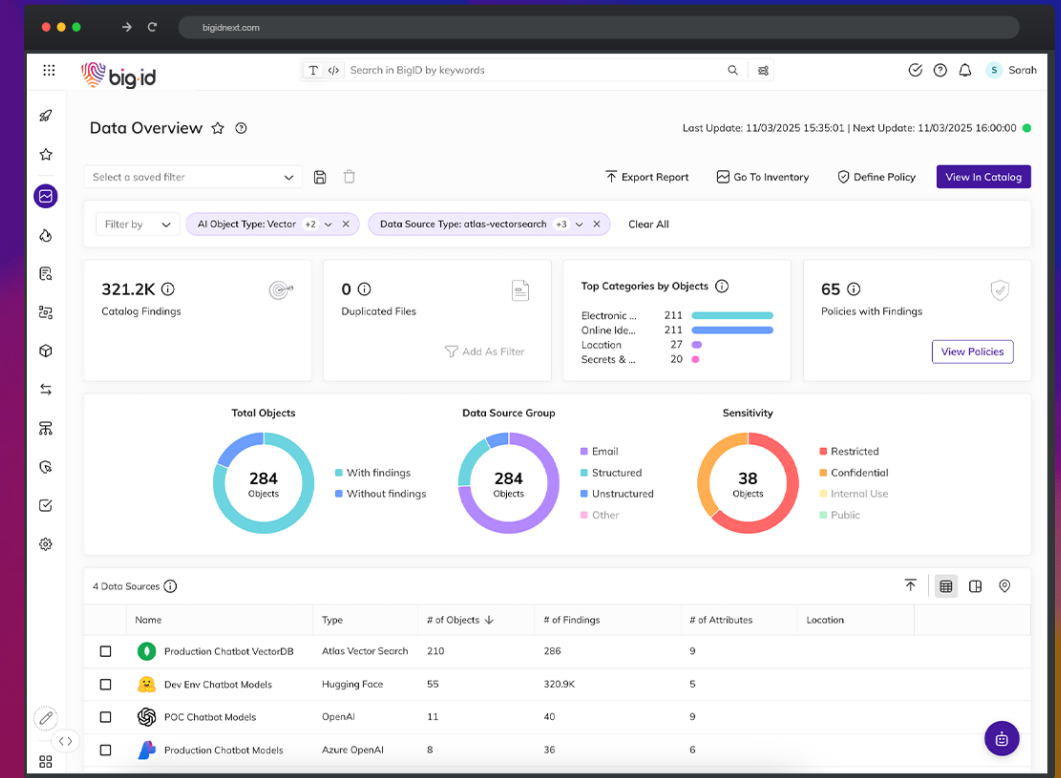
THE FORRESTER WAVE™ Privacy Management Software Q4 2023



iapp Meet BigID Next

Connecting the Dots in Data & AI

- Unified platform for data + AI visibility & control
- Addresses data & AI governance, security, privacy and compliance in one platform
- Built on a foundation of Know Your Data & AI
- With AI Powered Actions delivered as modular Apps on core
- AI augmentation spread across discovery, classification, inference, search and taking actions
- Bridges AI controls with genAI data



Questions and Answers

Panelists



Nimrod Vax
Co-Founder and Chief
Product Officer
BigID



David Ray
CIPP/US, CIPM, CIPT
Chief Privacy Officer
BigID

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/ACtQeZ5cKq>

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