iapp

The Crucial Role of Obtaining Valid Consent in the Era of AI Model Development

24 July 2024
08:00–09:00 PST
11:00-12:00 EST
17:00–18:00 CET

Agenda

Welcome and Introductions 03

Role of Data and AI 06

Regulatory Discussion 12

Best Practices 19

Essential Features of a Consent Management Tool 22

Conclusion and Q&A 24

© 2024 Exterro, Inc. All rights reserved.

Welcome and Introductions

Panelists

Fahad Diwan
JD, FIP, CIPP/C, CIPM

Director of Product Management & Marketing, Privacy & Data Governance
Exterro

Goli Mahdavi,
CIPP-US/E, AIGP

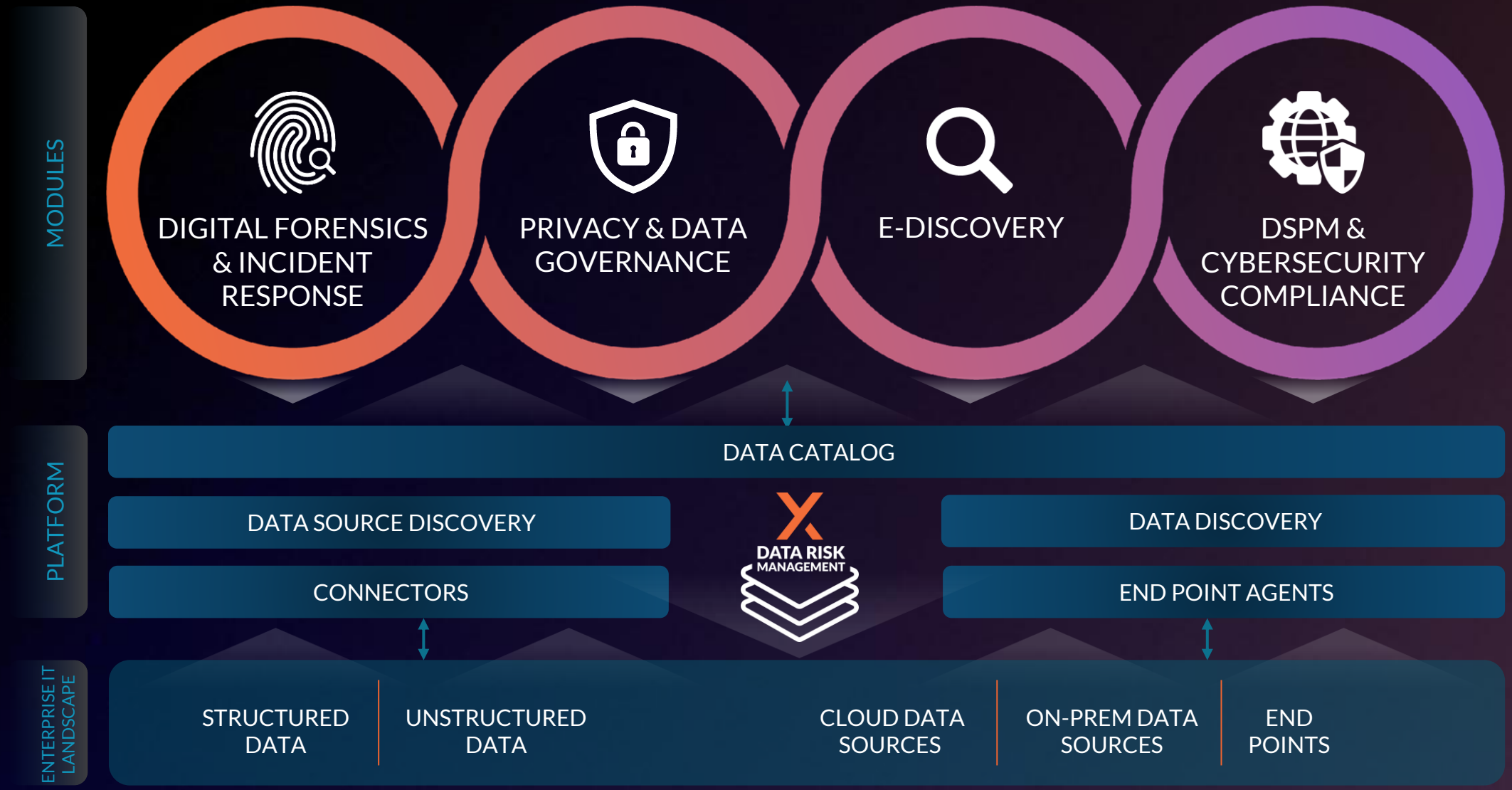
Counsel, Data Privacy and Cybersecurity,
Bryan Cave Leighton Paisner (BCLP)

Cristina Messerschmidt

Associate - Data Privacy & Security,
Baker McKenzie

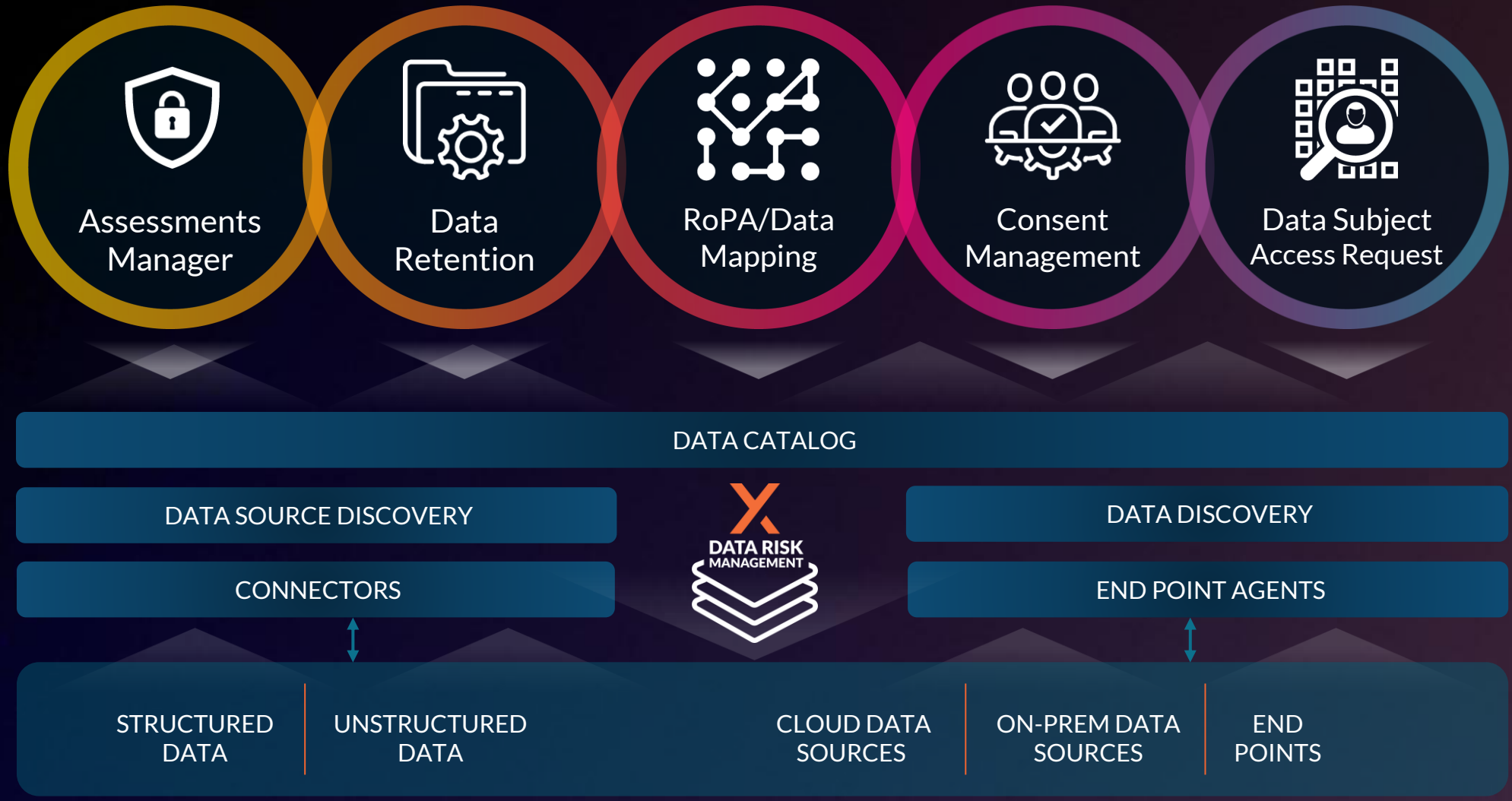
© 2024 Exterro, Inc. All rights reserved.

Exterro Data Risk Management Platform



© 2024 Exterro, Inc. All rights reserved.

Exterro Privacy and Data Governance Suite



© 2024 Exterro, Inc. All rights reserved.

Role of Data and AI

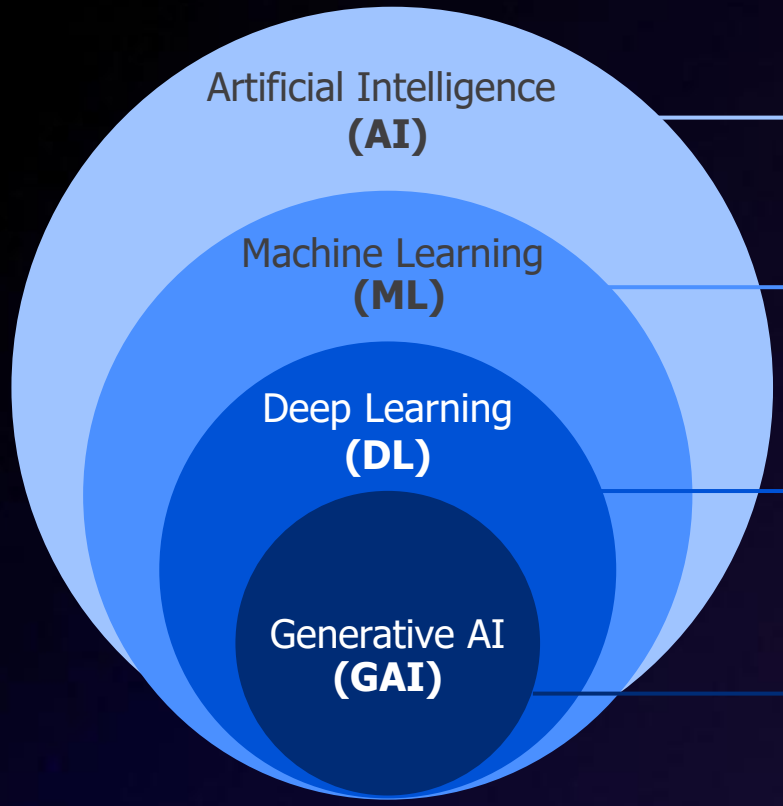
© 2024 Exterro, Inc. All rights reserved.

“Data Is the New Gold”

Modern AI and Its Dependency on Data

© 2024 Exterro, Inc. All rights reserved.

Artificial Intelligence: What is it?



Technology that processes data to produce information which augments human intelligence, perception and predictive abilities

The area of **AI** in which computer programs use certain methods to detect relationships and patterns in data

A type of **ML** technique based on artificial neural networks in which multiple layers of processing are used to extract progressively higher-level features from data

Generative AI is a collection of models and systems that can produce new text, images, video, audio, code and synthetic data

© 2024 Exterro, Inc. All rights reserved.

Large Language Model (LLM)

An AI system designed to understand and generate human-like text by learning from vast amounts of textual data.

It is trained in two steps:

1. **Pre-training**

   On vast datasets to learn grammar and facts and to predict the next word in a sentence by analyzing massive datasets containing diverse text sources.

2. **Fine-tuning**

   On specific datasets for targeted applications, improving contextual understanding and accuracy.

© 2024 Exterro, Inc. All rights reserved.

The Rise of Generative AI

Generative AI expected to:

Raise Global GDP by 7% in next 10 years

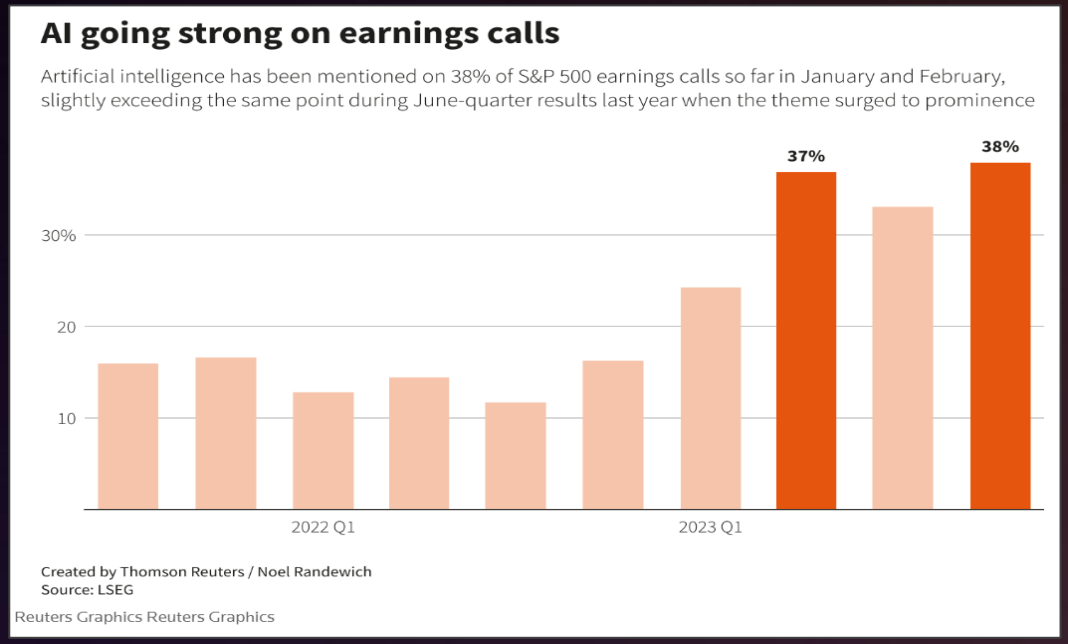
Source: Goldman Sachs

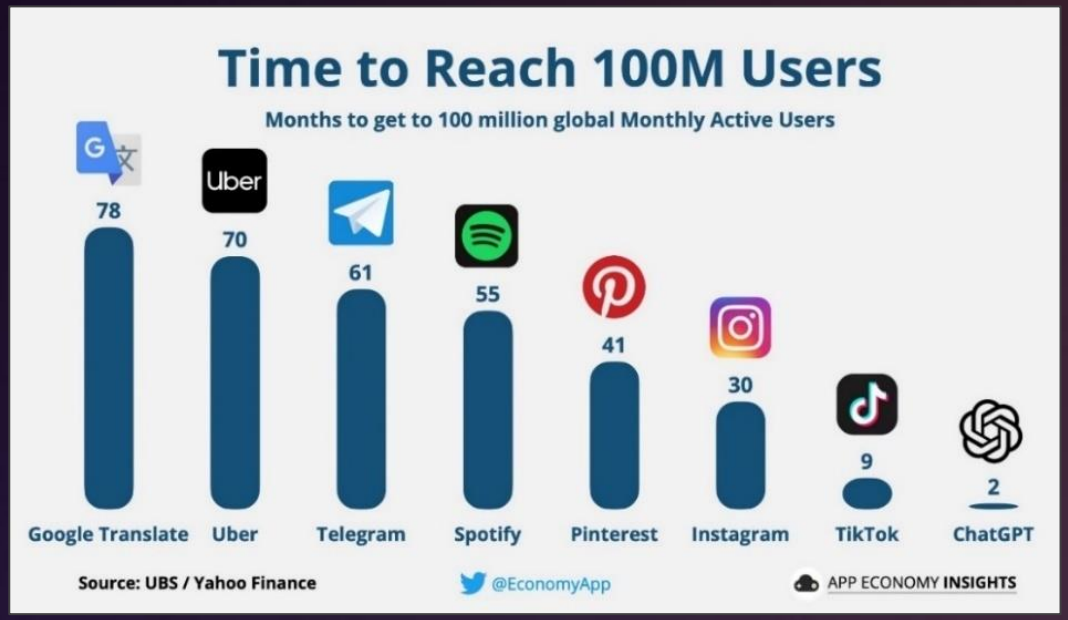
Add **$2.6-4.4 trillion** annually to economy

Source: McKinsey

Impact **10% of tasks** carried out daily by 80% of workers

Source: OpenAI/Upenn





© 2024 Exterro, Inc. All rights reserved.

Sources of Training Data

Public datasets

Essentially anything available online (copyrighted or not).

Private datasets

Collected by individuals or organizations for proprietary use, such as customer data.

User-generated content

Social media posts or reviews.

Custom data

Specific to an intended application, such as medical AI trained with a dataset of medical images.

Synthetic data

Generated using computer graphics or simulation techniques.

Generative AI content

Risks regarding training on content generated by generative AI.

© 2024 Exterro, Inc. All rights reserved.

Ethical vs. Responsible AI

- **Ethical AI** focuses on ethical guidelines and fundamental values – an initial focus on use of AI, what should the enterprise do regarding AI.
- **Responsible AI** focuses on ensuring that AI systems are consistent with governing principles such as fair, accountable, and transparent as well as broader goals such as environmental and social goals.

Technical

What **can** we do?

Legal

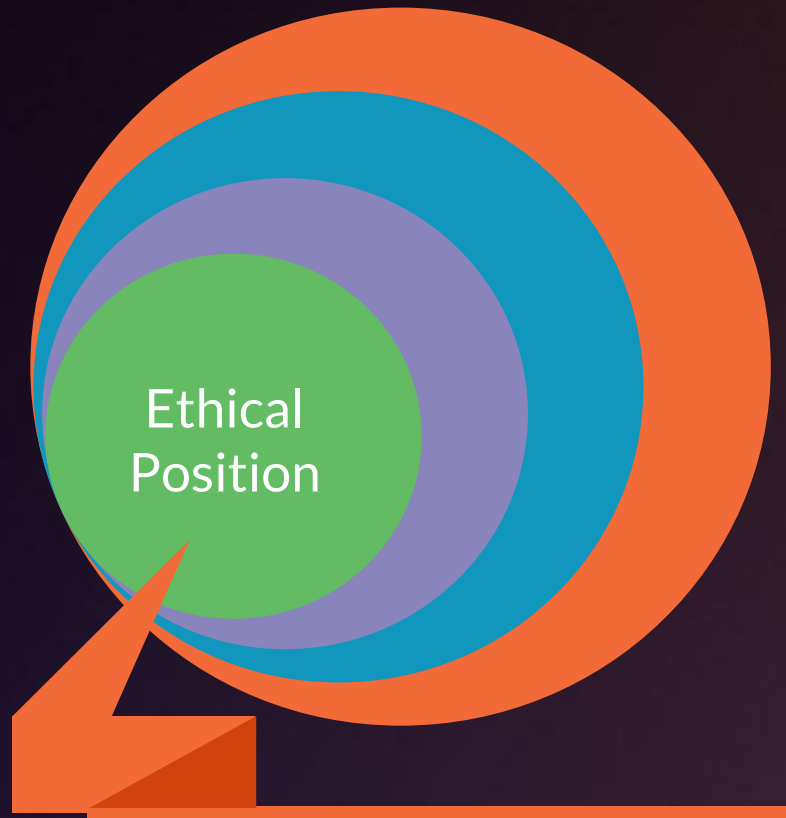
What **may** we do?

Desired

What do we **want to** do?

Ethical

What **should** we do?



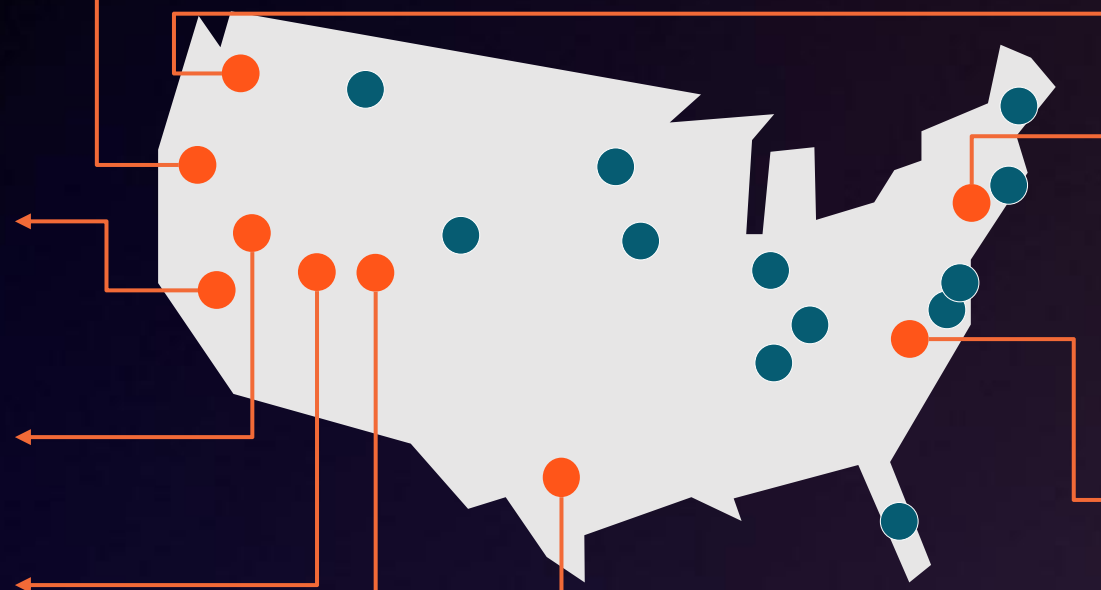
All of these issues overlap, but do not perfectly align. The goal of ethical controls should be to drive ethical decision making which considers all of these aspects in arriving at a balanced approach.

© 2024 Exterro, Inc. All rights reserved.

Regulatory Discussion

© 2024 Exterro, Inc. All rights reserved.

State Privacy Laws



* Pending laws in Delaware, Florida, Indiana, Iowa, Kentucky, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Rhode Island, and Tennessee.

© 2024 Exterro, Inc. All rights reserved.

“Secondary Uses” Consent Requirements

California Consumer Privacy Act (CCPA) as amended by the Consumer Privacy Rights Act (CPRA)	**Any time information is used in a manner that is inconsistent with what the “reasonable expectations” of the consumer, the business must obtain explicit consent for that use. (Sec. 7002(a)).**
Colorado Privacy Act (CPA)	A “secondary use” of personal information is any use that is different than the processing purposes disclosed to consumers at or before the time of collection. (Rule 6.08). If data is being used for secondary purposes, opt-in consent is needed before the processing activity takes place.
Connecticut Personal Data Privacy and Online Monitoring Act	Unless the controller obtains the consumer’s consent, the controller may not process personal data for purposes that are “neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed” as disclosed to the consumer.

© 2024 Exterro, Inc. All rights reserved.

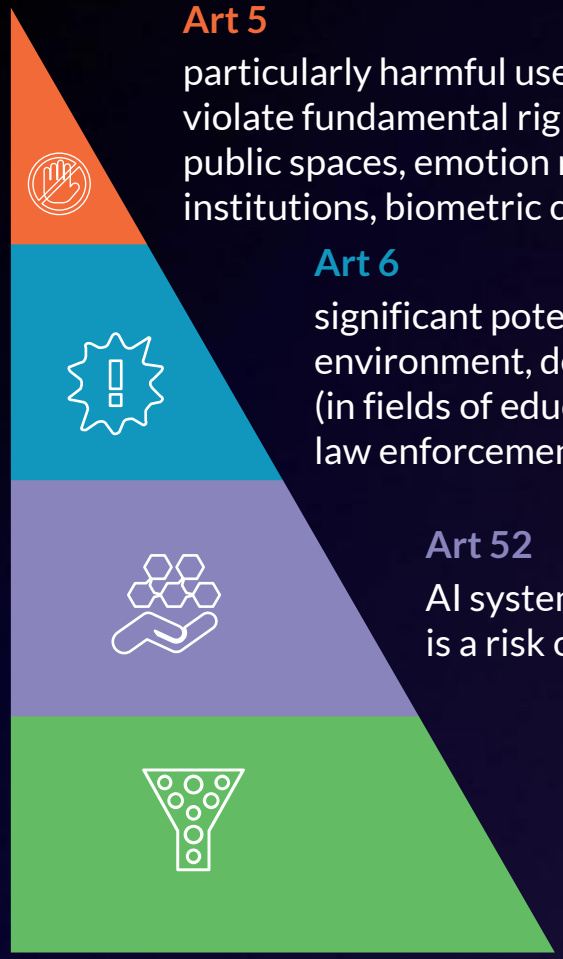
Next Gen AI Laws

- 400+ AI-related bills introduced in 2024
  - Transparency bills
  - Sector focused: employment, healthcare, housing, etc.
  - Broad AI bills
  - Miscellaneous
- The Colorado Artificial Intelligence Act (SB205)
  - Effective February 1, 2026
  - Notice Requirements
- The Utah AI Policy Act

© 2024 Exterro, Inc. All rights reserved.

EU AI Act - What are the risk categories?

The EU AI Act targets regulation to assigned risk categories. It identifies four specific levels of risk, as well as risks specific to general purpose models*:



Unacceptable risk: prohibited

Art 5

particularly harmful use of AI that contravene EU values because they violate fundamental rights, such as social scoring, facial recognition in public spaces, emotion recognition in the workplace and education institutions, biometric categorization using sensitive data

High risk: Conformity Assessment

Art 6

significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law - listed in Annex III (in fields of education*, employment*, critical infrastructure, law enforcement,...) and Annex II (AI as a medical device**,...)

Limited risk: Transparency

Art 52

AI systems interacting with natural persons where there is a risk of manipulation (e.g., chat bots**), deep fakes

Minimal risk: Voluntary code of conduct

Art 69

Spam filters, video games

Medical devices (**) : covered by Annex III to the AI Act, will qualify as high-risk (when subject to conformity assessment)

Employment and Education : see Annex III to the Data Act, e.g. AI systems intended to be used for recruitment or selection of natural persons

General purpose AI (*) : the AI Act considers **systemic risks** which could arise from **general-purpose AI models, including large generative AI models**

© 2024 Exterro, Inc. All rights reserved.

JOINT STATEMENT ON ENFORCEMENT EFFORTS AGAINST DISCRIMINATION AND BIAS IN AUTOMATED SYSTEMS

Rohit Chopra, Director of the Consumer Financial Protection Bureau,
Kristen Clarke, Assistant Attorney General for the Justice Department's Civil Rights Division,
Charlotte A. Burrows, Chair of the Equal Employment Opportunity Commission, and
Lina M. Khan, Chair of the Federal Trade Commission
issued the following joint statement about enforcement efforts to protect the public from bias in automated systems and artificial intelligence:

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

© 2024 Exterro, Inc. All rights reserved.

The A.I. tools that firms use to set prices for everything from laundry detergent to bowling lane reservations can facilitate collusive behavior that unfairly inflates prices . . . . The FTC is well equipped with legal jurisdiction to handle the issues brought to the fore by the rapidly developing A.I. sector, including collusion, monopolization, mergers, price discrimination, and unfair methods of competition. . . .

Enforcers have the dual responsibility of watching out for the dangers posed by new A.I. technologies while promoting the fair competition needed to ensure the market for these technologies develops lawfully.

Lina Khan, FTC Chair, May 2023

© 2024 Exterro, Inc. All rights reserved.

Best Practices

© 2024 Exterro, Inc. All rights reserved.

Organizational vs. Individual Consent

Contractual rights to use data (including personal data and/or confidential information)

- Training AI tools
- Use of AI tools

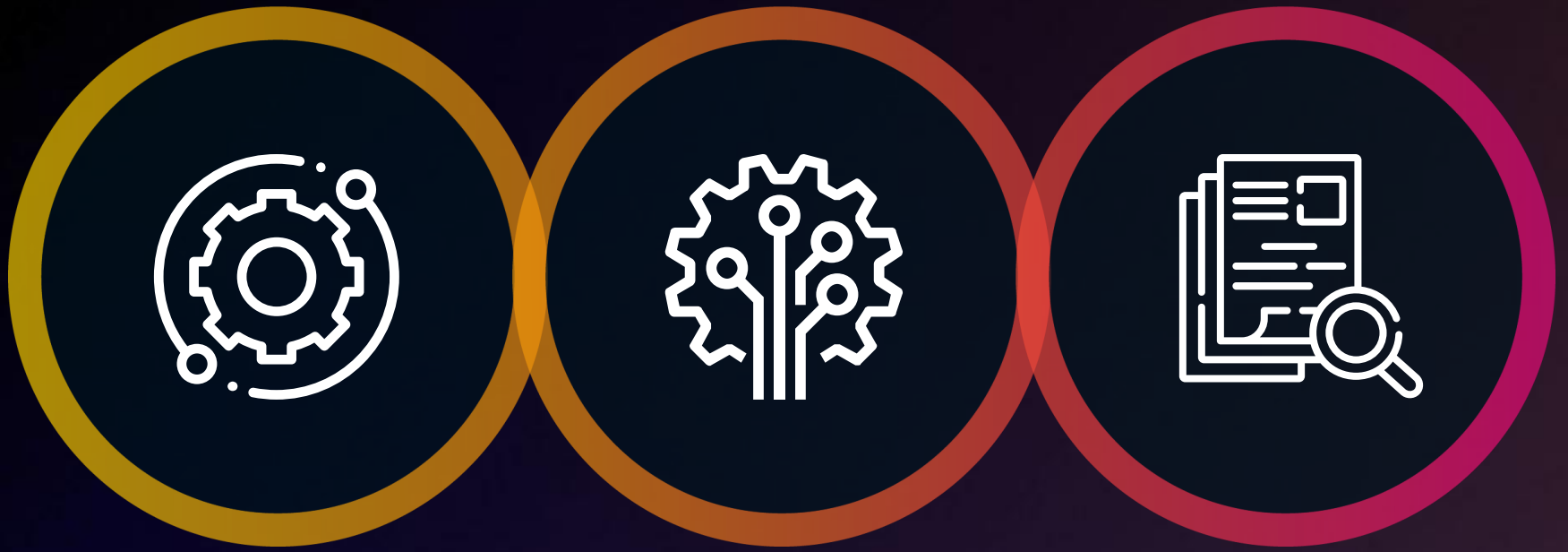
Individual rights to use data

- Notice vs. consent

Explicit or implicit consent?

© 2024 Exterro, Inc. All rights reserved.

Contract Formation & Amendment– Key Issues



Material updates to online terms require consent

FTC Guidance - *AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*

"Browsewrap/"Clickwrap"/ Sign-in wrap"

© 2024 Exterro, Inc. All rights reserved.

Essential Features of a Consent Management Tool

© 2024 Exterro, Inc. All rights reserved.

Essential Features of a Consent Management Tool

- Cookie Consent
- Universal Consent
- Synchronized
- Integration with Record of Processing Activities solution

© 2024 Exterro, Inc. All rights reserved.

Conclusion and Q&A

© 2024 Exterro, Inc. All rights reserved.

Questions?

Panelists

Fahad Diwan
JD, FIP, CIPP/C, CIPM

Director of Product Management & Marketing, Privacy & Data Governance
Exterro

Goli Mahdavi,
CIPP-US/E, AIGP

Counsel, Data Privacy and Cybersecurity,
Bryan Cave Leighton Paisner (BCLP)

Cristina Messerschmidt

Associate - Data Privacy & Security,
Baker McKenzie

© 2024 Exterro, Inc. All rights reserved.

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/ACtQeZ3CNK

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