May 9, 2024

Navigating the Complexities of AI Governance in Our Rapidly Evolving Technological Landscape

Lauren Misztal
SVP, General Counsel
Clario

Fran Faircloth
Partner, Data Privacy & Cybersecurity
Ropes & Gray LLP

Privacy+ Security Forum

Speakers

Lauren Misztal

SVP,
General Counsel
Clario

Fran Faircloth

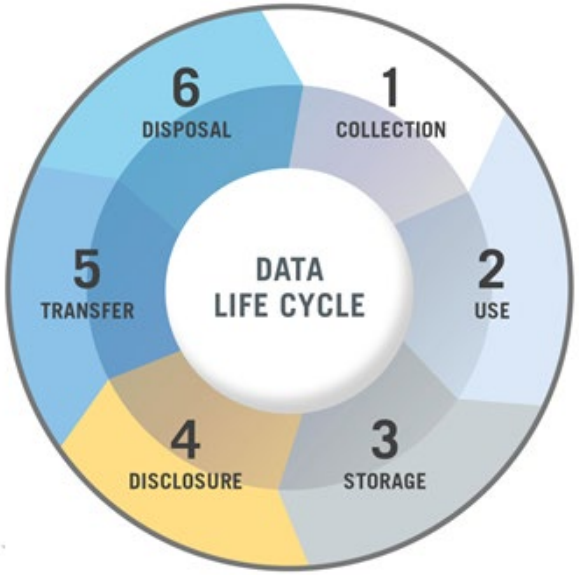
Partner, Data Privacy & Cybersecurity
Ropes & Gray LLP

Data: Generation, Collection, & Processing

Privacy+ Security Forum

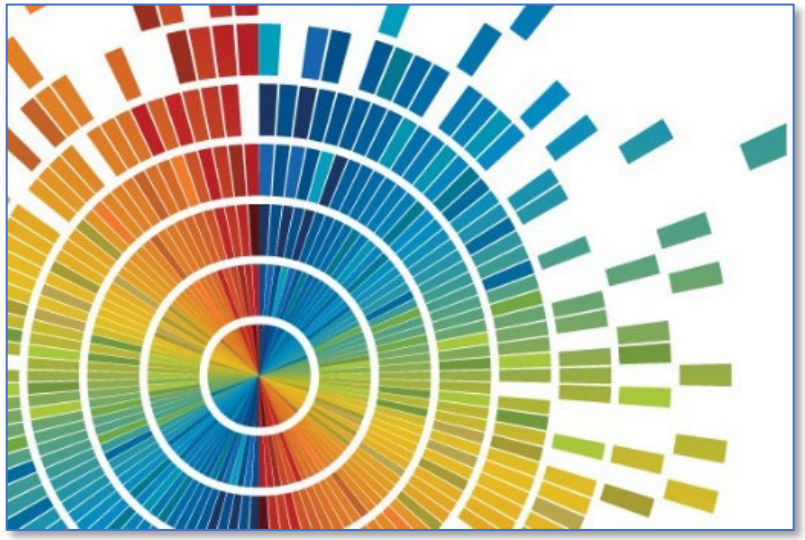
TRADITIONAL DATA LIFECYCLE

- Focused on tracking a relatively linear path of information from the point of collection through disposal
- In any context, data privacy and upstream contractual obligations must be kept in mind



TODAY'S BIG DATA LIFECYCLE

- Big data requires specific considerations of how data is compiled and consolidated, and how it is mined and analyzed
- The volume and variety of big data sets pose particular challenges

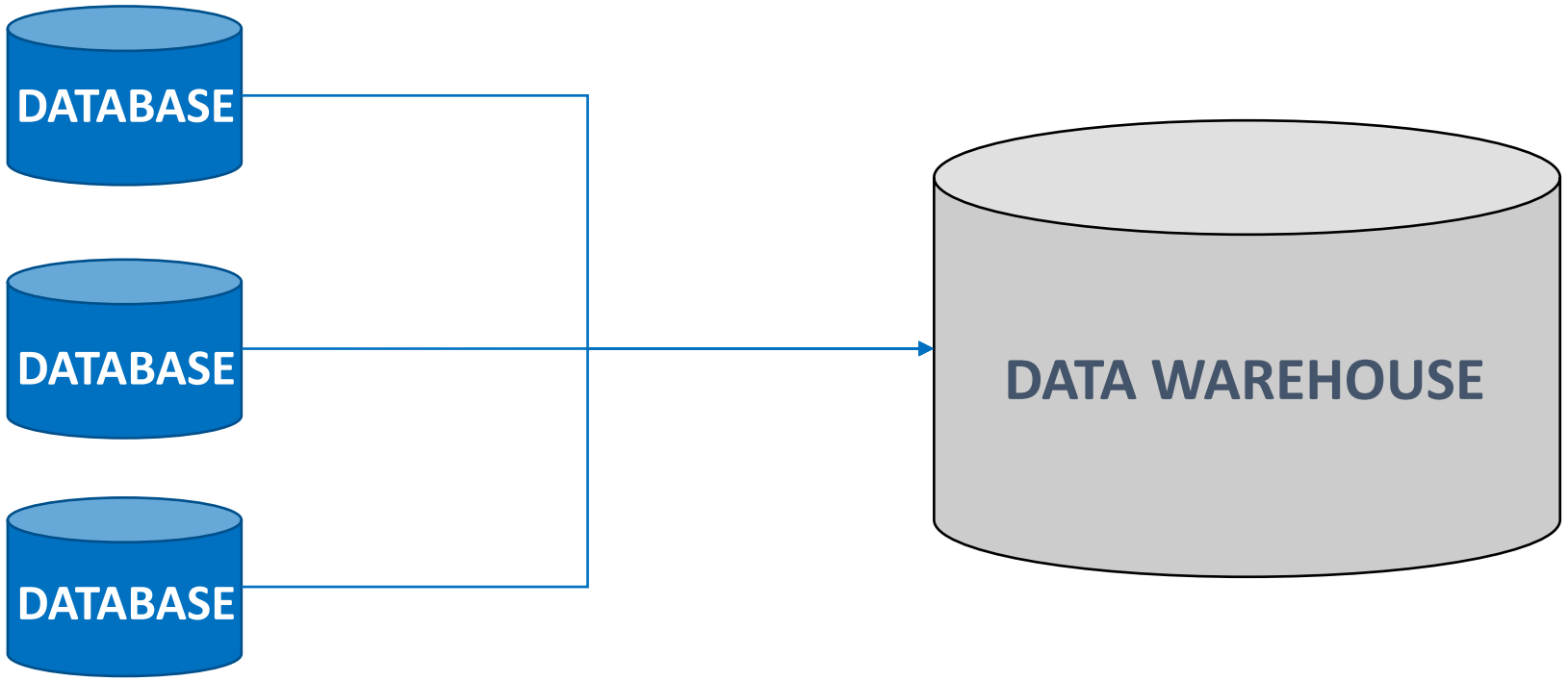


Data: Generation, Collection, & Processing

Privacy+ Security Forum

HOW WE THINK ABOUT DATA FLOWS

Transferring data from different databases to a single, central repository, a.k.a., a **data warehouse**

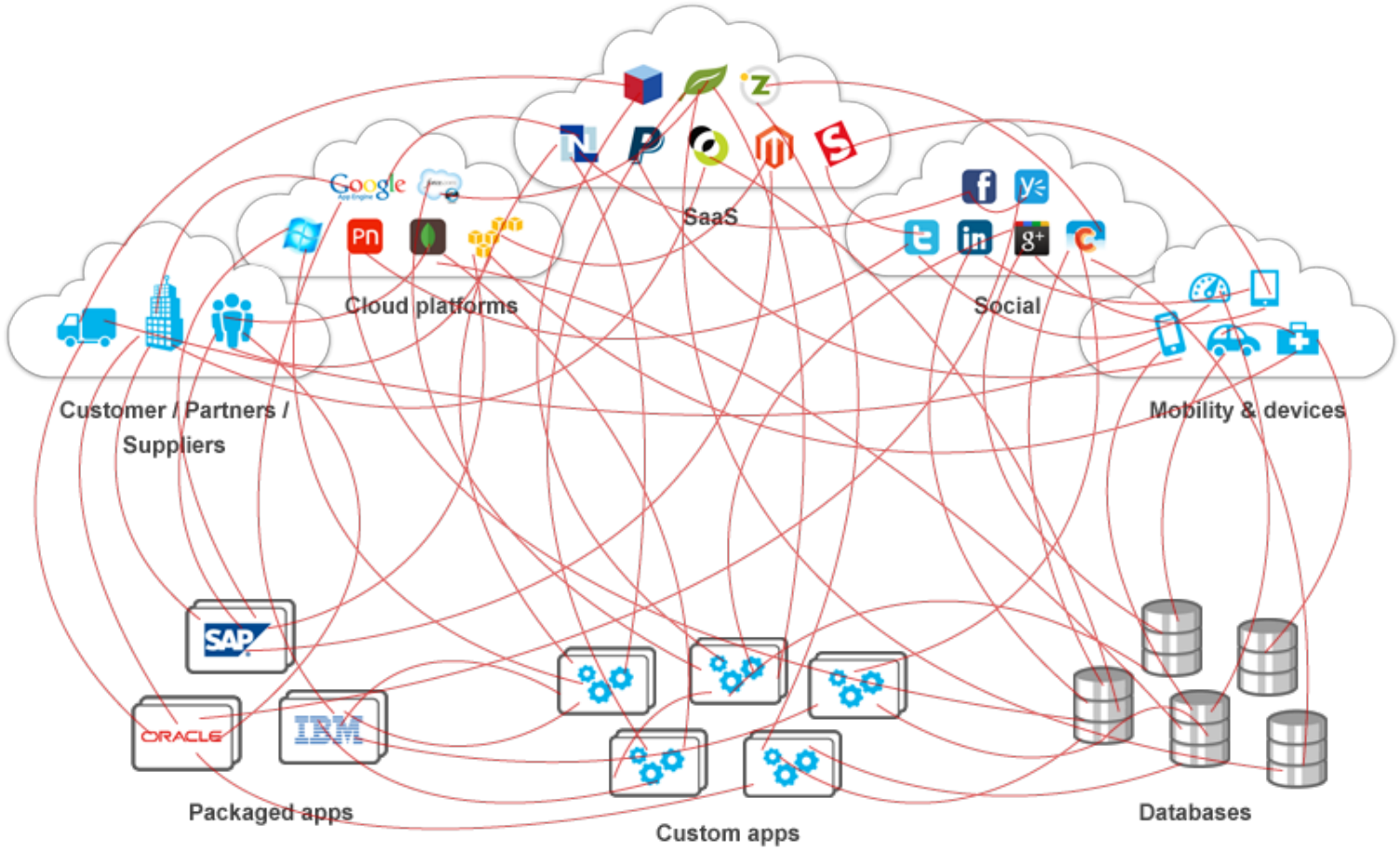


Data: Generation, Collection, & Processing

Privacy+ Security Forum

WHAT MODERN DATA FLOWS ACTUALLY LOOK LIKE

Today, virtual data warehouses are built to connect data residing in different databases and to service multiple systems, apps, and parties that are not natively compatible



Data: Generation, Collection, & Processing

Privacy+ Security Forum

COMMON THEMES WITH RESPECT TO DATA ACTIVITIES	COMMON THEMES WITH RESPECT TO TECHNOLOGY ACTIVITIES
▪ Collection ▪ Standardization ▪ Aggregation ▪ Analytics ▪ De-identification ▪ Exchange ▪ Benchmarking ▪ Reporting ▪ Publication	▪ Multi-institutional connectivity ▪ Data analysis vendors or parties ▪ Data storage vendors or parties ▪ Software or portals

Artificial Intelligence

Privacy+ Security Forum

WIDE-VARIETY OF TOOLS REFERRED TO AS AI

Artificial Intelligence
the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings

Machine Learning
a subset of AI that uses algorithms trained on data to produce models that can perform such complex tasks

Deep Learning
artificial neural networks that mimic the human brain are used to perform more complex reasoning tasks without human intervention

Generative Artificial Intelligence
deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on

Artificial Intelligence

Privacy+ Security Forum

COMMON POTENTIAL CONCERNS

- Patents / IP
- Protecting Data
- FDA regulation of drugs and medical devic
- FDA promotional restrictions
- Fraud and abuse
- Data privacy and security
- Telehealth regulation
- Licensure
- Corporate practice of medicine
- Consumer protection/transparency
- Conflict of interest

Risks of Using Third Party AI: Data Privacy

Privacy+ Security Forum

- AI tools often require access to large amounts of data in order to generate new content.
- Key data privacy regimes in the U.S. and EU (e.g., HIPAA, CCPA, GDPR) all contemplate limitations on both primary and secondary uses of personally identifiable data (and subsequently de-identified data)
  - Development and deployment of AI/ML is typically a secondary use of data which is not always contemplated during the primary data collection activity
- These data privacy regimes require a legal basis for processing, using, disclosing, and de-identifying personal data, and impose obligations on data controllers and data processors
  - Italian Data Protection Authority initially blocked ChatGPT because of potential unlawful collection of users' data and failing to prevent underage users from accessing inappropriate material
  - Access was restored April 28, 2023 after concerns were addressed
- May require careful review of consents and authorizations, terms of use and privacy policies, internal policies and procedures, and template contracts
- Also need to consider information security requirements, vendor-retained rights, and downstream use/ distribution restrictions and assurances

Risks of Using Third Party AI: Cyber

- AI platforms are equally subject to cybersecurity risks
- In March 2023, ChatGPT was taken offline after a bug in an open-source library allowed users to see titles from another active user's chat history, the first message of a newly-created conversation, and payment-related information

Risks of Using Third Party AI: Confidentiality

Privacy+ Security Forum

- Potential loss of trade secret status or breach of confidentiality
  - Third Party Confidential Information may not be protected in AI tools.
  - Confidential company information, including client information, should never be used in open-source AI

Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

LEADERSHIP · CHATGPT

Apple, Goldman Sachs, and Samsung among growing list of companies banning employees from using ChatGPT at work

Risks of Using Third Party AI: IP

- Potential copyright, trademark, or patent liability
  - Generated content may be based on or derived from copyrighted work, include trademarks, or infringe patents.
- No protections under copyright or patent for solely AI creators
  - Potential protection with “sufficient” human input

Risks of Using Third Party AI: Accuracy

Privacy+ Security Forum

- AI systems are just tools and do not produce final products or results
- AI may provide inaccurate and misleading results (“hallucinations”). For example, the technology behind ChatGPT works by predicting the next word in a sentence, which can result in errors in some cases
- These errors can be communicated with a sense of authority, which is misleading. Individuals should not rely solely on the output of an AI tool without independently evaluating the result and applying their own judgment in how to use the output

Risks of Using Third Party AI: Bias

- Generative AI tools can inadvertently perpetuate biases and discrimination
- Regulators including the FTC, DOJ, and EEOC are particularly focused on discrimination and bias in automated systems
- A New York City law places new restrictions on employers' use of AI and other automated tools in making decisions on hiring and promotions, including conducting a bias audit

Governance Framework for Using AI

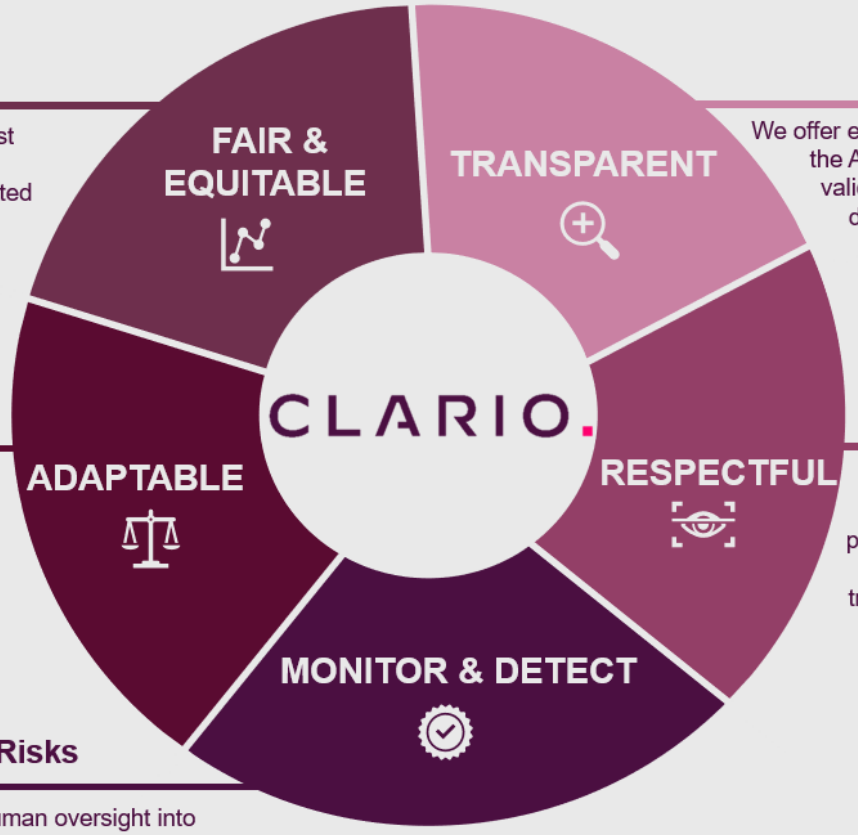
Privacy+ Security Forum

- Compliance policies should address all applicable risks, including:
  - Engagement
  - Controls to ensure that the AI tool is operating as intended
  - Updates to an AI service (or its components), where the legacy version is unavailable, may require a pause in its use until the updated version is analyzed and approved
  - Obligation and process for disclosing any errors in the model/tool or its application, both upward within organization and to clients and investors
  - Complete logs for the AI service (e.g., queries, responses, etc.) should be accessible to the compliance team
  - Procedures should exist for any service downtime, whether scheduled or unexpected
  - Team members with access to the AI tools should receive regular training, preferably annual or more frequent
    - Training should include guidelines to prevent the disclosure of trade secrets or other confidential information.

Governance Framework for Using AI

Privacy+ Security Forum

Clario's Commitment to the Responsible Use of AI



Minimizing bias

To reduce the potential for biased or unjust results, we use the most diverse data available to train the algorithms incorporated into our products and services

Ensuring Accountability

We offer explanations of the intended purpose of the AI, the data inputs used for training and validation of the algorithms, and what/how decisions are made by AI-enabled tools

Regulatory Landscape

To comply with applicable regulations as they come into force, we are committed to continuously monitoring the rapidly evolving regulation of AI

Privacy Rights

Our compliance with global data privacy laws and regulations is a priority. Using fully anonymized data to train AI models, the data is not traceable to any specific clinical trial, study sponsor, or study participant

Mitigating Risks

We integrate human oversight into development and use of our AI solutions to monitor outputs for accuracy and reliability

CLARIO.

Managing Adoption of AI Tools

Privacy+ Security Forum

- Specific areas of concern in leveraging generative AI:
  - Will confidential information ever be an input? How will that information be used by the service provider? Will it go into the model's or tool's library or knowledge base?
    - The company's or its clients' confidential information may be at risk of disclosure
    - The company may risk sharing information that is deemed confidential/sensitive
  - What risks are there that the service provider may cease to be able to perform its services? How will that impact the company's ability to provide services to its clients?
    - Key persons, geographic or political risks, etc.
  - Does the service provider rely on an underlying service or other business?
    - Is the model or tool built on top of ChatGPT or Bard?
  - Will the service provider provide advance notice of any changes to the code underlying its service?
    - What kind of documentation will be provided in cases of updates?

Contracting Considerations with AI

- How to define the AI platform, software, data, output?
- If the contract contemplates access to source code, should there be restrictions on field, territory, term? How to handle derivative works?
- Who provides the training data? Can the other party access? Are secure environments needed? What scope of data licenses are needed?
- Is the training of the AI done in a way that's compliant with applicable laws so that that the AI is not tainted?
- How will the output be used? What scope of output licenses are needed?

Best Practices and Key Takeaways: AI/ML

Privacy+ Security Forum

- Evaluate whether currently using or developing AI/ML tools
  - Convene cross-disciplinary teams to develop a thoughtful approach to vetting and overseeing these initiatives
  - The cross-disciplinary team should include members from the Legal, Compliance and Data Privacy/Security teams as well as data analysts, IT analysts and other applicable subject matter experts
- Assess accuracy, validity and reliability of AI/ML tools
  - Consider potential for bias/discrimination
  - Adopt standardized ethical principles/norms
- Ensure “privacy by design” and encourage transparency
- Keep an eye on state, federal, and international legal developments