May 12, 2023

Privacy and Related Considerations for Big Data and AI

Arianna Evers
WilmerHale

Lee Matheson
Future of Privacy Forum

Ali Jessani
WilmerHale

Privacy+ Security Forum

Speakers

Arianna Evers

Special Counsel
WilmerHale

Ali Jessani

Senior Associate
WilmerHale

Lee Matheson

Senior Counsel, Global Privacy
Future of Privacy Forum

Overview

Privacy+ Security Forum

- Key Concepts
- Legal Landscape
  - U.S.
  - International (with a focus on GDPR)
- Use Cases
- Takeaways

Key Concepts

Key Concepts

Privacy+ Security Forum

- What is Big Data?
  - Big data refers to large, diverse sets of information that grow at ever-increasing rates
- What is Machine Learning?
  - The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data
- What is Artificial Intelligence (AI)?
  - Artificial intelligence is the simulation of human intelligence processes by machines

Key Concepts

- What is Generative AI?
  - Describes algorithms (such as ChatGPT) that can be used to create new content, including audio, code, images, text, simulations, and videos.
- Different regulators have different definitions for these terms

Legal Landscape

Privacy+ Security Forum

Status Quo

- No federal law that meaningfully and comprehensively governs these technologies, and any near-term solution seems unlikely
- While existing federal law applies to these technologies and the harms they may enable, that regulation is at the margins
- States are filling the gap (again), and are regulating these technologies through comprehensive data privacy laws, as well as laws and regulations targeting specific issues
- The EU and other countries generally seem to be further along in thinking through these issues
- Regulators in the U.S. are paying attention. They are interested in understanding the underlying technologies and potential harms, and are asking a lot of questions

Federal Landscape

- **The White House**
  - Focus on automated systems that are used to make decisions that affect civil rights and underserved communities
  - Blueprint for an AI Bill of Rights & Technical Companion
    - Safe and Effective Systems
    - Algorithmic Discrimination Protections
    - Data Privacy
    - Notice and Explanation
    - Human Alternatives, Consideration, and Fallback
- **Congress**
  - Disagreement on overall approach to and multiple competing ideas
  - Schumer (D-NY) AI guardrails: Who, Where, How, Protect

Federal Landscape

- **Federal Trade Commission**
  - Existing laws apply to new technologies, specifically Section 5 of the FTC Act, Fair Credit Reporting Act, and Equal Credit Opportunity Act
  - Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems
  - Truthful, fair, and equitable use of AI
    - Importance of data sets
    - Discriminatory effects
    - Transparency and independent audits
    - Avoid false or unsubstantiated claims
    - Avoid misrepresentations about data uses
    - Do more good than harm
  - Use of AI to create or spread deception

Federal Landscape

- **Federal Trade Commission (cont.)**
  - Enforcement actions provide additional insight into agency approach
    - *Everalbum*: use of facial recognition technology without affirmative express consent to train models; data disgorgement
    - *BetterHelp & GoodRx:* sharing of sensitive health information without affirmative express consent for online advertising; refunds/civil penalties, burdensome injunctive terms, data disgorgement
  - Advanced Notice of Proposed Rulemaking
- National Telecommunications and Information Administration
  - "AI Accountability Policy Request for Comment" focuses on development of AI audits, assessments, certifications and other mechanisms to create earned trust in AI systems.
- **Numerous other actions across federal agencies focused on particular uses of automated decision-making (e.g., health care, housing, employment)**

Federal Landscape

- **NIST AI Risk Management Framework 1.0**
  - Intended to be universally appliable to AI use cases
  - Four functions to manage AI risks and develop trustworthy AI
    - (1) Govern
    - (2) Map
    - (3) Measure
    - (4) Manage
- **GAO Accountability Framework for Federal Agencies and Other Entities**

State Comprehensive Privacy Laws

- Nine states have passed or enacted “comprehensive” privacy laws that create data privacy rights for consumers and data processing obligations for companies
  - CA and VA are in effect
  - CO, CT, and UT will go into effect in 2023
  - IA, IN, TN, and MT passed in 2023; will go into effect 2024-2025
- These laws create obligations for the processing of “personal information” or “personal data”
  - Generally defined broadly to include information that is linked or reasonably linkable to an identified or identifiable individual
- To the extent the use of AI implicates PI, these laws will be relevant

California Privacy Rights Act

Privacy+ Security Forum

- The California Privacy Rights Act (CPRA) amended and expanded upon the existing California Consumer Privacy Act (CCPA) and brought the California law more in line with the GDPR
- Creates a new agency – California Privacy Protection Agency (CPPA) –that is responsible for rulemaking and enforcement
- One of the areas the agency has authority over is to issue “regulations governing access and opt-out rights with respect to businesses’ use of automated decision-making technology, including profiling and requiring businesses’ response to access requests to include meaningful information about the logic involved in such decision- making processes, as well as a description of the likely outcome of the process with respect to the consumer.”

CPRA Rulemaking

Privacy+ Security Forum

- The issues the agency may address through rulemaking include:
  - How should automated decision-making technology be defined?
  - How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?
  - What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer?

Other States

- CO, CT, and MT all provide consumers with the right to opt-out of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer
  - Similar to GDPR
- Profiling is generally defined as “any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. “
- "Decisions that produce legal or similarly significant effects concerning the consumer” is generally defined as “decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to necessities such as food and water.”
- CO provides CO AG with rulemaking authority on this issue

CO Rulemaking on Automated Decision-Making

Privacy+ Security Forum

- Rules distinguish between “Human Involved Automated Processing” (which is not subject to the rules”) and “Solely Automated Processing” and “Human Reviewed Automated Processing” (both of which are subject to the rules)
  - Human Involved Automated Processing means the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing.
  - Human Reviewed Automated Processing means the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the automated processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.
  - Solely Automated Processing means the automated processing of Personal Data with no human review, oversight, involvement, or intervention.

CO Rulemaking on Automated Decision-Making (cont.)

Privacy+ Security Forum

- If a company engages in “Solely Automated Processing” and “Human Reviewed Automated Processing” that produces “Legal or Other Similarly Significant Effects” concerning a consumer, it has to provide notice that includes the following information:
  - What decisions are subject to profiling
  - Categories of Personal Data involved
  - A non-technical, plain language explanation of the logic used
  - A non-technical, plain language explanation of how profiling is used in the decision-making process (including an explanation of any human involvement)
  - If the system has been evaluated for accuracy, fairness, or bias, including the use of any sensitive data, and the outcome of any such evaluation
  - The benefits and potential consequences of the decision based on the profiling
  - Information about how the consumer may opt out

CO Rulemaking on Automated Decision-Making (cont.)

Privacy+ Security Forum

- Other rules:
  - Data protection assessments required for "processing personal data for profiling if the profiling presents a reasonably foreseeable risk of:
    - Unfair or deceptive treatment of or unlawful disparate impact to consumers
    - Financial or physical injury to consumers
    - A physical or other intrusion upon the solitude or seclusion or private affairs of consumers, if the intrusion would be offensive to a reasonable person
    - Other substantial injury to consumers
  - Consent requirement for the same use case after a consumer has opted out of profiling

Other Relevant Considerations For Comprehensive Privacy Laws

Privacy+ Security Forum

- Definitions of “deidentified” and “aggregated” data
- Processor/service provider use cases
- Third party contracts (for CPRA)
- Data privacy rights
- Data protection assessments
- Special obligations related to “sensitive” data

Other AI Laws at the State Level

- Illinois and Maryland have enacted artificial intelligence video interview laws
- NYC will enforce an AI bias audit law beginning in July 2023
- Number of other states are considering AI-specific privacy laws (e.g., California)

AI and the GDPR

Privacy+ Security Forum

- GDPR < regulates an activity **not** a technology
- **Rec 4** GDPR < the processing of personal data should be designed to serve mankind
- **Art 1(2)** GDPR < protection of all rights and freedoms
- The GDPR regulates **two types of Automated Decision-Making**:
  1. decisions based solely on automated processing
  2. decisions based on automated processing (not solely automated)

Solely ADM

All GDPR provisions

Right to know the existence of that processing and meaningful information about the **logic involved**, the **significance** and the **envisaged consequences**.

Art 22: Right not to be subject to this type of ADM

ADM

All GDPR provisions

Right to know the existence of that processing and meaningful information about the **logic involved**, the **significance** and the **envisaged consequences**.

Other Existing DP Laws

- Ex 1: Brazil LGPD
- LGPD entered into force Sep 18th, 2020;
- ADM provision (Art 20)
  - Not a prohibition
  - Right to request a review of the decision – solely ADM + 'affects their interests'
  - Right to request information on the 'criteria and procedures used for the automated decision'
  - Controller: may refuse access request on the basis of 'business and industrial secrets'
  - No right to object to the processing / contest the decision / be heard
- Other examples:
  - Argentina (PDPA + Res. 2019)
  - China (PIPL)

EU AIA: Current Status

Privacy+ Security Forum

- European Commission's Proposal (2021)
- Council of EU Issues General Approach (December 2022)
- EP reaches "Political Agreement" on contents of file for committee/plenary votes (April 2023)
- Awaiting Parliament's formal position: expected soon (May 2023)
- Enter the trilogue negotiations
- Final agreement – Adoption of the AI Act
- Published in the *Official Journal of the EU*
  - Art 85(1) EU AIA*:* enters into force on the twentieth day following that of its publication
  - Art 85(2) EU AIA: applies [24 months following the entering into force of the Regulation]

The Proposed EU AIA

Privacy+ Security Forum

- Designed to promote lawful, safe and trustworthy AI systems
- **Treaty Basis**: 114 TFEU – internal market legal basis - & 16 TFEU on provisions relating to data protection
- **Overall design**: Risk based approach
- **Close Analogue**: Product safety legislation

Eu AIA: What is AI?

Privacy+ Security Forum

Definition of an AI system: technology neutral and future proof; two competing definitions:

EU Commission: (i) software (ii) developed with one or more of the techniques and approaches listed in Annex I (iii) for a given set of human-defined objectives (iv) can generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with and (v) can operate with varying levels of autonomy.

EU Parliament: an engineered or machine-based system that can, for a given set of objectives, generate output such as content, predictions, recommendations, or decisions influencing real or virtual environments. …Designed to operate with varying levels of autonomy.

Material Scope

Privacy+ Security Forum

GDPR

This Regulation applies to

the processing of personal data wholly or partly by automated means […]

Processing: any operation or set of operations which is performed on personal data **or on sets of personal data**

Proposed AI Act

This Regulation applies to

providers placing on the market or putting into service **AI systems** in the Union

users of AI systems

(Art 3(1)) AI system:

- software
- developed with one or more of the techniques and approaches listed in Annex I
- for a given set of human-defined objectives
- can generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with

Other Key Definitions

Privacy+ Security Forum

Proposed AI Act

Provider

a natural or legal person, public authority, agency or other body that **develops** an AI system or that **has an AI system developed** with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

User

any natural or legal person, public authority, agency or other body **using an AI system under its authority**, except where the AI system is used in the course of a personal non-professional activity

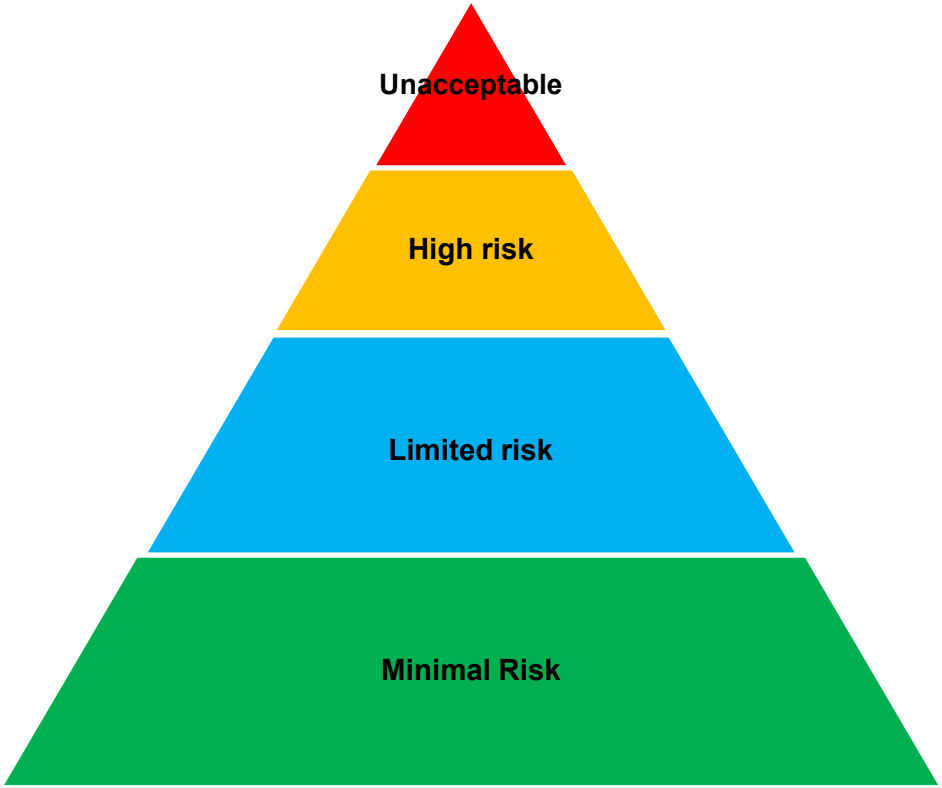
Material Scope (see above):

the placing on the market, putting into service and use of AI systems

Territorial Scope – extraterritoriality

Risk-based Approach

Privacy+ Security Forum



Unacceptable risk – Prohibited practices (Title II) [prohibition/authorization]

- Sub-liminal techniques to distort a person's behavior;
- Systems that exploit peoples' vulnerabilities to manipulate them;
- Social scoring systems;
- 'Real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement.

High risks (Title III)

- AI systems intended to be used as a safety component of a product, or are a product and the product is required to undergo a 3rd party CA
- AI systems used for the purposes enumerated under Annex III

Conformity Assessment: Process of verifying whether a provider of an AI system has put in place controls to assure the following:

- Risk management systems
- High quality of training, validation and testing data sets used
- Technical documentation
- Transparency
- Human oversight
- Record-keeping
- Robustness, accuracy and cybersecurity

Limited risks (Title IV – Art 52) - Transparency requirements

- Chatbots
- Emotion recognition systems
- Biometric categorization systems
- Systems that generate deep fakes

Minimal risks (Title IX – Art 69) - Possible voluntary codes of conduct

- Spam filters
- Codes of conduct : Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application

Governance

European AI Board → advice, assistance, guidance

- Chair: EU Commission
- Composition: national competent authorities + EDPS

National Competent Authorities

- Designated by each EU MS (not necessarily existing EU DPA)

Other Emerging Frameworks

Privacy+ Security Forum

Brazil Prescriptive Models

Self-Regulatory Frameworks

- Comprehensive study + recommendation presented to BR Senate

China

- "Regulations on the Administration of Algorithmic Recommendation of Internet Information Services"
- Draft "Administrative Measures for Generative Artificial Intelligence Services" (proposed April 2023)

Canada

- C-27 passed 2nd Parliamentary Reading April 2023

Self-Regulatory Frameworks

Singapore

- Model Framework on AI Governance published by PDPC

South Korea

- AI Self-Checklist published by the PIPC

Use Cases

Privacy+ Security Forum

- **Generative AI**: Company A develops policies and procedures for its employees to utilize ChatGPT to improve customer offerings
- **Employment**: Company B, in an effort to streamline hiring, deploys an HR tool to screen job candidates
- **Targeted Advertisement**: Company C uses machine learning to improve the quality of its personalized advertisement campaign

Takeaways

Privacy+ Security Forum

- Legal landscape is moving quickly
- Expect inconsistencies between how federal, state, and international lawmakers approach these issues
- Regulators are concerned about the potential ramifications of the technology; they are going to use investigations to better understand the technology and potential risks, as well as test novel theories
- Leverage frameworks and industry best practices
- Sound judgment and having a consistent and principled approach to deploying AI is important in the absence of clear legal guidance

Thank you ☺

Privacy+ Security Forum

Arianna Evers

Arianna.Evers@wilmerhale.com
@ariannaevers

Ali Jessani

Ali.Jessani@wilmerhale.com
@alijay24

- WilmerHale Privacy & Cybersecurity Law Blog

Lee Matheson

@PrivacLee
lmatheson@fpf.org

www.fpf.org
facebook.com/futureofprivacy
@futureofprivacy