Cooley

ACC Association of Corporate Counsel NEW YORK CITY

Top Things You Should Know about AI, Biometrics and Privacy

Justine Gauthier, Lei Shen, Bethany Lobo, and Liza Cotter

attorney advertisement

Justine Gauthier

Justine is the Director of Corporate & Legal Affairs at Mila, a prominent artificial intelligence research organization at the intersection of academia and industry. She is responsible for constructing and implementing Mila's IP strategy, and for providing counsel on the legal, regulatory, and ethical implications of developing cutting-edge machine learning technologies. Justine also negotiates complex collaborative technology agreements with a variety of public and private sector organizations, from F500s to startups and SMEs in fields such as biotech, software, healthcare, finance, retail and energy. Prior to joining Mila, Justine practiced corporate law at a top Canadian law firm.

Justine Gauthier
Director, Corporate & Legal Affairs / Privacy Officer

+1 514 690 2392
justine.gauthier@mila.quebec

Lei Shen

Lei advises clients on a wide range of global data privacy issues and works collaboratively to develop practical privacy and data protection strategies for their products and services. She helps companies navigate and comply with state, federal and international privacy regulations, including the California Consumer Privacy Act (CCPA), the EU General Data Protection Regulation (GDPR), and upcoming state consumer data protection laws. She also advises on issues concerning emerging technologies, such as telematics, connected products and services (including connected and autonomous vehicles), and AI.

Lei Shen
Partner

+1 312 881 6690
lshen@cooley.com

Bethany Lobo

Bethany Lobo is a partner who litigates from pleading stage to appeal for companies facing high-value business model challenges, particularly those concerning cutting-edge privacy, data security/data breach and other Internet law issues. She is a member of Cooley's cyber/data/privacy practice group that has repeatedly been recognized by Law360 as Privacy Practice of the Year, most recently in 2020. She is also a member of Cooley's commercial litigation and class action litigation practice groups, and she litigates a wide variety of other complex commercial and class action cases.

Bethany Lobo
Partner

+1 415 693 2187
blobo@cooley.com

Liza Cotter

Liza Cotter focuses her practice on privacy, data protection and cybersecurity. She advises clients across multiple industries on national and international regulatory compliance, data protection best practices, incident response and privacy and data security risk issues in corporate transactions. Liza is an IAPP Certified Information Privacy Professional for the United States (CIPP/US).

Liza Cotter
Associate

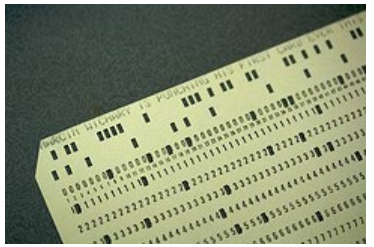
+1 212 479 6063
ecotter@cooley.com

General AI Issues & Considerations

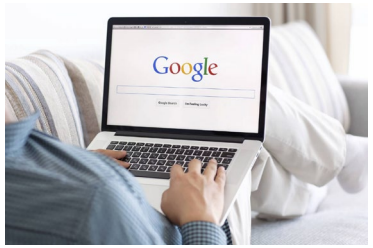
Cooley

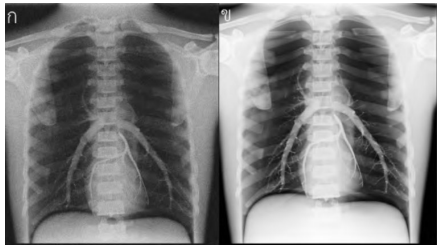
AI and Data: Brief Historic Overview

- The type of data used by AI has evolved over time
  - Earlier fundamental AI models were trained on very basic, non personal data



  - As AI evolved, potential applications – and types of data required for these applications - multiplied





Understanding your use of AI

- Input: What type of data is the AI using?
  - Personal vs. Non-personal data
  - Training data vs. Production data
- Processing: How is the AI processing the data?
  - Explainability requirements and black box issues
  - Bias
- Output: How are the results used?
  - Accuracy
  - Human oversight vs. Automated decision-making

Disclosing your use of AI

- Transparency is required by laws in the U.S., EU and elsewhere abroad when AI is processing personal information.
- In the U.S., laws at both the federal and state level require that notices be provided and/or consents obtained prior to processing personal data.
  - Current and upcoming U.S. consumer data privacy laws have disclosure requirements
- Under upcoming legislation in the EU and Canada, disclosure will be required even when not processing personal data.

Data Subject Rights

- Companies using personal data in connection with AI (e.g., machine learning) must be able to respond to data access and deletion requests.
- Consider “privacy by design” and “privacy by default” principles in designing AI programs and systems.
  - Data minimization
  - Anonymization
  - Synthetic data

Discrimination

- Concerns with bias and discrimination in AI and resulting harm
- NYC law regulating use of automated decision-making tools in the context of hiring/employee evaluation takes effect Jan. 2023
  - Requires a “bias audit”
  - Intended to help address discrimination in the employment context

Ethical Use of AI

- Currently, ethics of AI are not directly addressed in legislation
- Many organizations are taking steps towards ethical AI
- Proposed EU and Canadian laws do address ethical issues
  - EU: prohibition of all AI systems that intend to *materially distort a person's behaviour* or to *evaluate the trustworthiness of natural persons*
  - Canada: new *AI and Data Act* is centered around risks of bias and of harm to fundamental rights

Ethics by Design

- Project Infrared : AI solutions that sift through online advertisements and detect potential human trafficking activity
- Ethics by Design Approach:
  - Bi-disciplinary development team of AI and criminology professionals
  - Engaging with multiple stakeholders as early as the development stage (potential users (law enforcement), sex trafficking survivors, advocacy groups)
  - Outside expertise and guidance on legal and ethical implications (outside counsel, partnership with the Responsible AI Institute)

U.S. Biometric Laws

Cooley

Biometrics Laws

Dedicated biometrics laws: Illinois, Texas, Washington

- Illinois' Biometric Information Privacy Act
  - Notice and consent requirements
  - Retention and destruction requirements
  - Disclosure and sale restrictions
  - Security requirements
  - Private right of action

Biometrics Laws (cont'd)

Dedicated biometrics laws (cont'd)

- Texas' Capture or Use of Biometric Identifier Law ("CUBI")
- Washington Biometrics Law (H.B. 1493)
  - Both laws apply to biometric data captured for commercial purposes
  - Both laws contain many requirements similar to BIPA
  - Neither law has private right of action

Regulations at Federal, State & Local Level (3)

- U.S. Consumer Data Privacy Laws / State Data Breach Notification Laws
  - Included in definition of “personal information” under CCPA/CPRA and upcoming state consumer data privacy laws
  - Considered to be “sensitive data” / “sensitive personal information” under upcoming laws, some of which require opt-in consent
  - Certain state data breach notification laws amended to require reporting of biometric data breaches
- NYC’s Biometric Identifier Information Ordinance
  - Notification obligations via signage
  - Sale / disclosure restrictions
  - Private right of action (but cure period for certain violations)

U.S. Biometric Litigation

Cooley

BIPA: Private Right of Action

- Any individual whose rights under BIPA have been violated may sue, whether individually or on a classwide basis
  - Need not allege injury beyond a statutory violation
  - Statutory damages from $1,000-$5,000/violation
  - High class action exposure
- More than 1,500 cases filed to date

BIPA: Current Subject Matter Trends

- Types of cases:
  - Employee timekeeping (e.g., fingerprints)
  - Facial detection and recognition
    - Virtual try-on cases
    - Telematics in vehicle monitoring
  - Voiceprints
- BIPA AI litigation examples
  - *Stein v. Clarifai, Inc.*
  - *Clearview AI* cases

BIPA: Hot Litigation Issues

- **When does a BIPA cause of action accrue?**
  - *Cothron v. White Castle* (pending 2022)
- **What statute of limitations applies to BIPA claims?**
  - *Tims v. Black Horse Carriers* (pending 2022)
- **When may plaintiffs pursue BIPA claims in federal court?**
  - *Bryant v. Compass Group* (2020)
  - *Fox v. Dakkota Integrated Systems* (2020)
  - *Thornley v. Clearview AI* (2021)

Legislation in the EU and Beyond

Cooley

EU Proposal for a Regulation in a Nutshell

Presented by the EU Commission on 21 April 2021

Contained in a 125-page document

First ever legal framework dedicated to AI worldwide

Heavily drawn from data protection (GDPR), cybersecurity (NIS Directive) and product safety rules (EU Product Safety and Liability Directives; harmonized standard and CE mark)

Proposes a risk based approach in classifying AI (prohibited, high, limited, and minimal risk AI)

Broad Definition of AI

- *"'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I* and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"*

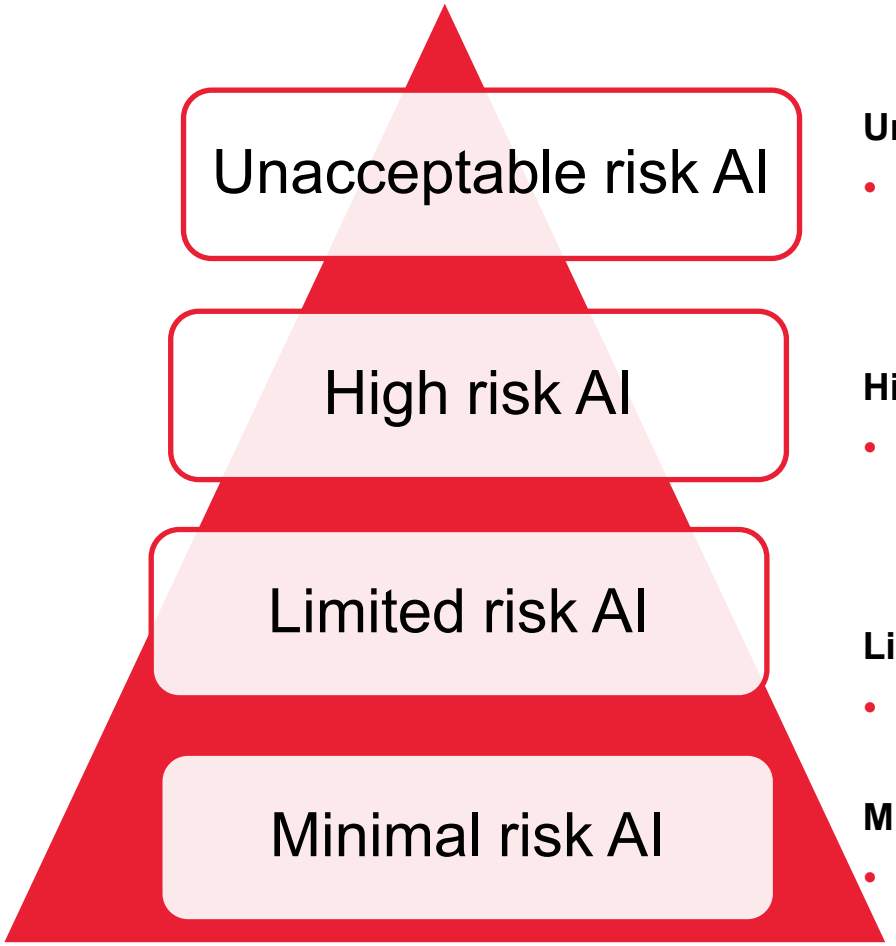
* Techniques and approaches:

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) Statistical approaches, Bayesian estimation, search and optimization methods

Broad Scope of Application

- Like the GDPR, **extraterritorial effect:** obligations extended to providers and users based outside of the EU
- Covers the **whole value chain**: the primary obligations are owed by the party placing the system on the market (the “provider”). Lesser but still onerous obligations are owed by importers, distributors and users of AI systems.
- Covers the **whole AI systems’ lifecycle**: pre-market to post-market surveillance obligations

Risk-Based Approach



Unacceptable risk AI

- Includes AI systems that deploy “subliminal techniques beyond a person’s consciousness,” exploit vulnerable groups, enable social scoring by governments, or allow live remote biometric identification in publicly accessible spaces used for law enforcement purposes (with some exceptions) => **Will be banned entirely in the EU**

High risk AI

- Includes AI systems performing a safety function in certain products (including, for example, mobile devices, IoT products, robotics and other machinery, toys and medical devices) or other stand-alone AI systems with mainly fundamental rights implications => **Permitted subject to compliance with a heavy set of requirements**

Limited risk AI

- Includes those AI systems intended to interact with natural persons=> **Will be subject to certain transparency requirements.**

Minimal risk AI

- Majority of AI systems, for example, AI-enabled video games and spam filters => **Will not be subject to significant regulatory interference.**

Obligations for High-Risk AI

- Pre-market obligations include:
  - **Registration in a European public database.**
  - **Appropriate human oversight** measures to minimise the risks;
  - **Adequate risk assessment and mitigation systems** throughout the entire lifecycle**;**
  - High level of **robustness**, **cybersecurity** and **accuracy;**
  - **Detailed documentation** and **record-keeping.**

- Post-market obligations include:
  - Appointment of a **representative;**
  - **Reporting of incidents** to the authorities.

Transparency obligation for certain AI systems

- It concerns AI systems that:
  - interact with humans,
  - are used to detect emotions or determine association with (social) categories based on biometric data,
  - generate or manipulate content (‘deep fakes’).
- Obligation to inform users that they are interacting with an AI system (except where it is obvious)
- Obligation to disclose that the content is generated through automated means (save for some exceptions)
- Specific notifications if personal data is being used to identify intentions or predict behaviors of persons, or to categorize persons to specific categories, such as sex, age, ethnic origin or sexual orientation.

Fines & Enforcement

Fines

- More stringent than under the GDPR
- **Fines of up to €30 million, or 6% of global annual turnover**, are envisaged for certain categories of breaches.

Governance and enforcement

- EU Member States need to designate a competent authority in charge of enforcing the AI Regulation.
- EU Member States market surveillance authorities will be given additional powers and competence to monitor certain AI systems subjected to such obligations.
- A European Artificial Intelligence Board will be set up (with a similar role as the EDPB).

Adoption Process

- The AI Proposal for a Regulation is currently debated in the Council of the EU and European Parliament – thousands of proposed amendments have been filed
- Expected time of adoption: likely not before 2023
- 2Y period of implementation once adopted

Canada's *Artificial Intelligence and Data Act* and Privacy Reform

- Bill C-27 - *Digital Charter Implementation Act, 2022* introduced to Canadian parliament on June 16th 2022
- If passed, C-27 will:
  - Implement Canada's first (and world's second) artificial intelligence legislation: the *Artificial Intelligence and Data Act (AIDA)*
  - Reform Canadian privacy law by replacing existing privacy legislation *(PIPEDA)* with the new *Consumer Privacy Protection Act (CPPA);*
  - Create a tribunal specific to privacy and data protection.

Broad Definitions

"artificial intelligence systems"

"a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions"

Broad Scope of Application

- Covers the **whole value chain** : entities or individuals who are “responsible for” AI systems, meaning those who design, develop, make available for use, or manage the operations of, AI systems
- Extraterritorial effects to the extent global AI systems are used, developed, designed or managed in Canada.

Obligations for all AI systems

- Obligations follow a 2-step structure:

1. Obligations required for all AI systems:
   - Establish measures to **manage anonymized data**
   - Conduct an **assessment** to determine if the AI system is “high-impact”
   - **Maintain records** of steps taken to meet requirements and describe how impact assessment conclusions are reached
2. Obligations required for AI systems deemed “high-impact”:
   - Develop a **risk mitigation plan** and monitor risk mitigation measures
   - **Publish a plain-language description** of how the system will be used, and what decisions/recommendations/predictions it will produce
   - **Notify** the federal government of systems with risk of “material harm”

Transparency

- Disclosure requirements:
  - Publication of plain-language description of high-impact AI systems
  - Right to be informed (but not opt-out of) automated decision making

- Explainability requirements:
  - Right to an explanation of automated decision making that could have a significant impact on an individual

Fines & Enforcement

Fines

- Administrative penalties left to regulators to define
- Criminal contraventions of AIDA: up to **$10 million or 3% of global revenues**
- **New criminal offence** related to making an AI system available for use, when the AI system causes serious physical/psychological harm or property damage or causes substantial economic loss to an individual : **up to $25 million or 5% of global revenues** (or up to 5 years of prison)

Governance and enforcement

- Creation of a specific privacy and data protection tribunal

Adoption Process

- Bill C-27 was introduced on June 16th, 2022

- Expected time of adoption and period of implementation TBD

Other International Developments

- Spanish DPA guidelines
- French Data Protection Authority's (CNIL) Initiative on AI
- UK DPA (ICO) AI Initiative

U.S. Enforcement Actions

Cooley

FTC Enforcement Actions Implicating AI (1)

- ***In the Matter of Everalbum, Inc.*, Docket No. C-4743 (2021)**
  - FTC alleged that photo app that derived facial recognition data from user photos to create databases to build and improve the app's features made false representations to users concerning their ability to prevent the use of the technology and related to data deletion.
  - Consent decree requires, among other things, that Everalbum obtain affirmative consent for all uses of biometric information, delete facial recognition data derived from photos and videos of users who have not provided affirmative consent, and delete or destroy any algorithms or models developed using such information.
  - **Takeaway**: FTC can and will utilize disgorgement as a remedy for legal violations, which, in the context of products and services dependent on machine learning and AI algorithms, could effectively prevent further use of those products/services or require retraining/redevelopment of algorithms and models from scratch.

FTC Enforcement Actions Implicating AI (2)

- ***In the Matter of Flo Health, Inc.*, Docket No. C-4747 (2021)**
  - FTC alleged that fertility tracking app shared its users' health information with third-party marketing and data analytics providers after promising users that such information would be kept private.
  - Consent decree requires, *inter alia*, that Flo Health provide certain notices to affected users related to the disclosure of their health information, obtain affirmative express consent to the collection and use of health information, and *instruct any third party that received health information belonging to app users to destroy such information*.
  - **Takeaway**: if using AI-based algorithms/machine learning, need to conduct diligence on your data sources.

FTC Enforcement Actions Implicating AI (3)

- ***U.S. v. Kurbo, Inc. & WW Int'l, Inc.*, Case No. 22-CV-946 (2022)**
  - DOJ, on behalf of the FTC, filed a complaint against the company f/k/a Weight Watchers and a subsidiary alleging that they collected personal information from children under the age of 13 without parental permission in violation of COPPA in connection with their marketing of a weight loss app.
  - Among other things, settlement requires that the companies delete the illegally obtained data and destroy any algorithms derived from the data.
  - **Takeaway**: Provides further evidence of the FTC's propensity to use the disgorgement remedy in the context of AI algorithms and models built / trained on ill-gotten data.

State AGs and Clearview AI

- Clearview AI is subject to a number of legal actions in the U.S., including federal multidistrict litigation in Illinois and an enforcement action brought by the Vermont Attorney General under VT's consumer protection law. Additionally, NJ's Attorney General has specifically banned law enforcement in the state from using Clearview AI's technology.
- Clearview AI has also faced a variety of actions in the EU.

Q&A

Cooley