Beyond LLMs: Privacy Issues in Video, Image, and Computer Vision Models

Privacy and Security Forum
May 7, 2025

FRESHFIELDS

Overview

01.

Primer on Foundation Models

02.

Incremental Risks of Multimodal and Computer Vision Models

03.

Current and Future Regulatory Landscape

04.

Case Studies and Predictions

01.

Primer on Foundation Models

Foundation Models

- Foundation Models are AI models trained on vast amounts of data that can be applied to a wide range of tasks
- AI models—large language models (***LLMs***), multimodal generative models, and computer vision models (***CVs***)—differ by training data and the outputs they generate

	Input	**Output**
LLMs	Text	Text
Multimodal, Video, and/or Image Generative Models	Text/Image/Audio	Text/Image/Video/ Audio
CV Models	Image/Video	Visual Labels

Multimodal Market at a Glance

- Global multimodal AI market:
  - $1.6bn in 2024
  - $2.51bn in 2025
  - Forecasted to be ~$42.4bn by 2034
- North America AI market:
  - Multimodal share of the market: 48 percent in 2024
- US multimodal AI market:
  - $790m in 2024
  - Forecasted to be ~$18.6bn by 2034

Multimodal Models ("MM")

AI models based on Transformer Architecture that process and combine information from multiple types of input data (called modalities) – like text, images, audio, and video – to make decisions or generate multimodal outputs.

Common Applications:

- Automated Content
  - Example personal use—allows generation or editing of multimedia content based on a text prompt
  - Example enterprise use—integrates various sensors – e.g., radar, lidar, and cameras – to enable spatial awareness
- Enhanced Customer Support
  - Brings customer support AI agents closer to human capabilities by enabling more inputs
- E-Commerce Experiences
  - Creates personal promotional visuals based on an individual's preferences
  - Customers can edit images to "try on" or customize products

CV Models

Use image or video as their input and generate visual labels as their output. CV models are trained using deep learning such as Convolutional Neural Networks (CNNs).

CV models are used for:

- Facial Recognition
- Image Classification
- Image Segmentation
- Pose Estimation
- Object Tracking
- Autonomous Vehicles (self-driving cars, driver-assist)
- Clinical Applications (e.g., disease detection from scans, surgical assistance)
- Surveillance and Biometric Identification Systems (e.g., facial recognition)
- Robotics
- Manufacturing
- Military/Targeting

● **Benefits Over LLMs and MM Models:**

- Fast
- Efficient with data and compute

02.

Enhanced Risks of Multimodal and Computer Vision Models

Inherent Challenges Compared to LLMs

1\.

Privacy implications of processing visual personal data as part of training, also harder to anonymize these data types

2\.

Challenges of consent in public spaces

3\.

Data integration challenges due to richness of multimedia data—both in size and particularity of data/ information about individuals)

- E.g., video clip reveals demographics, location, behavior, and associations beyond text’s scope

Input Risks

Type of Input Risk	Level of Risk for LLM	Level of Risk for MM	Level of Risk for CV
Training on or capturing personal data	+	++ Biometric data	+++ Third party exposure and biometric data
Illegal content used for training	+	++ Enhanced risk for IP violations	+++ Enhanced risk for IP violations or CSAM
Bias/unfairness	++	+++	+++
Adversarial attacks	+ Risk of training data poisoning and prompt injection attacks	++ Enhanced exposure of more sensitive data	+++ Risk of physical threats from AI systems

Output Risks

Type of Output Risk	Level of Risk for LLM	Level of Risk for MM	Level of Risk for CV
Hallucinations	++	+++	+
Bias/unfairness/ misidentification	++	+++	+++
IP Violations	++	+++	N/A
Explainability/ Transparency Issues	+	+++	++
Deepfakes (incl. voice cloning/CSAM/NCSI)	+	+++	N/A
Advanced Inference/Cross-modal Linkage/Triangulation	++	+++	N/A

03.

Current and Future Regulatory Landscape

Current U.S. Regulatory Frameworks

AI-Specific Laws

- Upcoming Federal Take It Down Act
- Patchwork of State AI Laws

Existing Legal Frameworks

- Privacy
- Cybersecurity

Guidelines

- NIST AI Risk Management Framework

U.S. Regulators of AI

- Federal Communications Commission (FCC)
- Federal Trade Commission (FTC)
- Consumer Financial Protection Bureau (CFPB)
- Committee on Foreign Investment in the United States (CFIUS)
- Securities and Exchange Commission (SEC)
- Department of Justice (DOJ)

Current Global Laws Applicable to AI

EU Artificial Intelligence Act

- Risk based approach based on use case and model power
- Most burdensome obligations for high-risk use cases and general-purpose models

South Korea: Act on the Development of Artificial Intelligence and Establishment of Trust (AI Basic Act)

- Creation of national AI infrastructures, such as training data and data centers
- Transparency and safety liability for “high impact” AI and generative AI developers

China: Cyberspace Administration of China’s (CAC) Interim Measures

- “[C]lear up and rectify the abuse of AI technology”

FTC Privacy and Data Security UDAPs

FTC Privacy and Data Security cases traditional focus on a few specific types of injuries, often referred to as informational injuries:

Deception injury or subverting consumer choice

Financial injury

- Commonly, in privacy and data security cases

Health and safety injury

- e.g., AccuSearch, SpyFone, Epic Games, 23andMe

Reputational injury

- Often pled with data breach/ unauthorized access/deception
- e.g., Eli Lily

Unwarranted intrusion injury

- Also, “intrusion on seclusion”
- e.g., Do Not Call registry, Aaron’s Furniture (rent-to-own), Amazon/Ring

Sensitive Information Used for Training

Enhanced privacy implications: sensitivity and richness of the data and the challenges with anonymization.

Current Regulatory Landscape

- Illinois AI Video Interview Act
- Illinois Biometric Information Privacy Act (BIPA)
- Georgia’s ion on the sale and dispensing of contact lenses (HB203)

Emerging Regulation

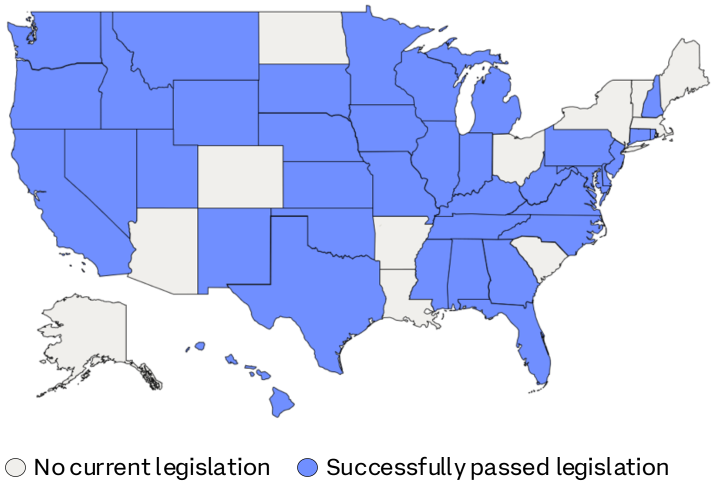
- Maryland’s Generative Artificial Intelligence – Training Data Transparency (HB0823)

Clearview AI

- Reached settlement of $51.75m for collecting 10 billion images from public websites and social media – without user consent – to create its biometric database for AI training

Deepfakes, Revenge Porn, CSAM, NCSI

The ability for CV and Multimodal Models to generate explicit and abusive content runs the risk of amplifying harm through scale, realism, and anonymity.



Source: Enoughabuse.org

Current Regulatory Landscape

- Upcoming Take It Down Act
- As of April 2025, 38 States criminalize AI-generated CSAM
- 17 states have Deepfake laws aimed at political ads and Revenge porn

Emerging Regulation

- Criminal codes related to obscene visual materials created by Gen AI

Impersonation Deepfakes

Enhance the risk of and decreased ability to detect and stop fraud, deception, and manipulation from technologies that combine realistic text, voice, and visual content.

Current Regulatory Landscape

- FTC's Voice Cloning Challenge
- FTC Impersonation Rule (16 CFR 461)
- FCC Telephone Consumer Protection Act (TCPA)
- FCC Truth in Caller ID Act of 2009

State Regulatory Landscape (Examples)

- Tennessee's ELVIS Act (Ensuring Likeness, Voice and Image Security)
- California's Unfair Competition Law and its Election Misinformation Prevention Laws (Elec. Code, § 18320)
- Louisiana's Deepfake Criminalization (SB175)
- Texas Unfair and Deceptive Practices (TX AG vs. Piece [AI Company])

Lingo Telecom, LLC

- In 2024, after the FCC initially proposed a $2m fine, Lingo Telecom agreed to pay a $1m fine for its role in the deepfake robocall that impersonated President Joe Biden's voice ahead of the New Hampshire Democratic primary
- FCC cited violated violation of 47 CFR § 64.6301(a), also known as STIR/SHAKEN

Prompt Injection Attacks

Multimodal and CV systems expand attack surfaces – including images, audio, and video – where malicious inputs can hide and manipulate AI behavior.

Current Regulatory Landscape

- 18 U.S.C. § 1030, the Computer Fraud and Abuse Act (CFAA)
- **FTC Section 5** enforcement actions related to cybersecurity hinge on questions of "reasonable" cyber practices

Danger of Prompt Injection Attack

- In safety-critical systems (e.g., autonomous vehicles, surveillance), a prompt-injected sign could mislead the AI into dangerous behavior

Surveillance and Biometric Identification

As multimodal AI and CV systems evolve, biometric data becomes a powerful yet dangerously persistent identifier—one that can be collected invisibly, misused globally, and spoofed convincingly.

Current Federal Regulatory Landscape

- BIPA
- FTC Section 5
- Article 5 of the AI Act (EU)
- HB1202 (MD)

Current State Regulatory Landscape (Examples)

- Illinois's BIPA
- Maryland's Prohibition of Use of Facial Recognition Services (HB1202)
- Washington Biometric Privacy Protection Act (HB1493)
- Texas Capture or Use of Biometric Identifier Act (CUBI)

Clearview AI

- January 2020 *New York Times* article revealed that Clearview used unconsented biometric information scraped from the internet to provide law enforcement and private companies with FRT to identify individuals who have purportedly committed a crime
- Raised First and Fourth Amendment concerns
- Tech giants halted selling FRT to police and called for further regulations from Congress

RiteAid

- In December 2023, FTC alleged that RiteAid's use of Facial Recognition Technology, intended to identify shoplifters, was an unfair practice under Section 5 as RiteAid failed to implement reasonable safeguards to prevent false positives

Immunity and Liability

MM and CV Models introduce novel theories of liability in copyright/trademark laws, tort claims, and privacy liabilities due to the magnified risk of harm to users from scaled, multi-pronged, and multi-faceted AI capacities.

Section 230 Content Liability

Fair Use and Copyright Claims

Tort Liability and "Black Box" Issues

04.

Case Studies and Predictions

Smart Cities, Autonomous Vehicles, and National Security

FRESHFIELDS

Thank you

This material is provided by Freshfields, an international legal practice. We operate across the globe through multiple firms. For more information about our organization, please see https://www.freshfields.com/en-gb/footer/legal-notice/.

This material is for general information only. It is not intended to provide legal advice.

Attorney Advertising: Prior results do not guarantee a similar outcome.