AI & Liability:

Emerging Challenges and Trends in US AI Litigation

Janice F. Mulligan
Lexis US West

A roadmap for this presentation:

- ✓ US law & AI litigation
- ✓ Why negligence is often pled
- ✓ FTC's current focus
- ✓ The battle over AI training data/algorithms
- ✓ Some high-risk areas of AI litigation
- ✓ "Takeaways"

Caveat: This presentation is *not* intended to offer legal advice for any specific case and it is for general educational purposes only.

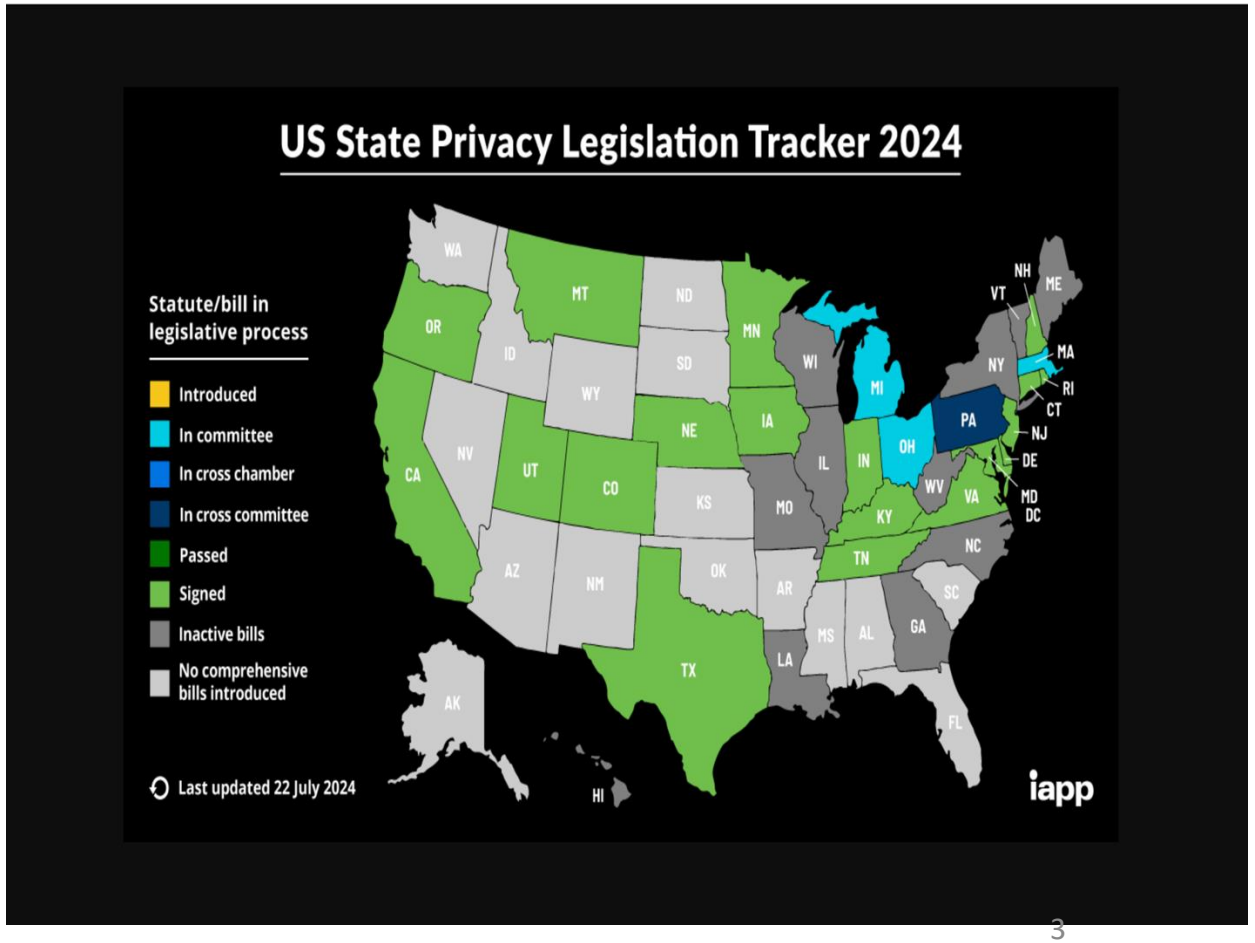
US Law & AI Litigation

Comprehensive AI Regulation
Builds on Comprehensive Privacy Regulation:
the US has Neither

The US relies on a ***patchwork*** of:

- ✓ **12+ sector-specific federal privacy laws** (health, banking, etc)
- ✓ **20 comprehensive state privacy laws**
- ✓ **3 state biometric laws**
- ✓ **1 state comprehensive AI laws**

LEXING NETWORK



The lack of comprehensive federal US privacy and AI laws *has not prevented AI litigation*

Some estimates are as high as 1000 US AI cases filed by the end of 2024

Today's analysis reviews highlights from the George Washington Law School's ongoing Database of AI Litigation (DAIL), which ***includes 195 US AI cases***

Other cases of note are also included

Because there is a separate Lexing IP panel, *IP is mostly excluded from this presentation*

DAIL's database shows a **lack of comprehensive privacy and AI regulation does *not prevent litigation***

Federal and state statutes

- ✓ Civil Rights Statutes
- ✓ **FTC Act, Section 5**
- ✓ Electronic Privacy Communications Act
- ✓ **Antiterrorism Act**
- ✓ Wiretap Laws
- ✓ **Computer Fraud and Abuse Act**
- ✓ State privacy & biometric laws

"Traditional" theories:

- ✓ Negligence
- ✓ **Invasion of privacy**
- ✓ Conversion
- ✓ **Contracts: breach implied warranty**
- ✓ Fraud
- ✓ **Property-based claims: theft, stolen property**
- ✓ Product liability: failure to warn/ design defect
- ✓ **False arrest**

Negligence is often included in US litigation, and it can *help businesses*! *Why?*

Of the 195 DIAL AI lawsuits, ***28 pled negligence***, along with a multitude of theories of liability

Plaintiff's attorneys will often include this theory of liability to trigger a defendant's insurance policy

While many AI theories of liability may not be covered by insurance, **negligence is covered** *if there is a plausible factual basis to support the theory*

If negligence is pled, a Commercial General Liability insurance policy (CGL) is often available to *pay the expensive cost of defense of the lawsuit,* sometimes with a reservation of rights as to whether the insurer is responsible for all or a part of any judgment

***Some of the many AI cases where negligence was pled with multiple other theories*:**

A.T. v. Open AI LP: Class action training Gen-AI with PI without consent

Chabon v. OpenAI Copyright infringement

Cousart v. Open AI: Web scraping to develop AI

Doe 1 v. Github: Training Codex, Copilot Gen Ai

Parsa v Google: Developing code/algorithms to polarize hate among political parties

PM v. Open AI: Lack of consent using PI

Tremblay v. Open AI: Copyright infringement

….. And the negligence case list goes on and on

DAIL Case Summary by Category

Data Privacy 59 cases: Focusing on the unauthorized use, collection, or disclosure of personal data, these cases often involve breaches of privacy policies, cybersecurity failures, compliance with regulations, and improper handling of personal information (PI)

Biometric Privacy 43 cases: Involving the use, collection, and storage of biometric data, such as facial recognition, fingerprints, and iris scans. Typically, they center on privacy violations, unlawful data collection, improper handling of sensitive biometric information, and claims under biometric privacy laws (eg Illinois' BIPA statute)

Intellectual Property (IP) 40 cases: Relating to trademarks, copyrights,& trade secrets involving AI technologies and encompass disputes over ownership, infringement, and use of AI in creating IP. Copyright cases typically involve disputes over the ownership of AI-generated works or the unauthorized use of copyrighted material by AI models

Employment Law 23 cases: Addressing issues such as workplace automation, the use of AI in hiring or performance management, and wrongful termination due to AI-driven decisions

Consumer Protection 23 cases: Focusing on claims against AI-powered consumer products or services, involving defective products, false advertising, AI misrepresentation, or deceptive practices in the sale of AI products

Civil Rights 7 cases: Involving bias or discrimination in housing, employment, and other sectors, often resulting from biased AI algorithms

From a drop in the bucket, a watershed "tipping point" is expected in US AI litigation

Existing US AI litigation is literally a "drop in the bucket," given that more than ***100 million civil cases are filed in the US every year*** *

Legal scholars predict a watershed in new US AI litigation…*soon*?

*Alliance for Justice, State Courts Hub www.afj.org.

Why is a surge of AI litigation expected in the US and *why* should you care?

Why a Surge in US AI litigation is expected:

-AI is in high demand

-Existing "test" cases may establish future precedent for others to follow

-Many novel legal theories are still untested

-AI isn't reliable, leaving itself open to litigation (eg hallucinations)

Why should you care?

When courts step in and tell us what is *permitted* and what is *forbidden,* developers, innovators, and deployers ***may need to change their approach*** in the US.

FTC’s current focus

In 2024, the US Supreme Court ***weakened all federal agencies' powers***

- ✓ ***No more broad deference*** *to* agencies' interpretation of statutes, *now "modicum of deference" Loper Bright Enterprises v. Raimondo*
- ✓ ***Strict limits*** *on internal investigations, adjudication of violations, and imposition of penalties SEC v. Jarkesy*
- ✓ ***New and explicit Congressional mandates are required*** *for "novel" issues, including AI*
- ✓ ***These rulings apply to the Federal Trade Commission (FTC),*** *the primary agency that regulates privacy and AI in the US*
- ✓ ***The FTC prosecutes via the FTC Act for "unfair or deceptive acts or practices"***

LEXING NETWORK

Three months after the USSC rulings, the FTC *escalated enforcement* with "Operation AI Comply"

No AI Lawyers: Charges levied against an AI service that claimed **"the world's first robot lawyer," with no human oversight.** It failed to live up to its claims that it could substitute for the expertise of a human lawyer. A quick settlement resulted in payment of $193,000 and notice to consumers who subscribed to the service warning them about the limitations of law-related features *FTC v. DoNotPay*

No AI Online Store Fronts: Three online business opportunity schemes all claimed their "cutting edge" AI-powered tools would help consumers quickly earn thousands of dollars a month in passive income by opening online storefronts. According to FTC's charges, the Ascend Form scheme **defrauded consumers of at least US $25 million and the Ecommerce and FBA schemes defrauded consumers out of unspecified "millions".** The cases are all pending in US federal court *FTC v. Ascend Form, Ecommerce Empire Builders, and FBA Machine*

FTC is also “doubling down” on
AI generated reviews and testimonials

Rytr marketed **false AI-generated reviews** created for users to copy and publish online, featuring information that would deceive potential consumers who were using reviews to make purchasing decisions

Some of Rytr’s subscribers used the service to *produce hundreds, and in some cases, tens of thousands, of reviews potentially containing false information*, although ***there was no evidence of actual harm***

Settlement is pending, which **forbids Rytr from marketing a version used to create product and service reviews *and waiving all right to judicial review***

FTC v. Rytr.

A case to watch:
FTC, data brokers, and geolocation data

The ability to track individuals to sensitive locations puts their privacy at risk. Kochava Inc. is a data broker that sells users' sensitive geolocation data

The FTC filed a lawsuit against Kochava, alleging ***it failed to properly anonymize the location data it sold,*** which made it possible to identify and track people visiting abortion clinics or addiction recovery centers

If the FTC wins, it could result in:

- ✓ **Stricter privacy standards for the collection and sale of geolocation data**
- ✓ More robust rules around data anonymization and consumer consent
- ✓ ***Enforcement actions against other data brokers engaging in similar practices***

The battle over AI training data/algorithms

How to keep your proprietary training data confidential….. ?

✓ Excluding IP cases, generally, *a US court is* ***more likely to keep the training data confidential if:***

It is intended for ***consideration by an intermediary professional who*** considers the training data together ***with other comprehensive data***

The Wisc. State Supreme Court rejected a post-conviction due process challenge to the state's criminal sentencing use of the COMPAS risk assessment algorithm. Loomis v. Wisconsin. The USSC denied review. ***This case has been followed by other courts***

✓ The training data ***will more likely be ordered disclosed if****:*

The output is used to ***"redline"*** *(withhold key resources from groups of people based on race, age, sexual orientation, etc.)* ***and*** *it is the only data considered*

Multiple ***civil rights*** *decisions ordered the data to be released were then settled. e.g. Flores v. Stanford Open The issue in pending in a* ***class action employment case*** *Mobley v. Workday*

Some high-risk areas of litigation

High-risk AI litigation involving "*sensitive data*" causes a ***heightened potential for liability*** because it often involves significant concerns around safety, fairness, privacy, and societal impacts

Of the various types of sensitive data, today we will discuss:

- ✓ **Biometric data**
- ✓ **Healthcare data (Protected health information or "PHI")**

High risk: biometric data

AI systems that collect or process biometric data (such as facial recognition, fingerprints, and voiceprints) are highly scrutinized. Unlike some other categories of personal data, ***biometric data is unique and generally cannot be changed***

Misuse or breaches of biometric data can lead to ***significant privacy penalties and class action lawsuits***

High risk: AI and facial recognition technology

Aside from IP cases, litigation involves biometric data in multiple types of cases including:

- ✓ **Privacy violations for lack of consent**
- ✓ Violation of biometric laws such as **BIPA or state privacy statutes**
- ✓ **Civil rights violations for bias in housing, benefits, wrongful arrest**
- ✓ Consumer protection claims for **deceptive or unfair practices**
- ✓ **Employment cases including hiring and monitoring**
- ✓ **Product liability lawsuits** for error in facial recognition software

Common themes: Lack of consent, lack of human oversight, incorrect identification

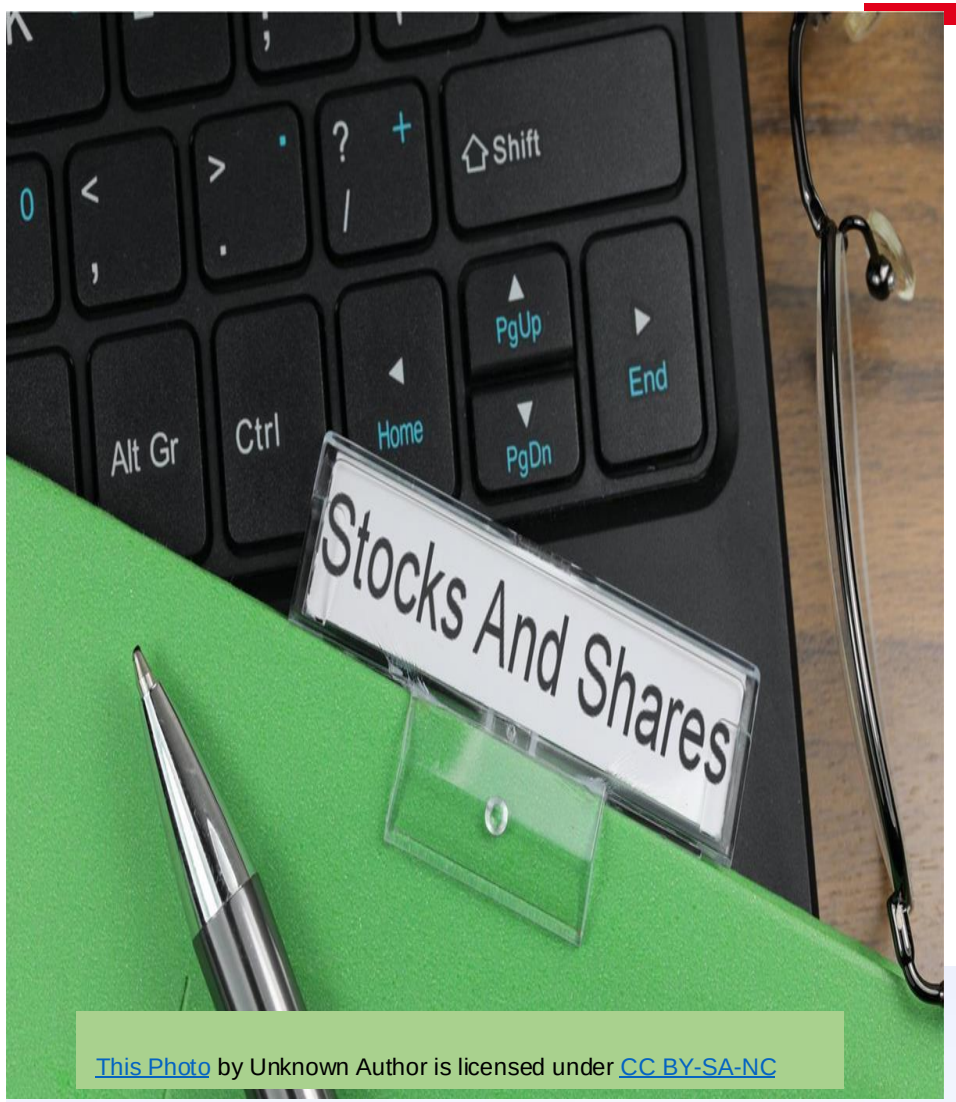
Creative & costly settlement: Clearview AI class actions

Clearview is a global biometric database company that collected facial images from websites and used the images to create a searchable facial recognition biometric database that it sold to both law enforcement and private companies

It recently agreed to pay more than **US$50 million** to resolve four biometric privacy class action lawsuits

As a term of the settlement, class members in four states can receive a pro rata share of the settlement fund ***in the form of stock in the company***

Settlement approval hearing is set for January 2025



More than money is at stake….
Algorithmic and database disgorgement

There have been *at least 16 AI lawsuits against Clearview* filed by the FTC, individuals and class actions. In addition to money, settlements included the following measures:

- **A permanent ban** on selling or granting access to its facial recognition database to private entities and a **five-year ban from granting access to its database to any governmental entities in Illinois**

- **Deletion of all facial vectors in its app in some states.**

Clearview is not a unique case: The FTC recently demanded that Weight Watchers **delete any models or algorithms developed in whole or in part using PI collected from children** in violation of the Children's Online Privacy Protection Act (COPPA)

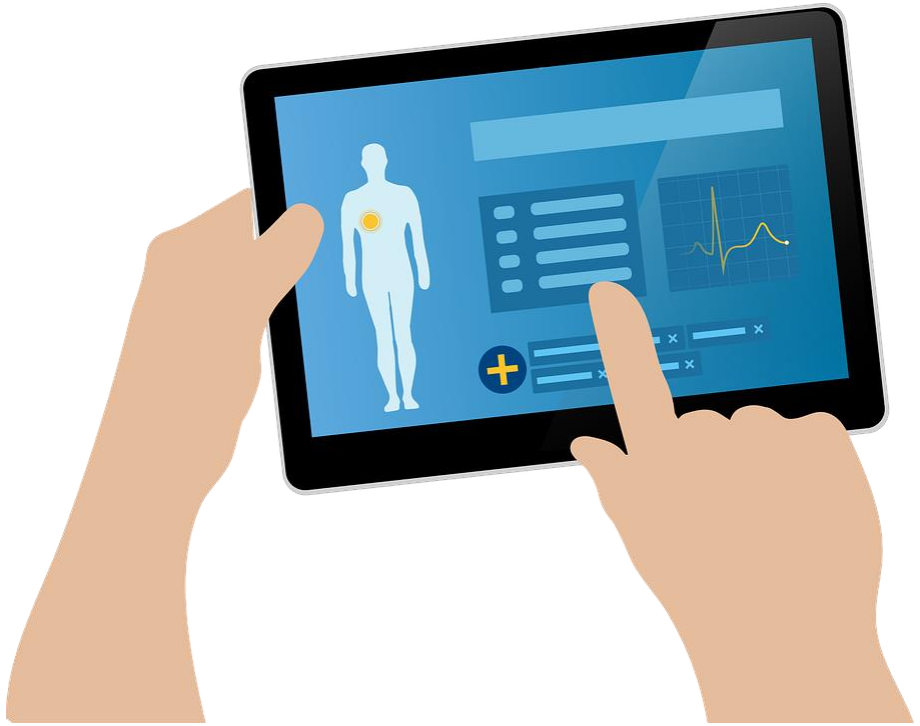
High Risk: Healthcare data

Protected health information (PHI), is sensitive data in a medical record set that can be used to *identify an individual* and that was created, used, or disclosed in the course of *providing a health care service such as diagnosis or treatment*

PHI class actions include:

-ADMT

-Pixel Litigation



Automatic Decision Making Technology (ADMT) "claims data activator" AI litigation

ADMT software "streamlines" the prior authorization process of insureds' claims and enables the ***denial of coverage en masse*** for treatments, medications, and testing *that do not match the preset criteria that AI was given.* ***There is no human oversight of the ADMT software***

A class action has been filed in California against Blue Shield for an alleged "illegal scheme" of implementing ADMT to instantly reject claims "on the lack of medical necessity" even though treating doctors provided documentation as to why medical treatment is medically necessary *Jong v. Blue Shield*

A separate class action suit is also pending on similar charges in federal district court in Kentucky *Barrows v. Humana*

Class Action Healthcare Data Privacy Claims Involving META PIXEL

Meta Pixel is a tracking code that website owners embed in a website to gather and share data with Meta.

Example: If a user clicks on a breast cancer video, Meta Pixel shares the data regarding the fact that the user clicked on it, what the video was about, the URL visited, and embedded metadata regarding the webpage. *Frequently, the user received targeted advertising about breast cancer which was the subject of the video*

664 hospital systems **used this tool to send sensitive data to Facebook.** In 2022, Mass General Hospital settled a pixel class action brought by patients for **US$18.4 million** and the Advocate Aurora Health settled for **US$12.225 million** ***in a class of ~2,500,000 people***

After these settlements, healthcare website tracking lawsuits exploded, ***with cases pending across the US***

Because users' PHI is implicated by their licensed healthcare providers, sharing the data is a violation of federal HIPAA privacy, a breach of common law torts, and a violation of some state privacy laws

Meta's defense: Meta discloses to website owners (hospitals) that it configures its pixel to share data with Meta. The website owner can re-configure the Meta Pixel to share less, and Meta's terms and conditions *warn not to use it with sensitive data*. **At least one hospital, Palomar Health, won the suit on technical grounds**

Takeaways

- ✓ **American law surrounding AI is still very unclear although litigation is expanding quickly**
- ✓ **Get a Commercial General Liability insurance policy (CGL) if you are doing business in the US**
- ✓ **Courts prefer to decide cases on procedural grounds** (jurisdiction, standing) so have your lawyers file strong procedural motions *when applicable*
- ✓ **Human oversight** improves the odds of not being sued or winning the case
- ✓ Requiring an **"intermediary professional"** rather than the lay public access to the AI system reduces liability

More Takeaways:

- ✓ One way businesses can comply with state biometric data laws and state privacy laws is by **implementing blanket policies that comply with the most stringent state data regulations** (eg Illinois on biometrics)

- ✓ **Make sure that terms and conditions, privacy policies, and notices fully disclose the use of AI** (*see Meta's winning defense above in pixel litigation)*

- ✓ **Consult a Lexing US lawyer… Jennifer and I are available to assist you** in different parts of US and with different practice areas.

After 30+ years of California and federal health law and privacy trial experience *on behalf of consumers*, I am now available to draft policies and contracts that comply with California law. With my vast network of legal specialists, I try to help you avoid litigation. I also specialize in litigation strategy and monitor litigation and trials across the US.

Merci pour votre attention ! Des questions ?

Thank you for your attention! Do you have any questions?