

# Cooley



## The Data Evolution: Data Privacy and Cybersecurity in the AI Era

attorney advertisement

Copyright © Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.

# Speakers



**Michael Egan**  
Partner  
Cooley LLP  
Washington, DC  
megan@cooley.com



**Liza Cotter**  
Associate  
Cooley LLP  
Boston, MA  
ecotter@cooley.com



**Mary Ann Le Fort**  
Chief Privacy Officer  
Priceline.com LLC  
Norwalk, CT  
maryann.lefort@priceline.com

# Disclaimer

These materials are intended as an introduction to the subject matter covered in the presentation. The presentation and the materials contained herein do not attempt to provide legal advice for any particular situation. Each situation must be analyzed individually in light of all of the surrounding facts and circumstances. Because of the complexity of the legal issues related to the subject matter hereof, it is critical that counsel be involved. These materials are provided for educational and discussion purposes only and are not to be copied, used or distributed outside of this seminar without the express written consent of Cooley LLP.

# Agenda overview



- Industry developments
- Core privacy/cyber risks
- Consequences
- Risk mitigation



“Photograph of a man in a suit standing on a sandy beach. He is facing the ocean, and only his back is visible. The tide has receded hundreds of yards. In the distance a large tsunami is approaching.” – via Midjourney

... and via Runway Gen-2

# Checking the pulse of the AI revolution

Cooley



# Where we were a year ago...

The New York Times

NEW YORK

Intelligencer

SCREEN TIME | SEPT. 19, 2022

AI Art Is Here and the World Is Different How we work — even changes when we can instantly convincing images into existence

By John Herrman



## OpenAI Rival Anthropic Funding at \$4.1 Billion Valuation

By Kate Clark | March 8, 2023 1:37 PM PST

Photo: Dario Amodei, CEO and co-founder of Anthropic. Photo: YouTube/Centre for Effective Altruism.

GatesNotes THE BLOG OF BILL GATES

LOG IN

SIGN UP



PERFECT

THE HIGHLIGHT

MORE

Give



A NEW ERA

## The Age of AI has begun

Artificial intelligence is as revolutionary as mobile phones and the Internet.

By Bill Gates | March 21, 2023 • 14 minute read



In my lifetime, I've seen two demonstrations of technology that struck me as revolutionary.

more widely available to the public in the coming weeks, a Monday blog post stated.

## Let the AI Gold Rush

US Edition

Your Account

Subscribe

Economics Industries **Technology** Politics Wealth Pursuits Opinion Businessweek Equality More

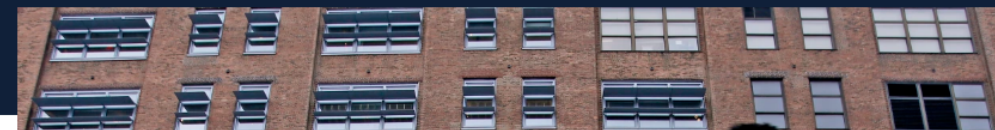
## Targeted in FTC Complaint halt of GPT Rollouts

nes after AI experts called for a temporary pause this week to look closely at growing AI industry

and Edward Ludlow

:36 PM PDT Updated on March 30, 2023 at 6:38 AM

technology to "trusted testers" ahead of making it



# Where we were a year ago... (cont'd)



"A photograph of an adorable English Bulldog puppy wearing a raincoat." – via Midjourney



"Detailed, high resolution photograph of an elephant in a kayak on the high seas." – via Stable Diffusion



"Oil painting representing the societal impact of Generative AI." – via DALL-E



"Photograph of an elderly British nature documentary narrator." – via DALL-E

J Write an explanation of the themes of *Bartleby, the Scrivener*



Certainly! "*Bartleby, the Scrivener*" by Herman Melville is a rich text filled with multifaceted themes. Here's a breakdown of some of the story's primary themes:

1. **The Dehumanizing Effects of Capitalism and Modernization:**

Set against the backdrop of Wall Street, Melville offers a critique of a burgeoning capitalist society. The repetitiveness of Bartleby's job as a copyist serves as a metaphor for the mechanized, rote tasks of modern workplaces, which can strip individuals of their humanity and individuality. Bartleby's eventual refusal to work can be interpreted as a silent protest against this dehumanization.

2. **Isolation and Alienation:**

Throughout the story, Bartleby becomes increasingly isolated, both physically and emotionally. This isolation underscores the broader theme of alienation in the urban environment. Even as cities become crowded, individuals can feel more alone and disconnected. Bartleby's silent presence in the law office, and later in the prison, serves as a powerful symbol of this urban solitude.

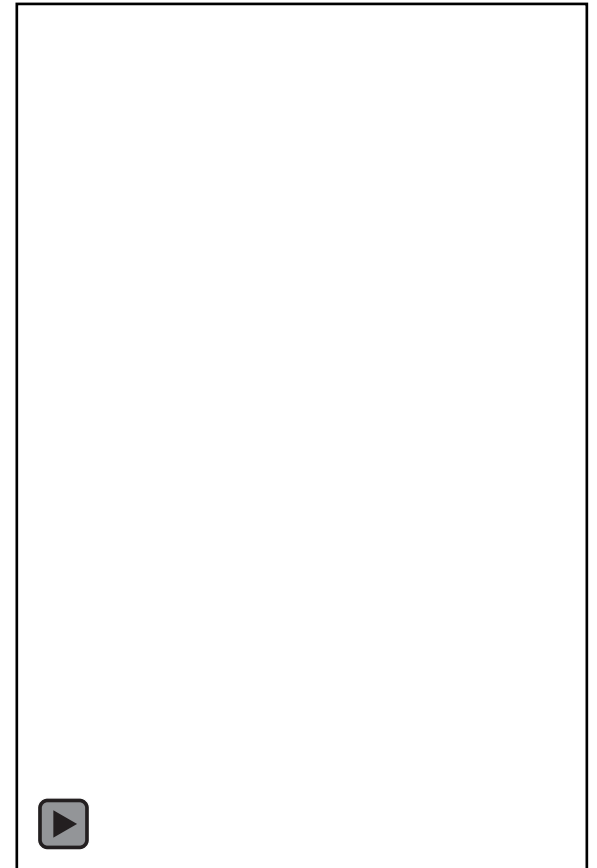
3. **Resistance and Non-conformity:**

Bartleby's consistent response of "I would prefer not to" whenever asked to perform a task is an act of passive resistance. It's a quiet refusal to conform to societal expectations. His non-conformity is not loud or aggressive but is perplexing and powerful in its consistency, highlighting the inherent human desire for autonomy and the tensions that arise when individual will clashes with societal norms.

4. **The Limits of Empathy and Charity:**

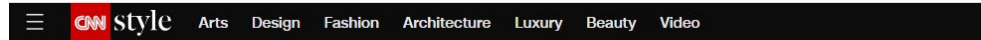
The lawyer's response to Bartleby is complex. On one hand, he demonstrates patience and a certain degree of empathy, attempting to understand and help Bartleby. On the other hand, he is also motivated by a sense of guilt and even fear. The story raises questions about genuine altruism and the boundaries

Stop generating



@unreal\_Keanu (TikTok)

# What's happened since...



FAKE

AI-GENERATED IMAGE

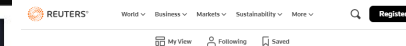


The false reports of the explosion also made their way to air on a major Indian television network. Republic TV reported that an explosion had taken place, showing the fake image on its air and citing reports from the Russian news outlet RT. It later retracted the report when it became clear the incident had not taken place.



AI-GENERATED FAKE IMAGE

A fake image purporting to show an explosion near the Pentagon was shared by multiple verified Twitter accounts on Monday, causing confusion and leading to a brief dip in the stock market. Local officials later confirmed no such incident had occurred. AI-Generated Fake Image/Twitter



### Getty Images lawsuit says Stability AI misused photos to train AI

By Blake Brittain  
February 6, 2023 9:32 AM PST · Updated 8 months ago



BOY COURT

### ChatGPT Is Making Up Lies — Now It's Being Sued for Defamation

A Florida radio host alleges that OpenAI's software concocted a story about him being accused of fraud and embezzlement, and he's seeking damages

BY HILLES KLEE

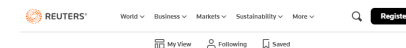
JUNE 8, 2023

CNN BUSINESS

### OpenAI, maker of ChatGPT, hit with proposed class action lawsuit alleging it stole people's data

By Catherine Thorbecke, CNN

Published 5:55 PM EDT, Wed June 26, 2023

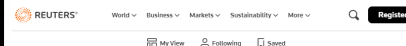


### Google hit with class-action lawsuit over AI data scraping

By Blake Brittain

July 11, 2023 6:09 PM PDT · Updated 3 months ago

Q Aa <



### Pulitzer winner Chabon, other authors sue Meta over AI program

By Blake Brittain and Katie Paul

September 12, 2023 11:13 AM PDT · Updated 18 days ago

Q Aa <



### John Grisham, other top US authors sue OpenAI over copyrights

By Blake Brittain

September 21, 2023 3:34 AM PDT · Updated 10 days ago

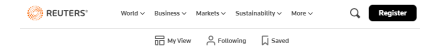
Q Aa <



### Reality Star Claims Deepfake App Violates Publicity Rights

Los Angeles Times

### Bestselling authors Mona Awad and Paul Tremblay sue OpenAI over copyright infringement

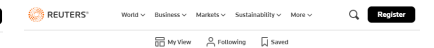


### Sarah Silverman sues Meta, OpenAI for copyright infringement

By Jack Queen

July 10, 2023 9:27 AM PDT · Updated 3 months ago

Q Aa <



### More writers sue OpenAI for copyright infringement over AI training

By Blake Brittain

September 11, 2023 12:33 PM PDT · Updated 19 days ago

Q Aa <



### OpenAI, Microsoft hit with new US consumer privacy class action

By Blake Brittain

September 6, 2023 12:52 PM PDT · Updated 24 days ago



Privacy risks

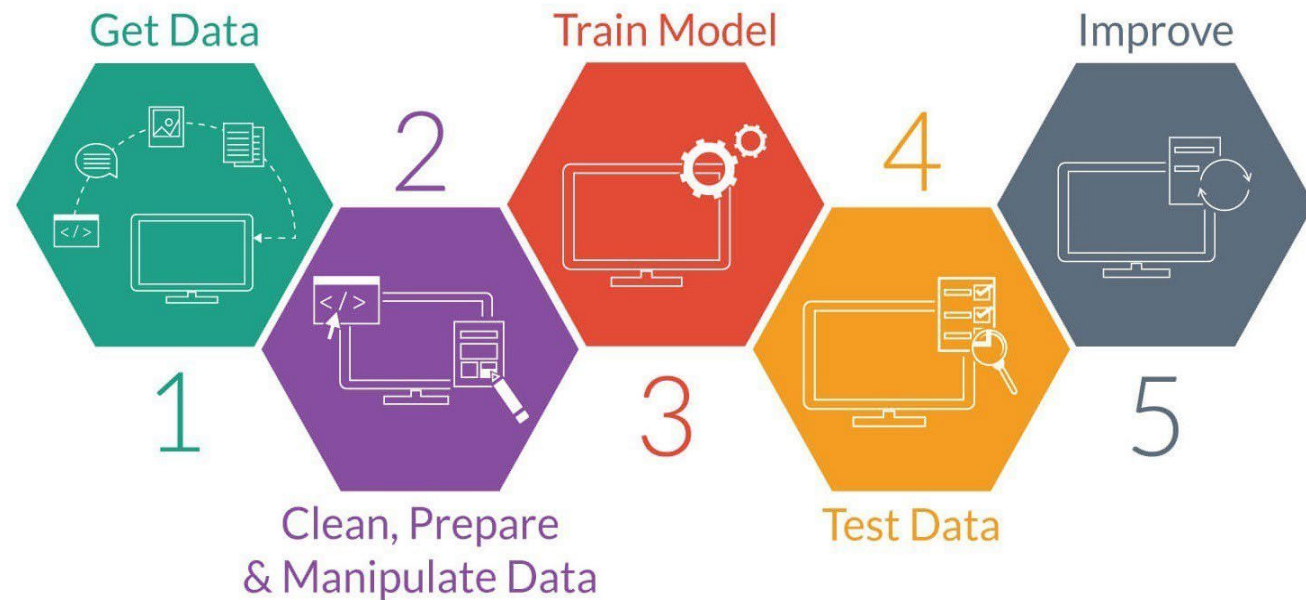
# Complex tapestry of privacy laws

- **More laws on national and global level**
  - Comprehensive US state consumer privacy laws
  - Omnibus foreign privacy laws (e.g., EU/UK GDPR, China's PIPL, Brazil's LGPD)
  - AI-specific laws (e.g., EU AI Act, Colorado's AI Act)
  - Other sector-/data-specific laws (e.g., Illinois's Biometric Information Privacy Act, children's data privacy laws, health data privacy laws, etc.)
- **Broad understanding of “personal information” or “personal data”**
  - Definitions vary but essentially any data that relates to an identified or identifiable person
- **More advanced processing techniques (AI/ML)**
- **More enforcement/litigation**

**SPOILER ALERT:** It's much harder for companies to process personal information, and privacy laws are cutting to the core of some business models

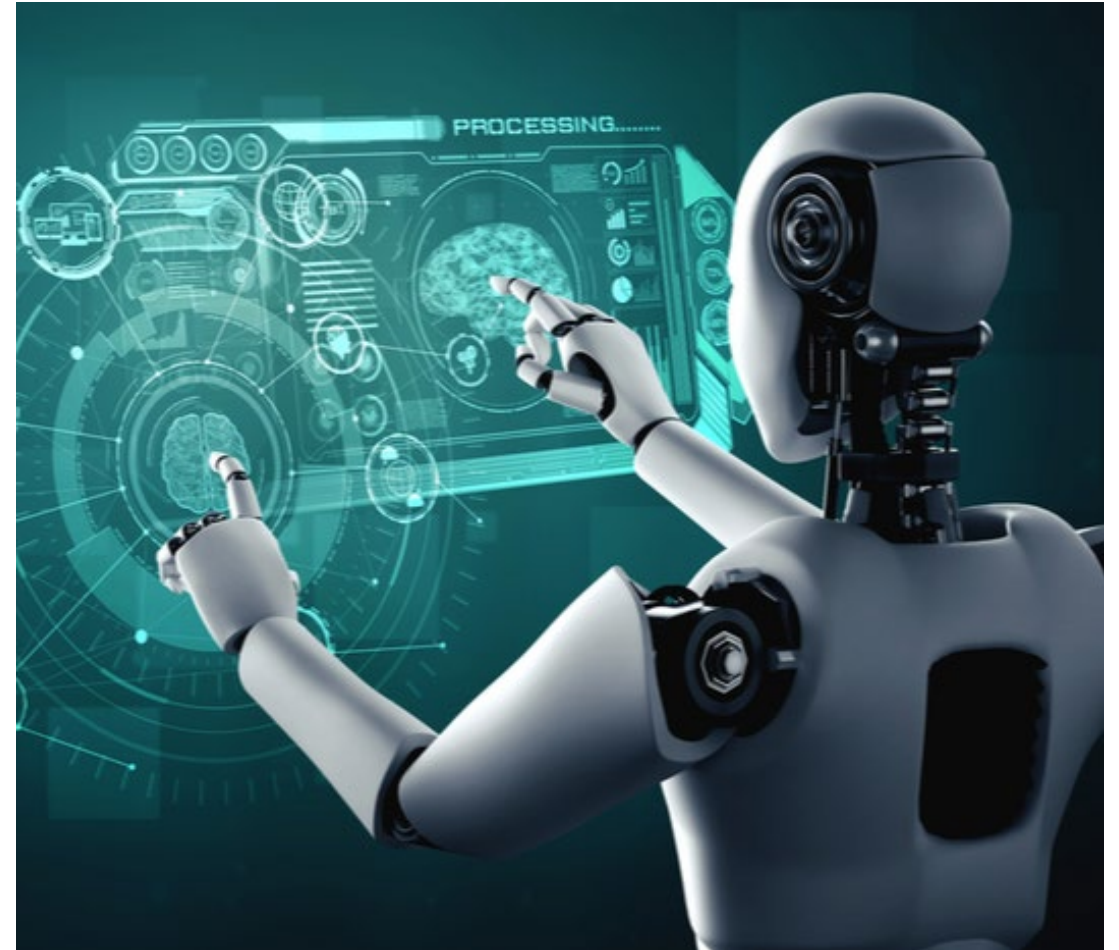
# Training data

- Privacy laws in the US and abroad provide individuals with certain rights with respect to their personal information
  - E.g.: access, deletion, correction, opt-out of certain automated decision-making/profiling, opt-out of sales/targeted advertising, etc.
- It may be difficult to fully comply with these rights where personal information is used to train AI
  - For example, can AI forget?
- Training alternatives?



# High-risk ADMT/biased AI

- Automated decision-making technologies (ADMT) are regulated by a growing body of laws.
  - Increasing number of laws aimed at preventing algorithmic biases/discrimination
  - Laws requiring risk assessments and imposing other obligations prior to deployment of ADMT used in connection with making consequential decisions or profiling
  - Laws providing opt-in/opt-out rights
  - Antidiscrimination laws





# High-risk ADMT/biased AI (cont'd)

- **Risk mitigation measures**

- Maintain records of processing mapping all data processing activities and the data types involved and identifying any processing that involves automated decision-making
- Perform data protection and other risk assessments prior to deploying higher-risk AI solutions
  - This is particularly true with respect to data processing activities that present a heightened risk of harm to consumers (e.g., where processing sensitive personal information or where engaged in automated decision-making or profiling that presents a risk of unfair or deceptive treatment, financial or physical harm, or other substantial injury)
  - Include: (i) the potential impacts on individuals, (ii) the legal bases under the GDPR (if any are available) on which the company may rely to engage in the processing, and (iii) how the company will obtain required consents and/or offer required opt-outs (including alternatives, such as human review, the company will offer should an individual not consent to the automated processing)
- Conduct bias audits pre- and post-deployment of AI solutions
  - Consider all types of biases (e.g., training data biases, biases in algorithmic design/development, biased output/outcomes)
  - Remember that real world data has baked in biases

# Biometric data

- No universal definition
  - Definition under Illinois's BIPA ---->
- Generally understood to mean data capturing a person's unique physical characteristics used for automated recognition or identification
- Commonly regulated types of biometric data include:
  - Retinal scans
  - Iris scans
  - Fingerprints
  - Voiceprints
  - Scans of facial geometry
- With growth of AI capabilities, what may be considered biometric data is being tested/expanded

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

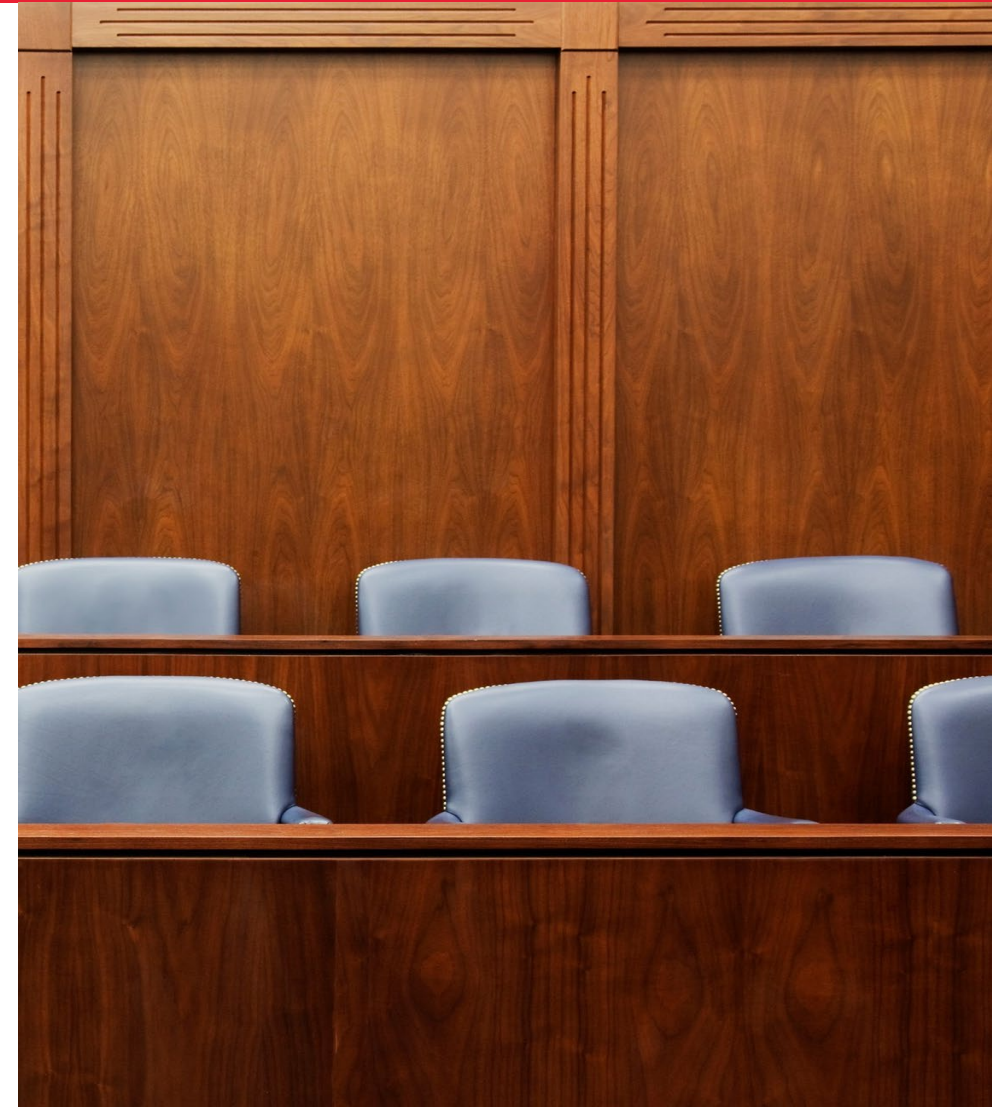
# Litigation/enforcement actions

- **Common claims (not exhaustive)**

- Wiretapping/eavesdropping
- Privacy tort claims (e.g., invasion of privacy and intrusion upon seclusion)
- Negligence
- Property – allegations that individuals have property rights in content they post online
- Consumer protection laws – alleged unfair/deceptive conduct
- Claims under biometric privacy laws

- **Algorithmic disgorgement**

- FTC trend in recent enforcement actions toward requiring companies that have trained on data obtained in violation of privacy and consumer protection laws to delete not only the underlying data but all algorithms/models trained on such data
  - *See, e.g., In re Everalbum, In re Flo Health, In re Rite Aid Corp.*



# Cyber risks



# AI and cybersecurity



- Data leaks/breaches
  - Could occur when data used to train is leaked to third parties, whether through intentional/malicious or inadvertent prompting of the model
- Model/data poisoning
  - Injecting training data with poisoned/inaccurate data or incorrect labels to cause the model to learn the wrong information
- Code vulnerabilities
- Deepfakes
- Hackers using generative AI tools to improve the sophistication of attacks
  - E.g., “ChatGPT: create a phishing email”

# AI and cybersecurity

TOP STARTUPS FOR THE ENTERPRISE | COUNCIL MEMBERS | FOUNDING MEMBERS | ADVISORY BOARD

NEWS

TECHNOLOGY EXECUTIVE COUNCIL

## 'Cyber-physical attacks' fueled by AI are a growing threat, experts say

PUBLISHED SUN, MAR 3 2024 10:05 AM EST

Kevin Williams

SHARE f X

### KEY POINTS

- FBI Director Christopher Wray said Chinese government hackers are targeting treatment plans, the electrical grid, transportation systems and other critical infrastructure inside the U.S.
- MIT researchers have simulated cyberattacks in the lab that can trigger fires and explosions in equipment such as motors, pumps, valves and gauges.
- Attacks on physical infrastructure would be tantamount to war, and so far, that's something nation-states have avoided.

Forbes

SPEAK TO A PARTNER

Advisory see and Exchange approval by Investing in

FORBES > INNOVATION

## How AI-Driven Cyberattacks Will Reshape Cyber Protection

Dewayne Hart Forbes Councils Member  
Forbes Technology Council  
COUNCIL POST | Membership (Fee-Based)

Mar 19, 2024, 09:45am EDT

f SEMAIS President and CEO.

## NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

...line learning" threats, describing mitigation strategies and their

...thy data, and attackers are exploiting this issue. ...ng with mitigation approaches. ...misdirection, and AI developers and users should be

MEDIA CONTACT  
Chad Boutin  
charles.boutin@nist.gov  
(301) 975-4261

# AI cyber risk mitigation

- Use hosted/walled-garden models
- Diligence third-party providers
- Red teaming
- Use open source with caution
- Employee training
- Regularly check training data labels for accuracy
- Fight AI with AI

# SEC cyber disclosure requirements

Disclosure item	SEC form(s)	Summary of disclosures
Material cybersecurity incidents	8-K	<ul style="list-style-type: none"><li>• Disclose material cybersecurity incident within four business days of determining materiality (subject to narrow national security and public safety delay exception)</li><li>• Describe the <i>material</i> aspects of the incident's (i) nature, scope and timing; and (ii) impact, or reasonably likely impact, on the company, including its financial condition and results of operations</li></ul>
Risk management and strategy	10-K	<ul style="list-style-type: none"><li>• Describe processes for the assessment, identification and management of material risks from cybersecurity threats</li><li>• Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected, or are reasonably likely to materially affect, the company's business strategy, results of operations or financial condition</li></ul>
Governance	10-K	<ul style="list-style-type: none"><li>• Describe management's role in assessing and managing material risks from cybersecurity threats</li><li>• Board's oversight of risks from cybersecurity threats</li></ul>



# Key terms

- “**Cybersecurity incident**”: an *unauthorized occurrence*, or a *series of related unauthorized occurrences*, on or conducted through a *company’s information systems* that jeopardizes the confidentiality, integrity or availability of a company’s information systems or any information residing therein
  - “Paper breaches”
  - Accidental/inadvertent disclosures
  - Unexploited vulnerabilities?
- “**Material**”: substantial likelihood that a reasonable investor would consider information important in making an investment decision or if the information would have significantly altered the "total mix" of information made available
  - SEC 2011 and 2018 cyber guidance discusses materiality for purposes of financial reporting
- “**Cybersecurity threat**”: any potential unauthorized occurrence on or conducted through a company’s information systems that may result in adverse effects on the confidentiality, integrity or availability of a company’s information systems or any information residing therein

# Q&A with Mary Ann Le Fort