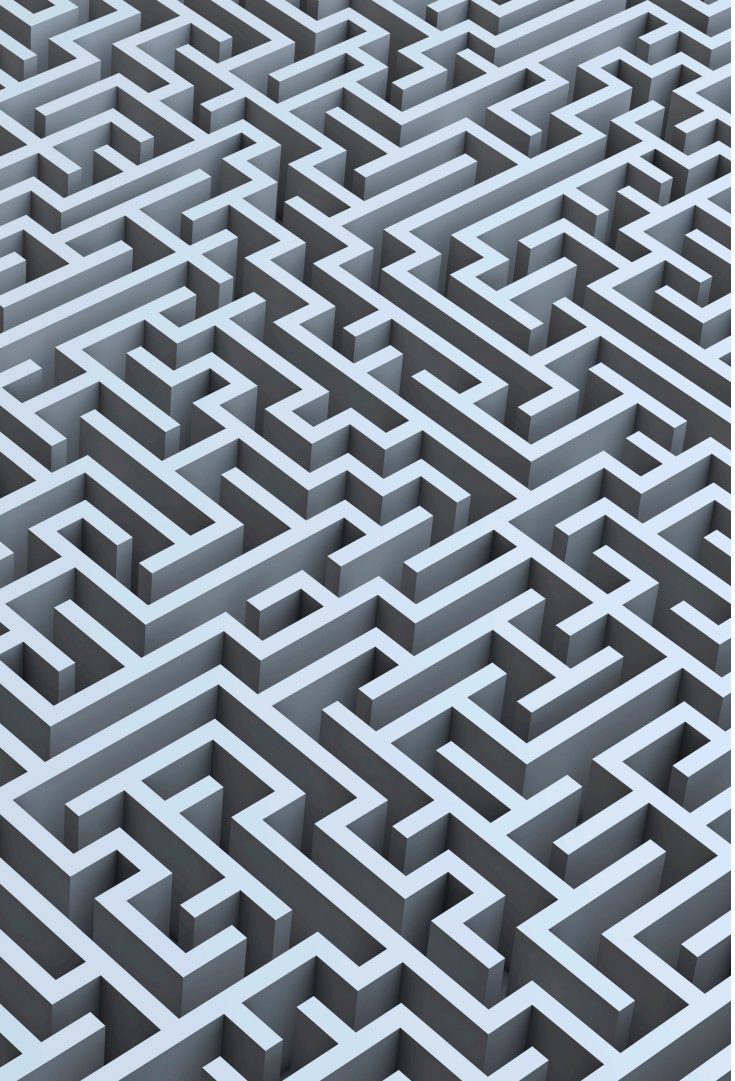
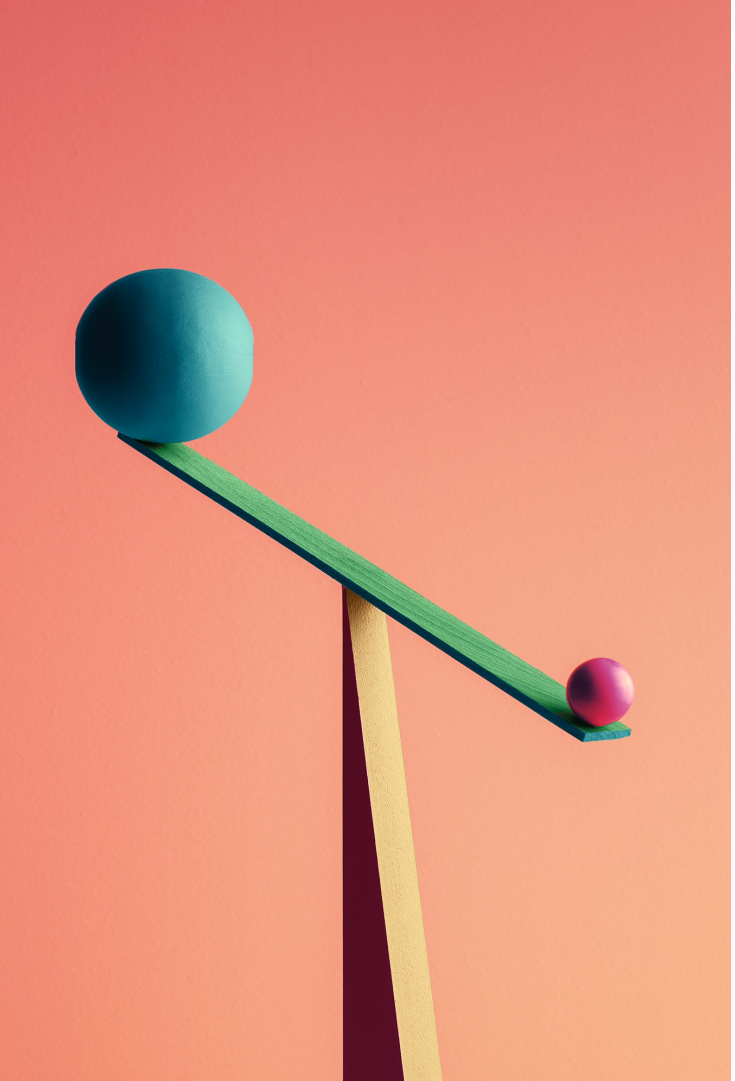
Key Legal Concerns with Artificial Intelligence Cybersecurity

- **Data Privacy and Confidentiality**
  - Building AI systems that comply with evolving data privacy and cybersecurity laws and regulations.
  - Managing client data protection (including through vendors) while being sufficiently transparent with regulators.
- **Data Security**
  - Data breaches affecting data sets containing sensitive information.
  - Data poisoning or adversarial attacks by malicious actors affecting the function of AI systems and manipulating outputs.
- **Liability and Accountability**
  - Determining liability in a cybersecurity incident affecting an AI product, from the developer to the user.



Artificial Intelligence Regulation is in its Infancy

- Before anything else: No one knows anything.
- One of the driving challenges is the difficulty in determining who is responsible actions of AI systems, or who can take credit for them.
  - For example: An attempt to patent AI-generated work was rejected by the U.S. Court of Appeals for the Federal Circuit, finding that the Patent Statute provides that "only a natural person can be an inventor, so AI cannot be."
- An increasing number of states and government organizations have begun including AI specific requirements in their data privacy laws.
- The few AI-specific regulations are focused on data privacy concerns or potential bias.



Artificial Intelligence Governance in the United States

- The U.S. approach to AI regulation has been partitioned, taking a sectoral and risk-specific approach.
- In late 2023, President Biden signed the "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," which includes provisions to:
  - "Require that developers of the most powerful AI systems share their safety test results [..] with the U.S. government."
  - "Develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy."
- On November 26, 2023, the U.S. DHS and the CISA released joint "Guidelines for Secure AI System Development" with the UK's National Cyber Security Center.

The European Union's Artificial Intelligence Act

- In May 2023, the EU Internal Market Committee and the Civil Liberties Committee adopted the AI Act.
- The primary aim of this legislation is to balance the benefits of AI use while ensuring that AI systems are "safe, transparent, traceable, non-discriminatory and environmentally friendly." (European Parliament)
- Approach of the EU AI Act
  - The regulation takes a risk-based approach to AI.
  - It would ban the use of AI for biometric surveillance, predictive policing or emotion recognition.

Uncertainties and Potential Conflicts Going Forward

- For the foreseeable future, litigations against AI companies for data privacy violations, bias, or copyright infringement may be the driver of transparency and accountability for organizations developing or using AI in the U.S.
- This delay in oversight or an explicit legal framework poses numerous risks and legal questions.
- Example: Delay in Google's AI chatbot, Bard, being offered in the E.U. due to privacy concerns as defined by the GDPR.

Daniel B. Garrie, Esq.
Law & Forensics LLC – Founder
JAMS – Neutral
Harvard - Faculty
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.