



Big Data, AI Tools, and Developments in Generative AI

ACC NCR - April 2, 2024

What a law firm
should be.



Self-Driving Cars



<https://www.latimes.com/business/la-fi-michigan-self-driving-20160907-snap-story.html>

Food Delivery Droids



<https://www.supermarketnews.com/online-retail/robots-take-streets-food-delivery-tests>

Pharmacy Droids



<https://ajp.com.au/in-depth/longer-read/robots-give-rise-future-pharmacy-dispensing/>

But AI is much more than just Robots

- Machine Learning
- Big Data Analysis
- Behavioral Analytics



Current Applications

- Natural-Language Processing for Research and Professional Decision Support
- Voice-to-Text Transcription
- Assisted Imaging
- Robot-Assisted Activities
- Fraud Detection
- Cybersecurity



Data Privacy Issues

- Data Aggregation: Is any information really de-identified?
- Machine Learning: How far should machine learning be allowed to go?
- Behavioral Analysis: AI predictive capabilities have privacy implications.
- Other Potential Data Disclosures: To whom is your robot giving your data?
- Contractual Issues: Is the disclosure of data to the AI tool permissible?



Data Security Issues

- Networked Devices: IoT devices are generally vulnerable.
- Risk Analysis and Risk Management
- Access Controls
- Data Repositories: Large amounts of data mean large amounts of risk.
- Back Doors: Who built your robot?
- Machine Learning: The dark side can use it too!



Other Potential Issues

- AI and Machines Only Do What you Tell Them To Do!
- Who's your engineer?
- Societal Implications: “Diminished Resilience.”
- Unintended Consequences: Discrimination/Bias



Legal Risks

- Privacy Violations and Enforcement
 - The HHS, FTC, DOJ, and State Attorneys General all have (and have exercised) authority to enforce privacy rules and promises.
- Upstream Contractual Breaches
 - Downstream secondary uses and disclosures of data can run afoul of upstream contractual limitations leading to disputes and damages.
- Increased Risk of Data Breach
 - As data flows through the chain of custody, risk of unauthorized access and acquisition of data grows as evidenced by increasing breaches occurring at the vendor level.
- IP issues
- Reputational Damage
 - Even where no law or regulation is violated, the court of public opinion may frown upon unethical uses and sharing of data.



Prohibitions on Sale of Data

- **SALE OF IDENTIFIABLE INFORMATION IS GENERALLY PROHIBITED BY STATE, FEDERAL, AND INTERNATIONAL LAW**
- Direct OR Indirect Remuneration is considered a “sale”
- State Law Requirements for Consent
- Federal Law Requirements for Consent or Authorization
 - HIPAA, FERPA, FTC Requirements
- International Law Requirements for Consent
 - GDPR and Other Countries



Vendor Requests for De-identified Data

How does a data owner consider request for its de-identified data by a vendor or other business partner?

How does a vendor or other business partner request such data?

- What is the value of the de-identified data to be provided to the vendor?
- What does the license for such data look like?
- What remuneration should be considered?
- What other “guardrails” should be contemplated for the relationship?



Who Owns the Data and the Work Product?

- Ownership/license rights to ‘results’
 - Modified data (structured data, de-identified data)
 - What if the data is combined with data from third parties?
 - Tools used to work with the data
 - Updates to the tools/AI engines
 - Results/insights learned from access
- **In each case, whether or not you receive ownership rights, consider preserving your own use rights, and understand any limitations on your ability to use, to share with others.**



Questions?



Iliana L. Peters, J.D., LL.M., CISSP

ipeters@polsinelli.com

202-626-8327

