



AI Impact on Privacy

Katy Ruckle, JD, FIP

State Chief Privacy Officer

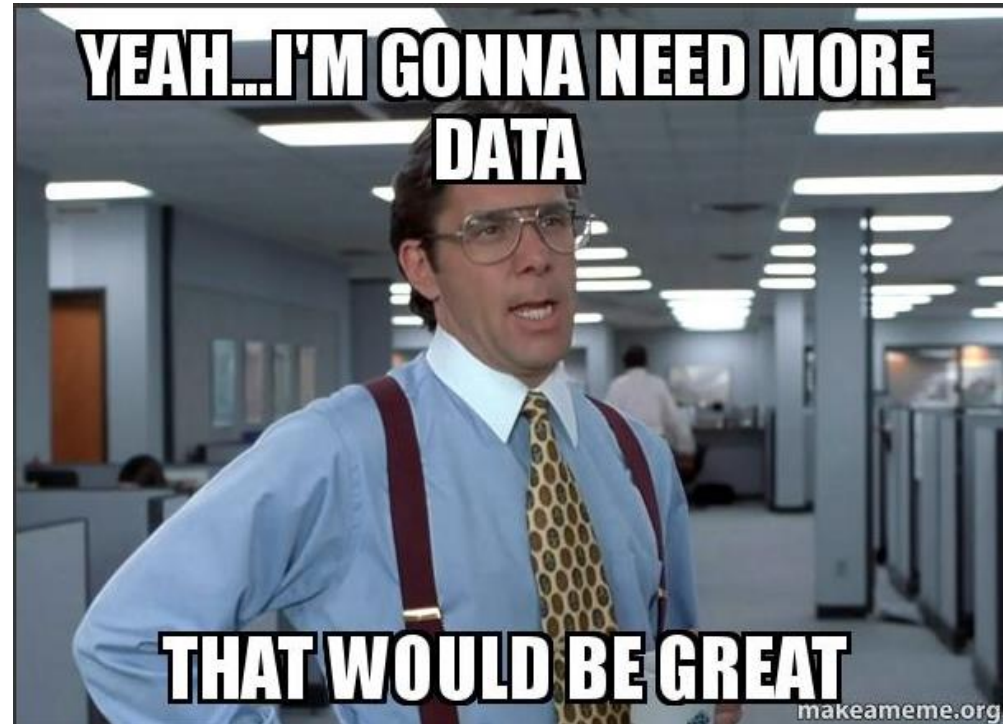
Cybersecurity Awareness Month Presentation

October 17, 2023

What are the
privacy implications
of using AI?

More data is
needed to:

- ✓ Build AI
- ✓ Train AI
- ✓ Maintain AI



What is the issue with more data from a privacy perspective?

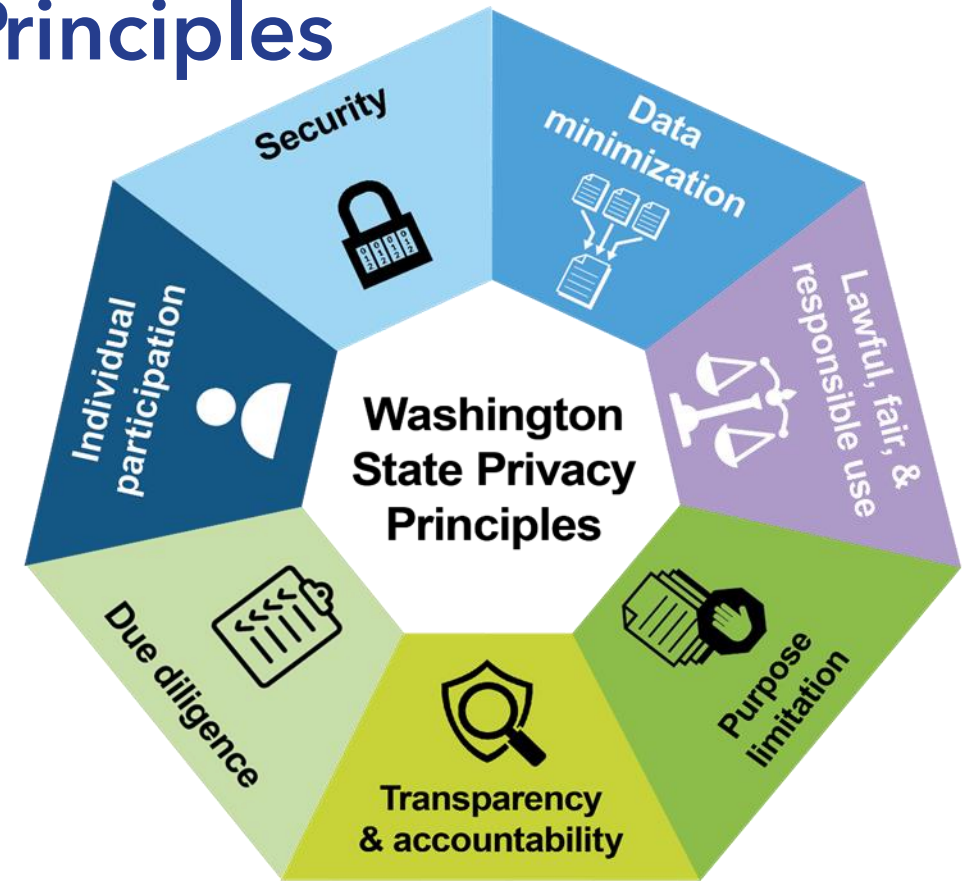
- **Risk of**

- **Data persistence**
- **Data repurposing**
- **Data spillovers**
- **Data commingling**
- **Data integrity**



Washington State Agency Privacy Principles

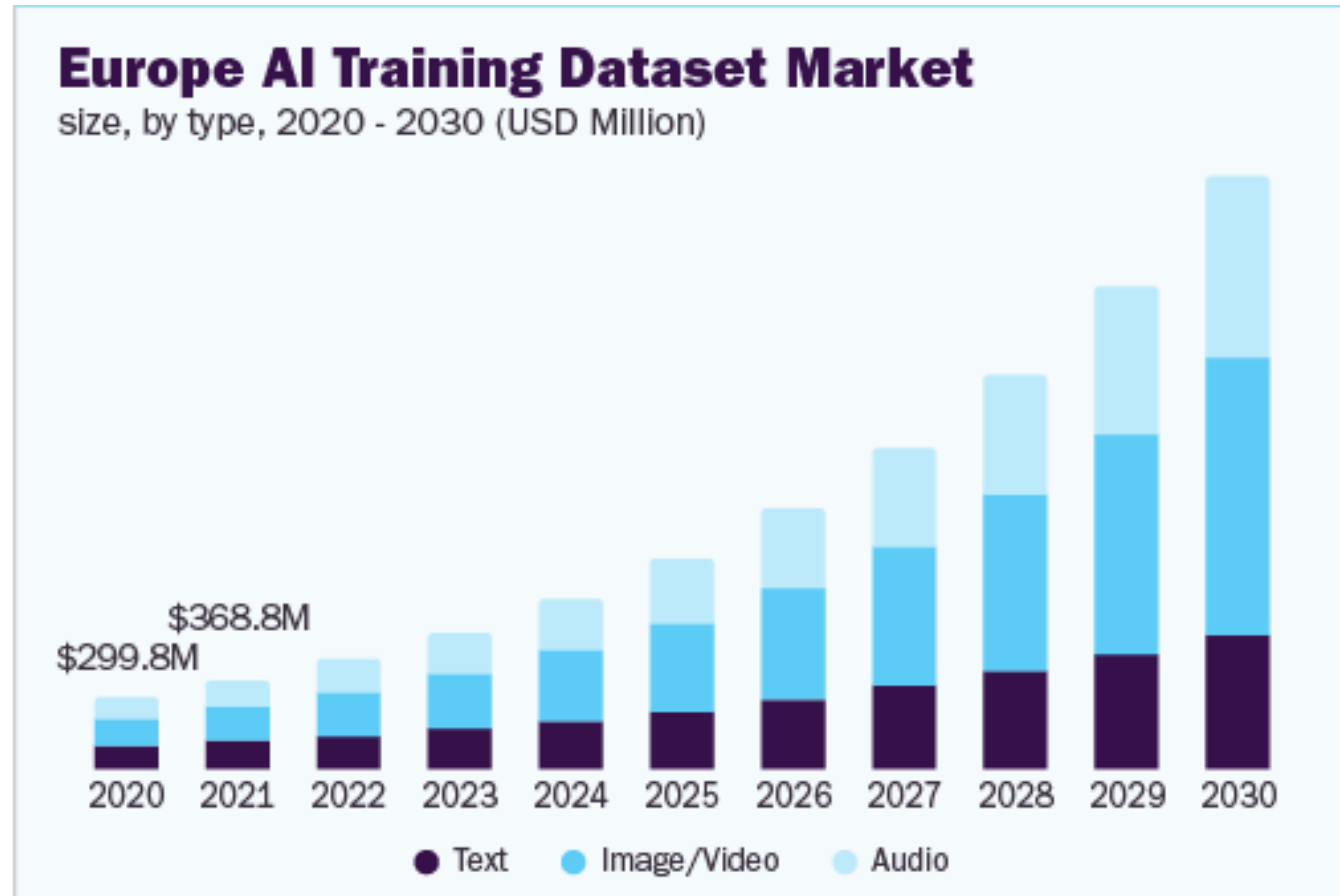
- Lawful, fair, & responsible use
- Data minimization
- Purpose Limitation
- Transparency & accountability
- Due diligence
- Individual participation
- Security



[Washington State Agency Privacy Principles](#)

Growing demand for Data

- Application specific training data needed to support machine learning processes
- Data types
 - Text
 - Image/video
 - Audio



Source Grandviewresearch.com

~37% North America Market Revenue Share

Europeans Take a Major Step Toward Regulating A.I.

A draft law in the European Parliament has become the world's most far-reaching attempt to address the potentially harmful effects of artificial intelligence.

ARTIFICIAL INTELLIGENCE / TECH / POLICY

ChatGPT returns to Italy after ban

Artificial Intelligence Market

Trends, by Region, 2023 - 2030



Privacy considerations for AI Training Data

Where did the training data
come from?

Was the training data legally
obtained?

Data being used as a proxy
for something else?

What are the
consequences?

The FTC's biggest AI enforcement tool? Forcing companies to delete their algorithms

Algorithm disgorgement requires companies to remove products built on data they shouldn't have used in the first place.

Has this happened?

Artificial Intelligence

FTC COPPA Settlement Requires Deletion of Children's Personal Information and "Affected Work Product"

What are other
issues with more
data from privacy
perspective?

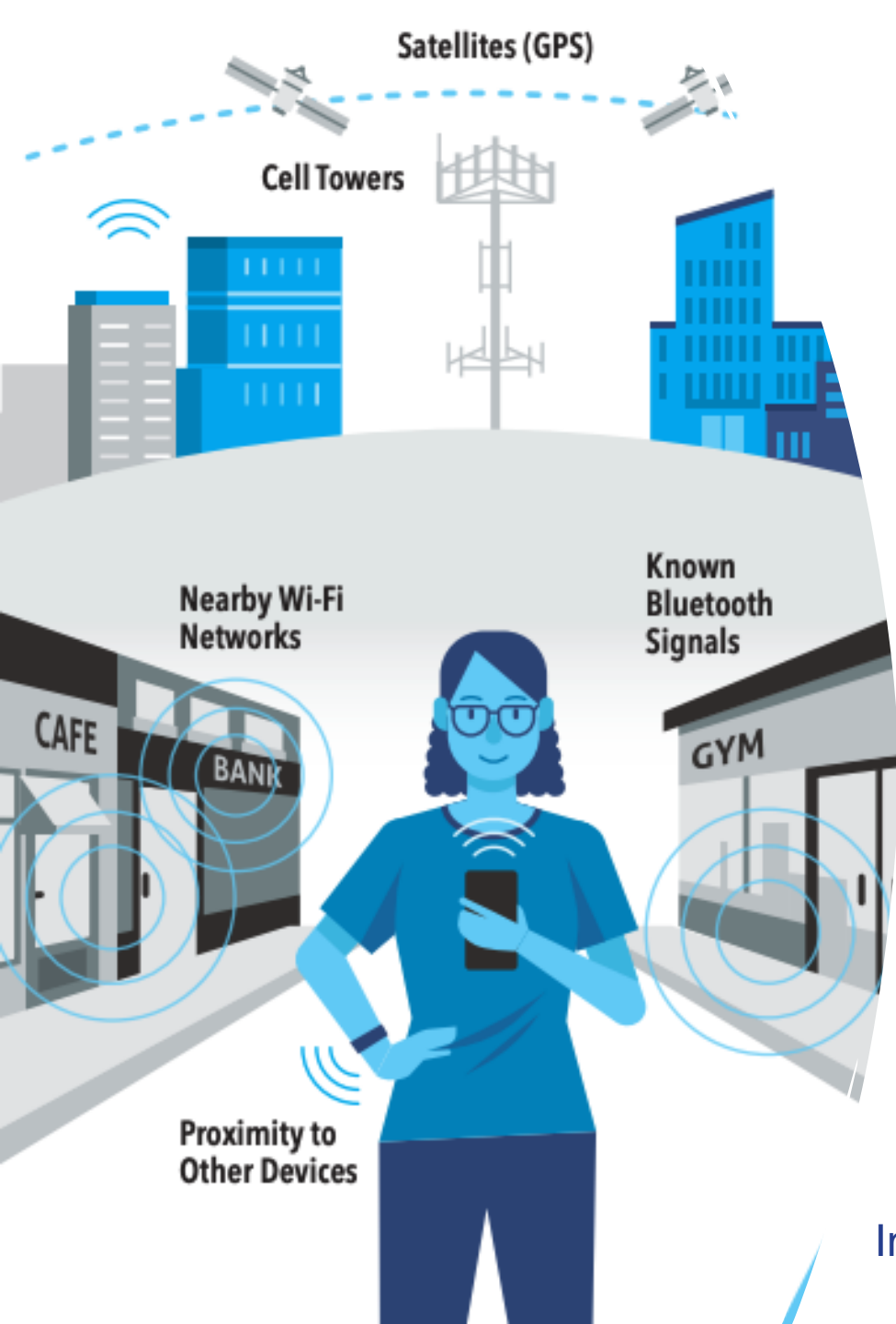
Collection of Sensitive Data:

- Biometric Data
- Health Data
- Location data
 - Vast amounts of data processed without knowledge or consent



Types of biometric data

- Facial geometry
- Fingerprints
- Hand
- Retina or iris scan
- Voiceprints
- DNA
- Keystroke patterns
- Gait patterns
- Vein patterns
- Ears
- “measurement or technological processing of an individual’s physiological, biological or behavioral characteristics”



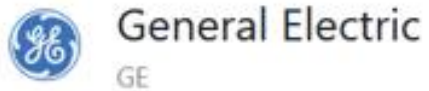
Location Data

- Risk of Location Datasets
 - Proximity to signals
 - Precision and Accuracy
 - Persistency and Frequency
 - Sensitive locations

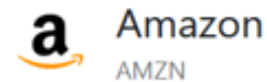
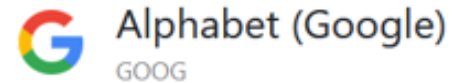
Infographic: Future of Privacy Form

Top 5 U.S. Companies by Market Cap

- 2003



- 2023



Where does this
lead?

Surveillance

- AI Powered
 - Web Scraping
 - Data Mining
 - Workplace monitoring
 - Location tracking
 - Object recognition



Proactive Real Time Security?

Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies

MSG Entertainment, the owner of the arena and Radio City Music Hall, has put lawyers who represent people suing it on an "exclusion list" to keep them out of concerts and sporting events.



South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?

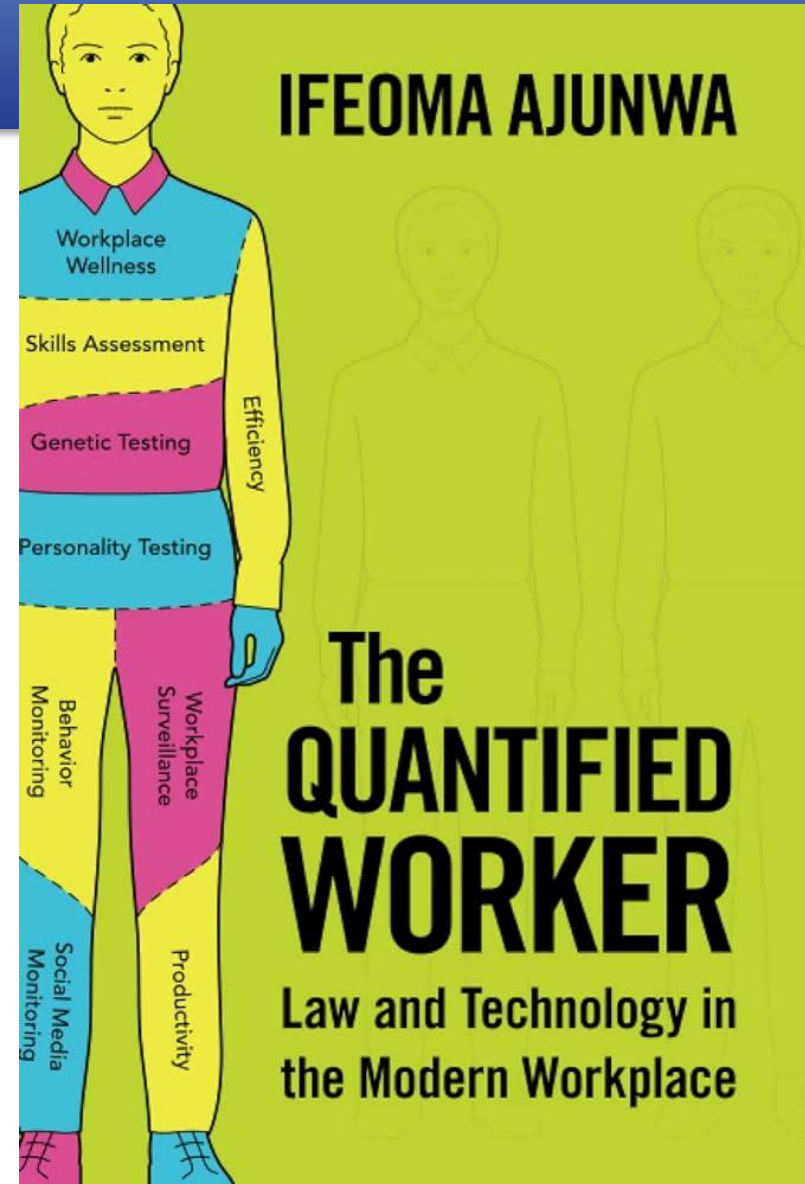
Web Scraping

- Clearview AI - Scrapped billions of photos from the internet
 - Contracts with law enforcement
 - 1000s of police dept.
 - Homeland Security
 - FBI
 - Armed Services



Workplace Surveillance

- Regulation?
- Bargaining?



Risks of discrimination and bias

- Discrimination: AI can reinforce existing prejudices and discrimination in society
 - Gender
 - Race
 - National origin
 - Class
- Bias: AI can lead to biased Decision-Making:
 - Healthcare
 - Housing
 - Employment
 - Education

AI and Identity Verification



- Identity risk scoring
 - Age verification
 - Document & Selfie Verification
 - Fraud detection
 - Synthetic fraud
 - Watchlist Screening & Monitoring

Government Use Cases

TEXAS LEGISLATURE 2023

DPS sent at least 3,000 driver's licenses to organized crime group targeting Asian Texans

A Chinese crime operation bypassed the password clues of Texas.gov by using stolen identity information to fraudulently obtain replacement driver's licenses.

STATE OF OHIO – TRANSFORMING DELIVERY OF HEALTH & HUMAN SERVICES THROUGH ROBOTICS PROCESS AUTOMATION

AI Use Case in Washington

Washington to combat wildfire threats with artificial intelligence technology

The new pilot program will enable early detection and monitoring to provide better data on wildfires as they emerge.

How artificial intelligence is helping Washington state fight wildfires



By KIRO 7 News Staff
September 07, 2023 at 2:01 pm PDT

DNR engages AI firm to assist firespotting



How did AI become
a privacy issue?

What are the rules?



BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR
THE AMERICAN PEOPLE



EXECUTIVE DEPARTMENT STATE OF CALIFORNIA

EXECUTIVE ORDER N-12-23

WHEREAS the State of California is a global leader in innovation, research, development, human capital, and entrepreneurship; and

WHEREAS Generative Artificial Intelligence ("GenAI") represents a significant leap forward in technology, by generating novel text, images, and other content, which will transform the way that the State and the world conduct business and serve the public; and

WHEREAS GenAI has the potential to catalyze innovation and the rapid development of a wide range of benefits for Californians and the California economy, such as advances in medicine, wildfire forecasting and prevention, and climate science, and to push the bounds of human creativity and capacity; and



Artificial Intelligence Risk Management Framework (AI RMF 1.0)

Self Regulation?

Empowering responsible AI practices

We are committed to the advancement of AI driven by ethical principles.



Responsible AI practices

The development of AI has created new opportunities to improve the lives of people around the world, from business to healthcare to education. It has also raised new questions about the best way to build fairness, interpretability, privacy, and safety into these systems.



Transform responsible AI from theory into practice

Promoting the safe and responsible development of AI as a force for good

Data Privacy is a Value Embraced by Responsible AI



But that's not all...



Questions

privacy@watech.wa.gov