Vennard Wright

RVASEC 2025

Leveraging AI for Public Safety

Amid Privacy Concerns

WHY THIS MATTERS NOW

Setting the Stage

The use of AI in law enforcement and surveillance is growing

The double-edged nature of AI makes it powerful but intrusive

Key question: Can we protect lives without compromising liberties?

AI IN PUBLIC SAFETY

Key Applications

The consequences of data breaches and privacy violations are far-reaching and devastating. From crippling financial losses (the average cost of a data breach is estimated at **nearly $5 million**) to irreparable reputational damage and even threats to national security, the stakes are undeniably high.

Protecting our data and privacy is no longer just a technical concern; it's a critical business and societal imperative.

- Real-Time Surveillance Analytics
- Gunshot and Anomaly Detection
- Predictive Policing
- Facial Recognition in Public Places

REAL-WORLD EXAMPLES

Understanding The Surveillance Landscape

New Orleans PD

Suspension of real-time facial recognition

NYC Subway

Weapon detection pilot “objectively a faillure”

Chicago PD

ShotSpotter gunshot detection contract cancelled

SEPTA

Ended year-long pilot amid a spike in violent crime

Baton Rouge PD

Cancelled ShotSpotter contract because of budge cuts

PUBLIC SAFETY

Protecting Public Places

- Faster emergency response
- Resource optimization
- Improved situational awareness
- Potential to prevent violence
- Pattern recognition

Always-on surveillance	Potential for overreach and misuse based on continuous data collection.
False positive and algorithmic bias	False identifications and lack of transparency.
Data ownership and sharing concerns	Who owns the data and how is it stored or shared?

THE PRIVACY TRADE-OFF

The Human Factor in AI Surveillance

Technology alone isn't enough. Human error remains a significant vulnerability. Educating users about privacy threats is paramount. Regular training and simulations can significantly reduce the risk of human error leading to privacy violations.

FACIAL RECOGNITION RISKS

Misidentifications and wrongful arrests

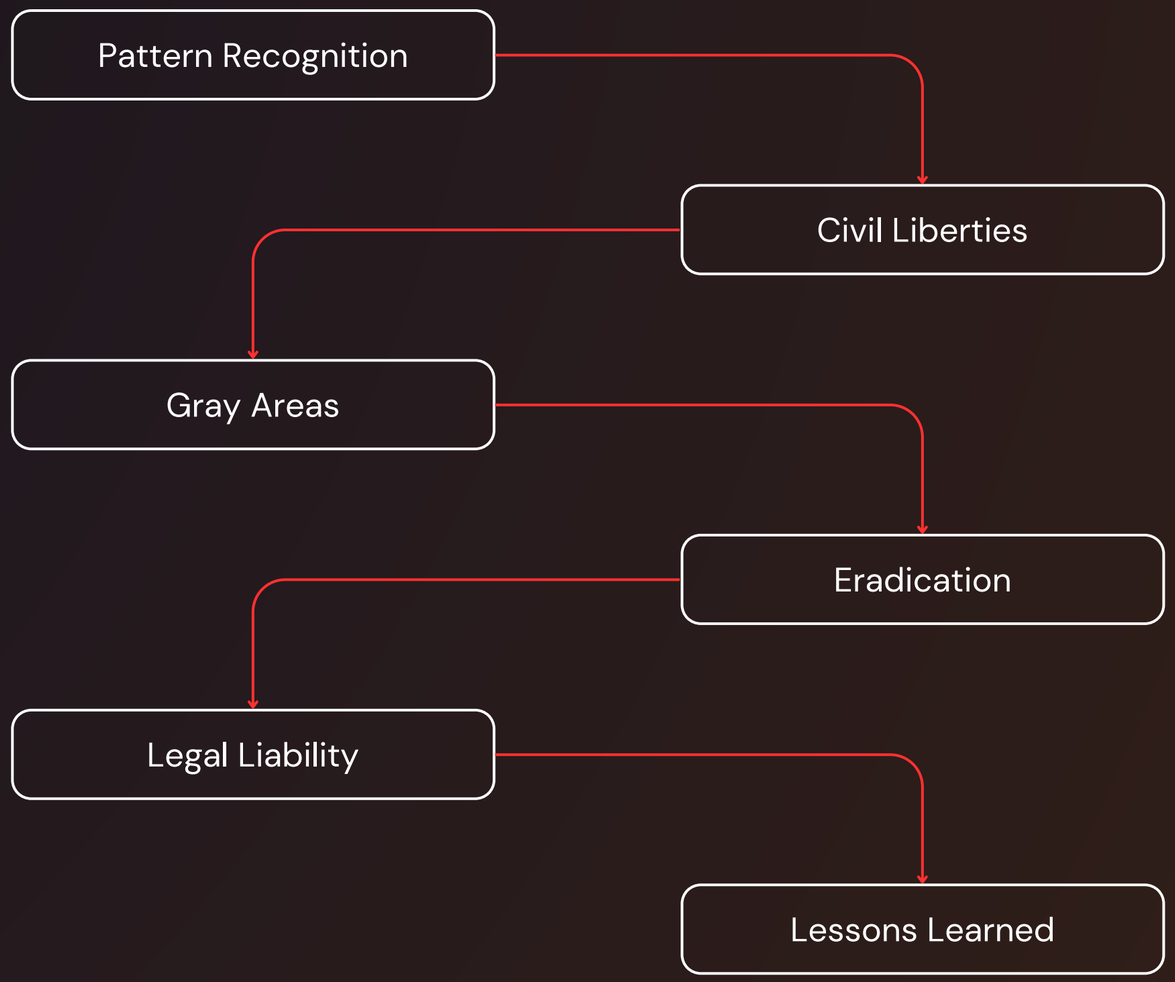
Disproportionate impact on communities of color

Lack of consent or public awareness

PREDICTIVE BEHAVIOR CHALLENGES

Predicting the Future

Even with the best models, incidents can still occur. Having a well-defined predictive model is crucial.

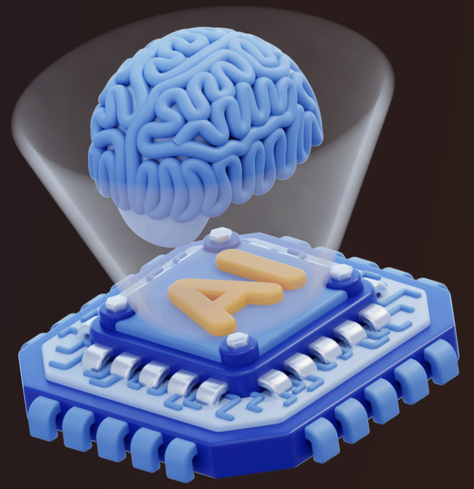


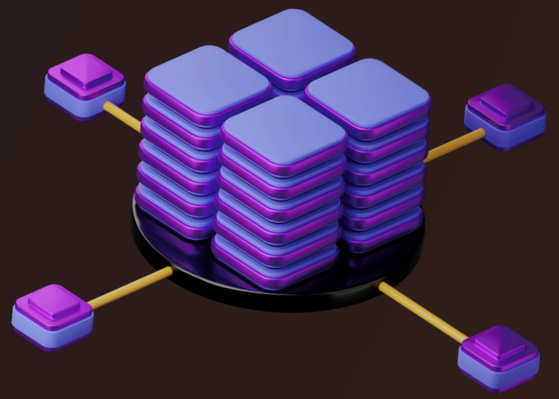
EVOLVING LEGAL LANDSCAPE

Liability Risk in an AI World

AI and automated technologies play a vital role in modern surveillance and policing.

- State Laws: BIPA (IL), CCPA (CA)
- Municipal Bans: San Francisco, Portland
- Lack of consistent federal regulation





RVASEC

VENNARD WRIGHT

ETHICAL FRAMEWORKS IN AI

Working Together for a Safer World

- Transparency
- Accountability
- Explainability
- Fairness

VENNARD WRIGHT

DESIGNING AI

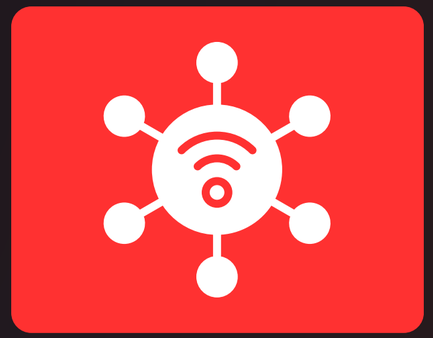
With Privacy in Mind

- “Privacy by Design” principles
- Federated learning and anonymization
- Limited data retention

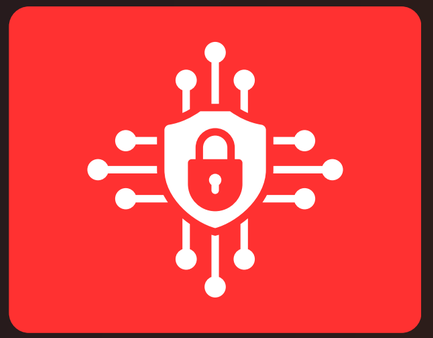
BUILDING PUBLIC TRUST

Against Evolving Threats and Emerging Technologies

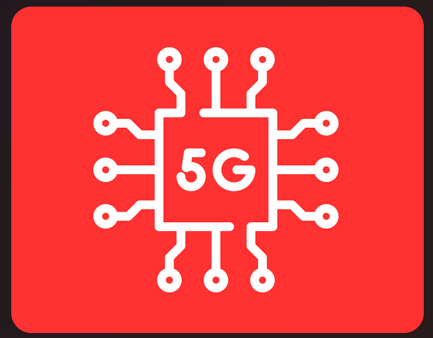
- Community Engagement and Consent
- Independent Audits and Oversight Boards
- Clear Public Communications



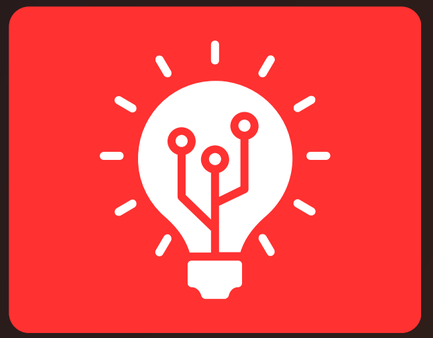
Internet Of Things



Quantum Computing



The Rise of 5G



Continuous Adaptation

A COLLABORATIVE APPROACH

Protecting Yourself and Your Organization

We've covered a lot of ground today, exploring the various threats and privacy concerns in the AI surveillance space. But knowledge is only powerful when put into action.

Now, let's talk about the practical steps you can take, both personally and within your organizations, to bolster your AI surveillance framework.

- Tech Companies
- Government Agencies
- Privacy Advocates
- Dialogue & Alignment

A CALL TO ACTION

Let's Discuss

- Develop responsibly
- Regulate intelligently
- Empower transparently
- Let AI serve **EVERYONE**, not just a select few

RVASec

Leveraging AI for Public Safety
Amid Privacy Concerns

THANK YOU

We appreciate you
joining us today

Contact Information:

Vennard Wright

CEO of PerVista AI

vwright@pervista.com

www.pervista.ai

@pervistaai