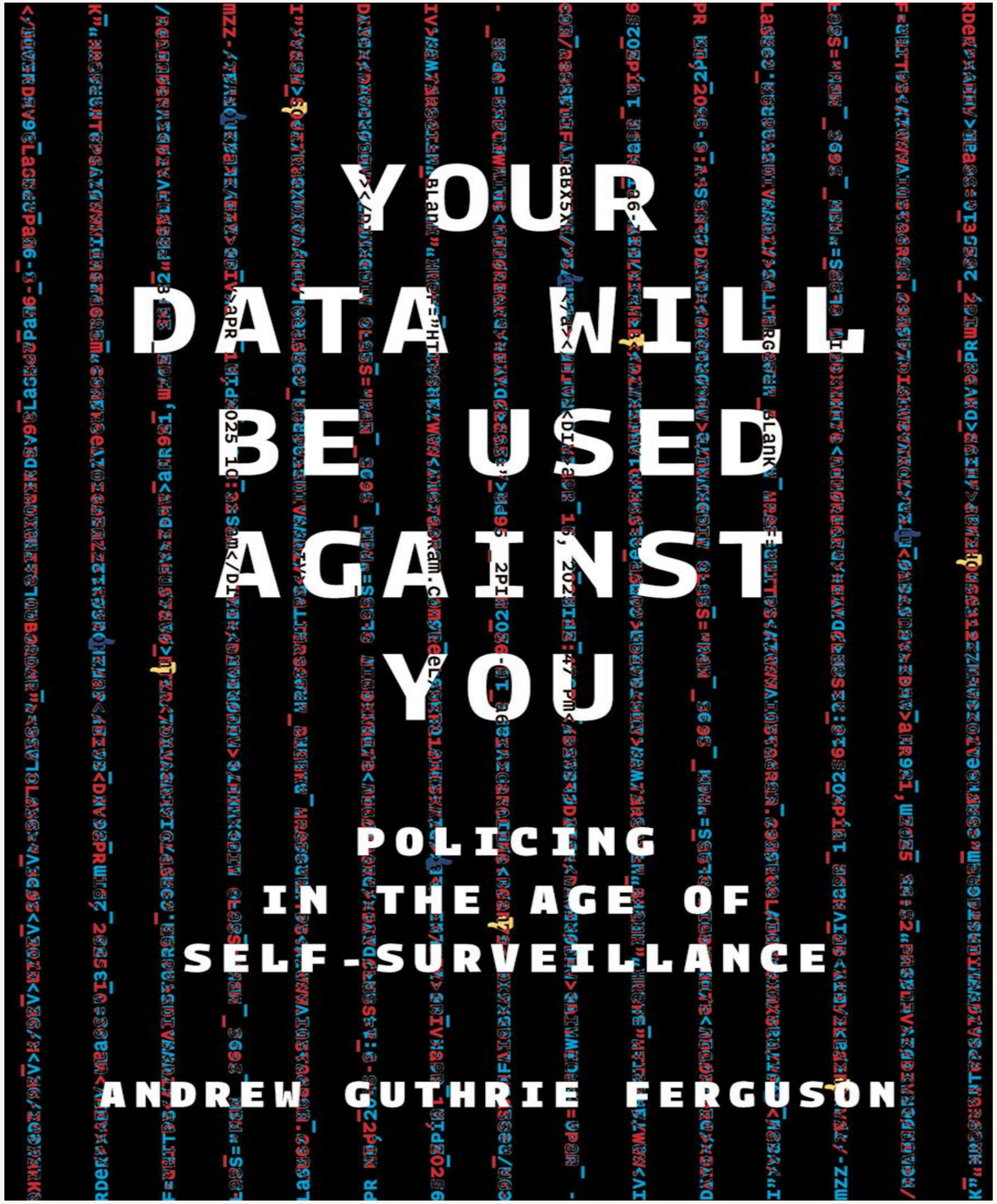


Privacy Week

(May 14, 2026)

Professor Andrew Guthrie Ferguson
George Washington University Law School

This book is about you

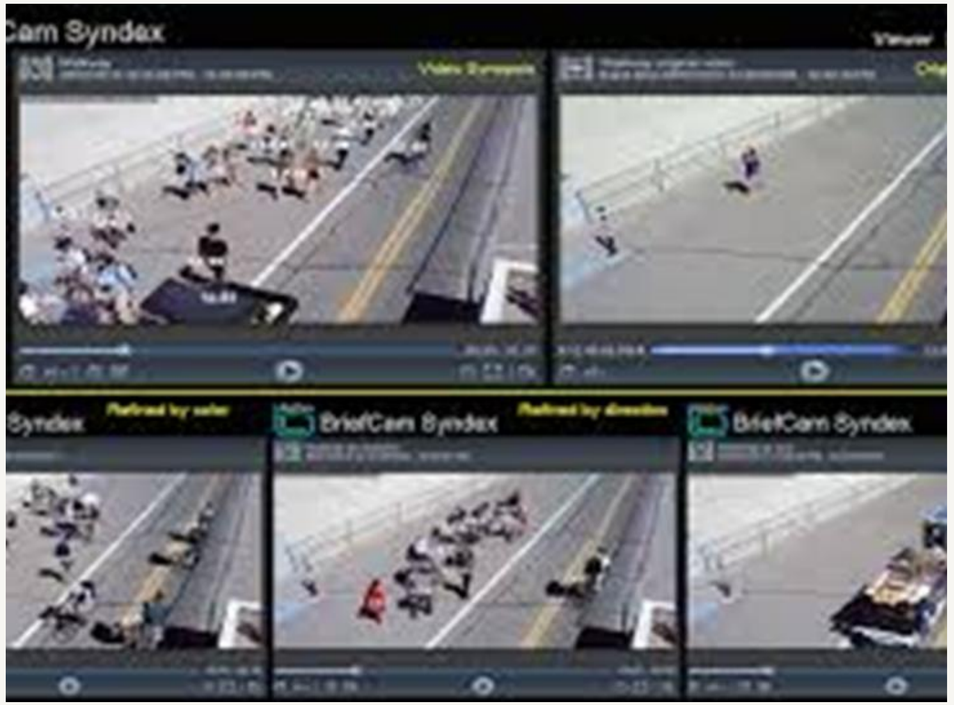
Reality 1: Nothing Is Too Personal for Prosecution

Reality 2: Currently Not Much Private in Public

The Book: What Happens When Data Reveals the Personal? And Digital Systems Expose the Public?

The Rise of Two Technology/Power Stories

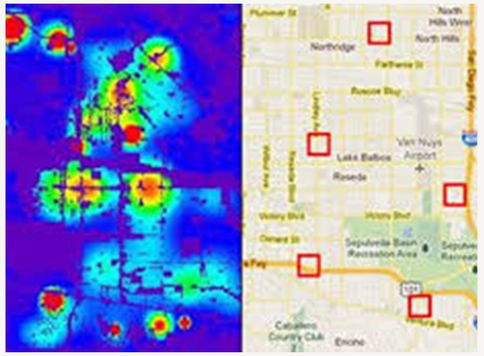
Selling Surveillance as a Service



Buying Surveillance as Security

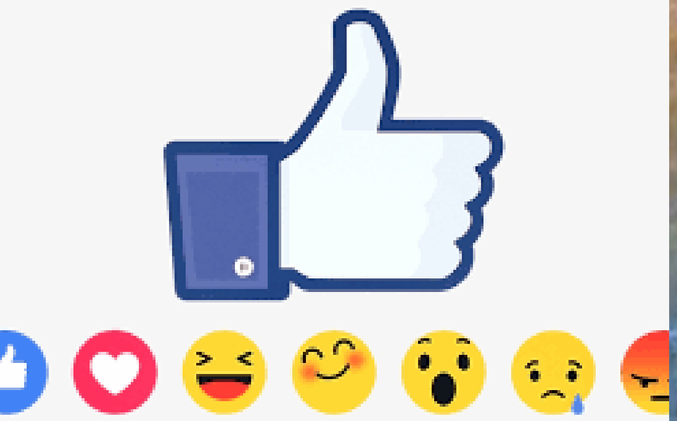
How the Stories Intersect

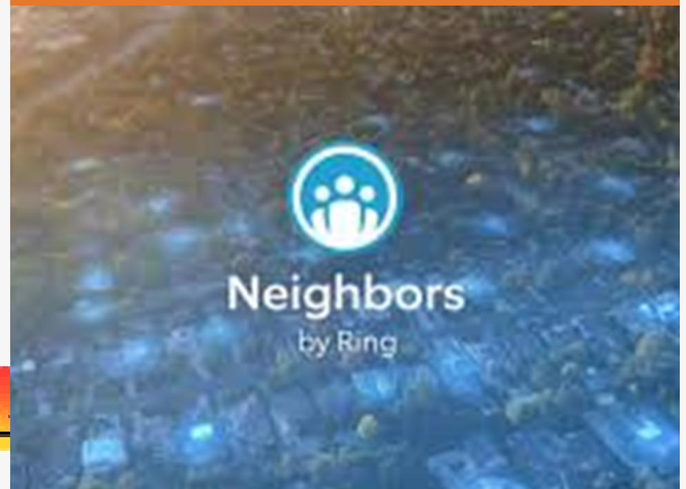
Personal: The digitization of ordinary life – smart phones, smart homes, social media – will betray us as our digital trails will be used against us by police.



Governmental: The digitization of police surveillance systems will create an exponentially powerful system in terms of scale, scope, and speed.

Fault: Personal and Democratic Choices (influenced strongly by corporate pressures)





Story 1: The Dangers of Digital Self-Surveillance

Each “innovation” transforming our things, homes, bodies, papers, likes, and cities into “smart” devices is **<u>at best</u>** a warrant away from government access.

A single document by a single judicial official (not even necessarily a lawyer) is all that protects you.

Our Things

- Smartphones
  - CSLI/GPS
  - Content
- Smart cars
  - GPS
  - Content
- Location, Location, Location
  - Patterns
  - Tracking
- Buying data (all for $ale)

Our Homes

Alexa, What Is Probable Cause?

An Amazon Echo might have recorded a murder. Is that enough for police to get access to information from it?

BY ANDREW GUTHRIE FERGUSON

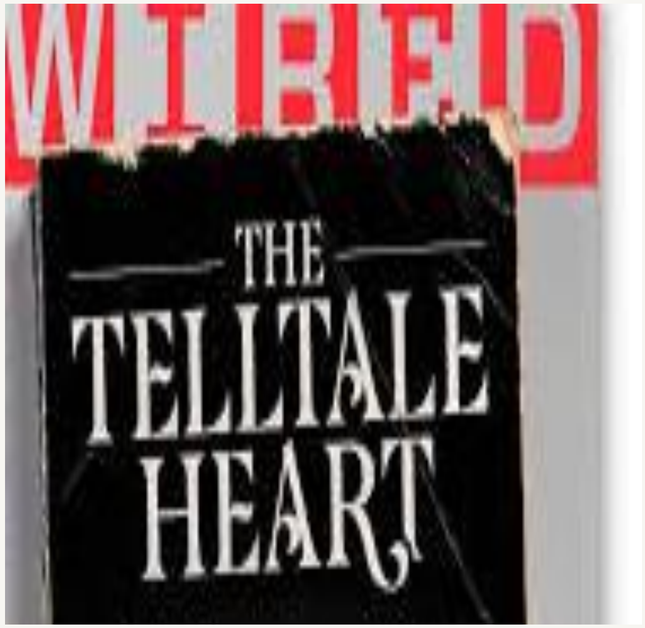
NOV 20, 2018 • 10:30 AM

INSIDE

- Smart Assistants (Echo’s etc.).
- Catcams
- Smart TVs, refrigerators
- Neighbors App
- Doorbell cameras

OUTSIDE

- Pole cameras
- Public Housing cameras
- Neighborhood ALPRs



Our Bodies

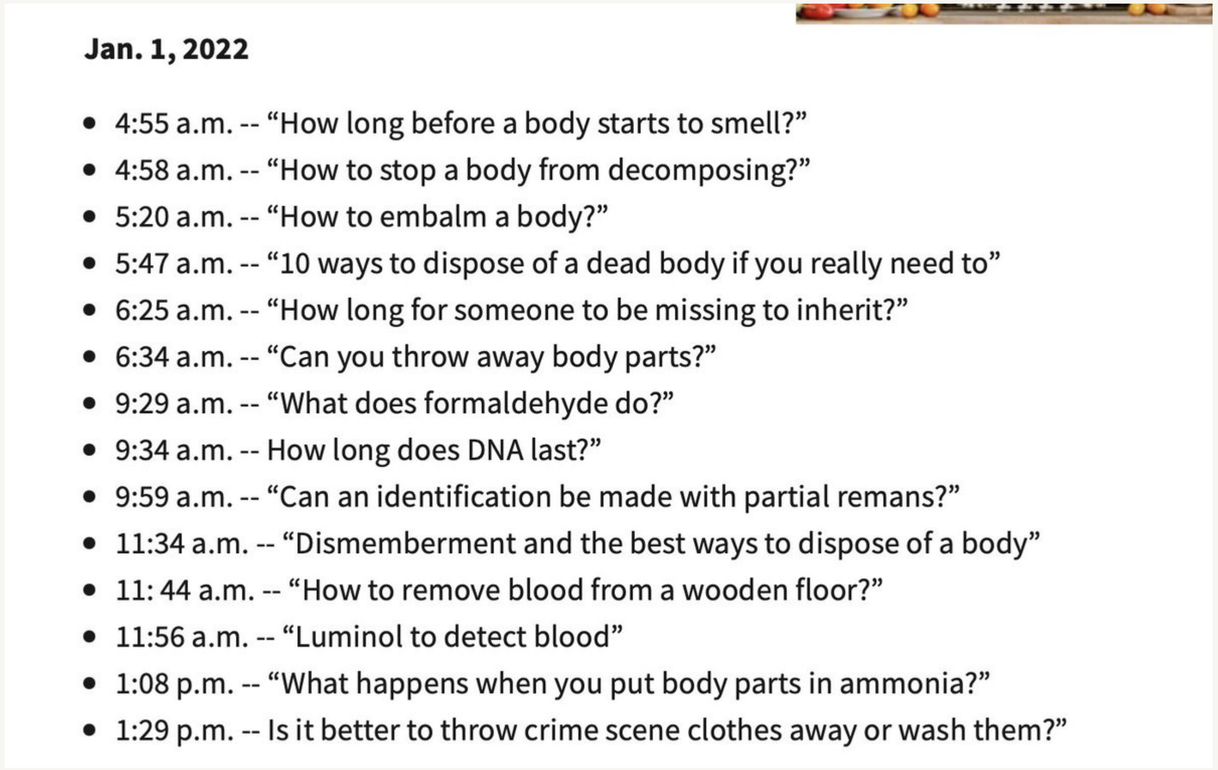
QUANTIFIED LIVES

- Smart watches
- FitBits
- Smart pacemakers, pill bottles, etc.
- Smart fabrics, clothes
- Fertility/Period tracking Apps

BIOMETRICS

- Facial Recognition
- Genetic Testing (23 & Me)
- Familial DNA Searches

Our Papers



Jan. 1, 2022

- 4:55 a.m. -- “How long before a body starts to smell?”
- 4:58 a.m. -- “How to stop a body from decomposing?”
- 5:20 a.m. -- “How to embalm a body?”
- 5:47 a.m. -- “10 ways to dispose of a dead body if you really need to”
- 6:25 a.m. -- “How long for someone to be missing to inherit?”
- 6:34 a.m. -- “Can you throw away body parts?”
- 9:29 a.m. -- “What does formaldehyde do?”
- 9:34 a.m. -- How long does DNA last?”
- 9:59 a.m. -- “Can an identification be made with partial remans?”
- 11:34 a.m. -- “Dismemberment and the best ways to dispose of a body”
- 11: 44 a.m. -- “How to remove blood from a wooden floor?”
- 11:56 a.m. -- “Luminol to detect blood”
- 1:08 p.m. -- “What happens when you put body parts in ammonia?”
- 1:29 p.m. -- Is it better to throw crime scene clothes away or wash them?”

- Keyword searches
- Texts/Emails
- Payment details (Venmo etc.)
- Computers/Clouds
- Digital photographs
- Digital Papers
- Digital health records

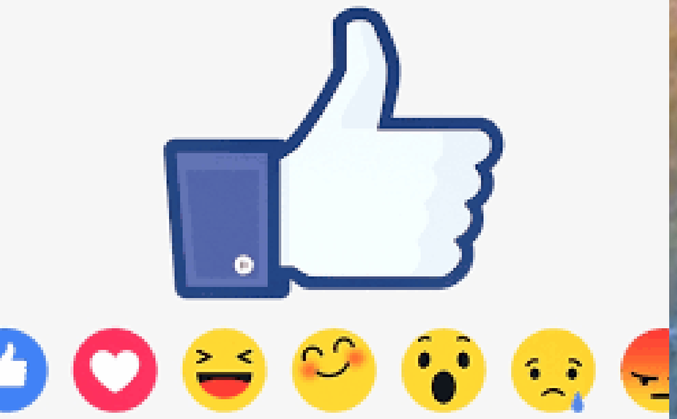
Can your text messages be used against you in court?

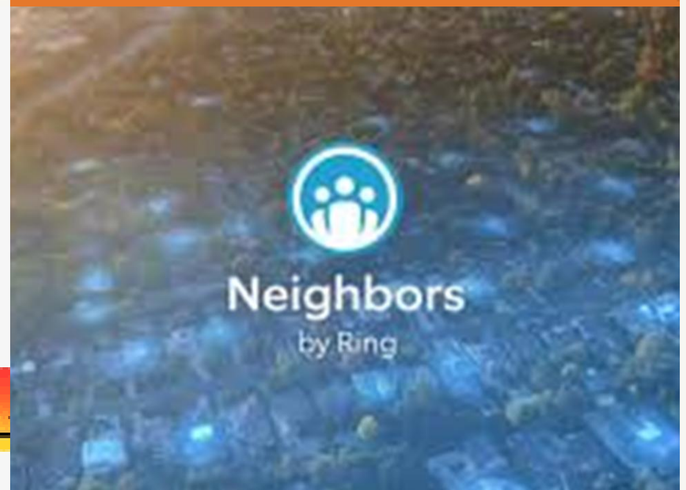
Our Likes

Social Media

- Scraping
- Spying
- Tracking
- Threat Monitoring

- Internet Cookies
- Data brokers
- Location Data Apps
- Mobile Purchases
- App Downloads
- Readings
- Dating Apps





Moral of Story 1 = Self-surveillance is a trap.

If the data trails exist. The data will be obtained by investigators.

If there is a crime and there is data, police will get access to the material – no matter how private or intimate or embarrassing.

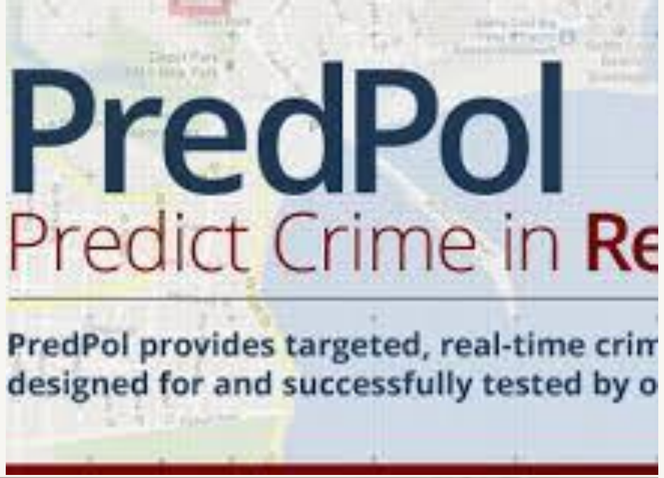
In the US – few countervailing law or protections.

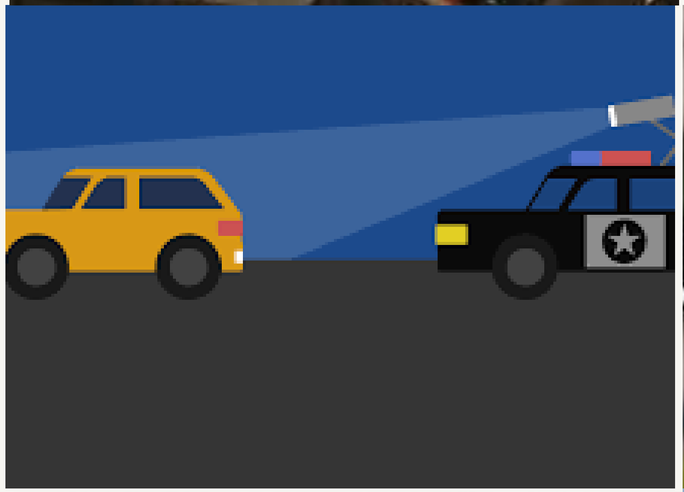
Story 2: The Allure of Surveillance Systems as Public Safety

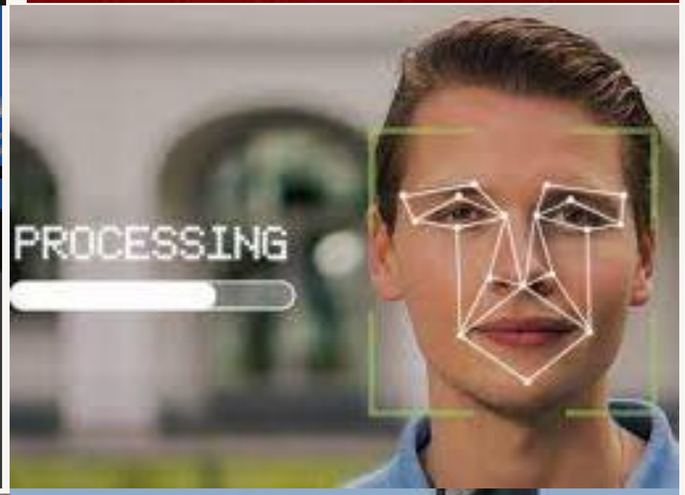
- Communities are investing in police surveillance systems – but the systems are far more powerful and integrated than ever before.
- Systems of persistent, aggregated surveillance are greatly enhancing police monitoring and investigatory powers.
- Democratically-mediated self-surveillance

The Tech

- Real-Time Crime Centers
- Predictive policing
- ALPR
- Facial recognition
- Drones
- Gunshot detection

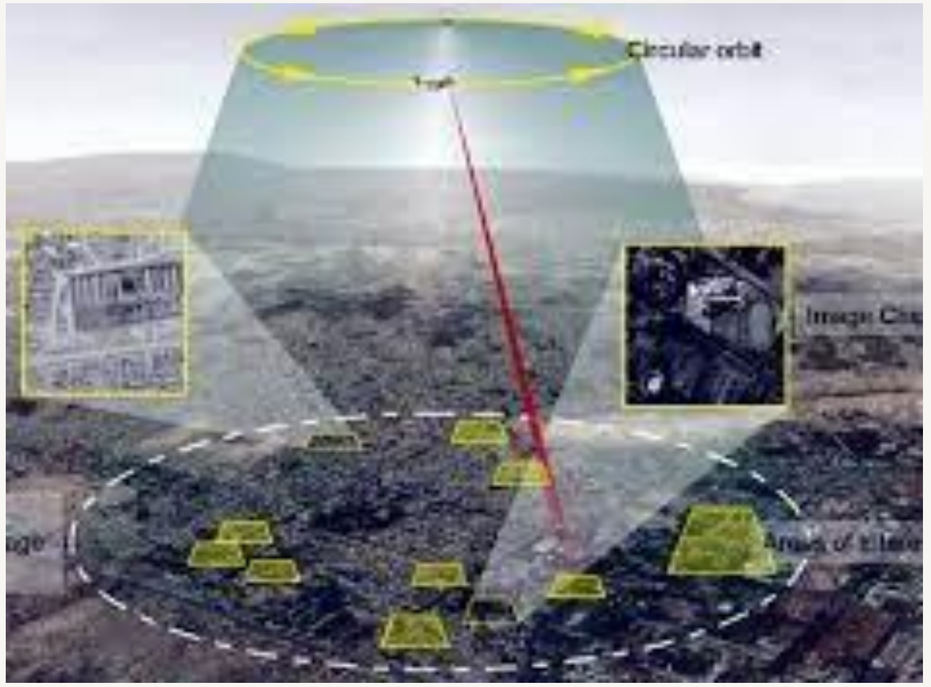






A Transformation of Police Power in Public

Digital Policing is Different



Persistent Surveillance is Different

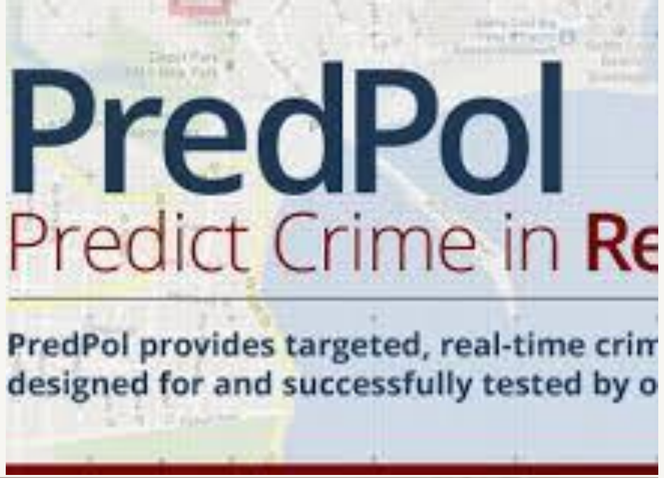
Moral of Story 2

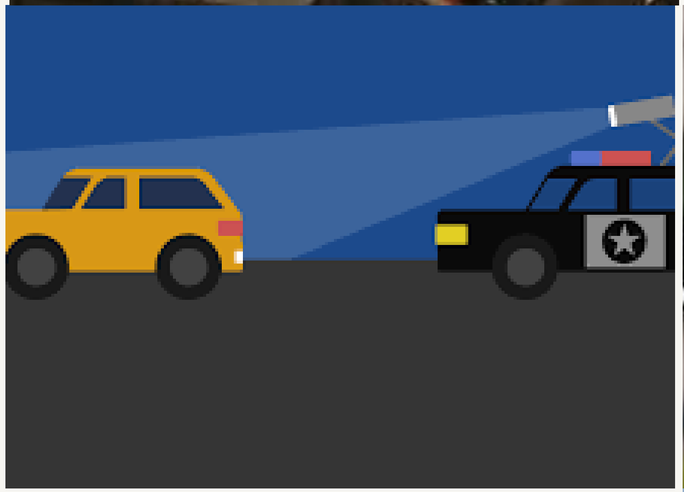
Systems of city-wide surveillance are being developed and integrated in large cities and small towns.

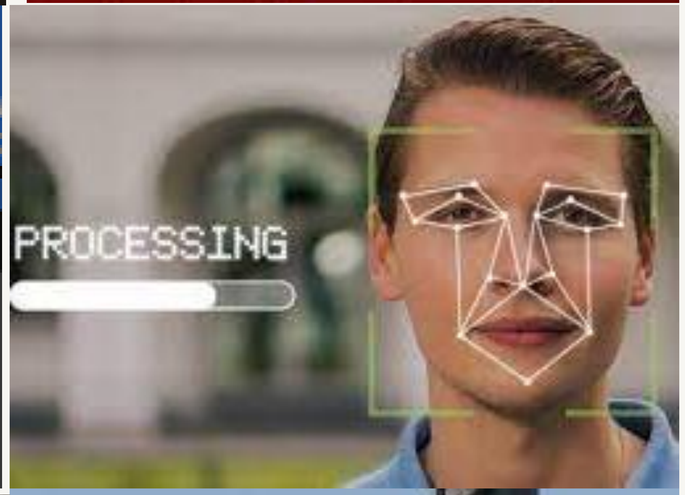
Each of the surveillance tools can be linked into a system and used for monitoring and investigation.

Time machine like capabilities to find objects, people, and events.

Radically changing conceptions of privacy in public.







What Changes When Everything is Evidence?

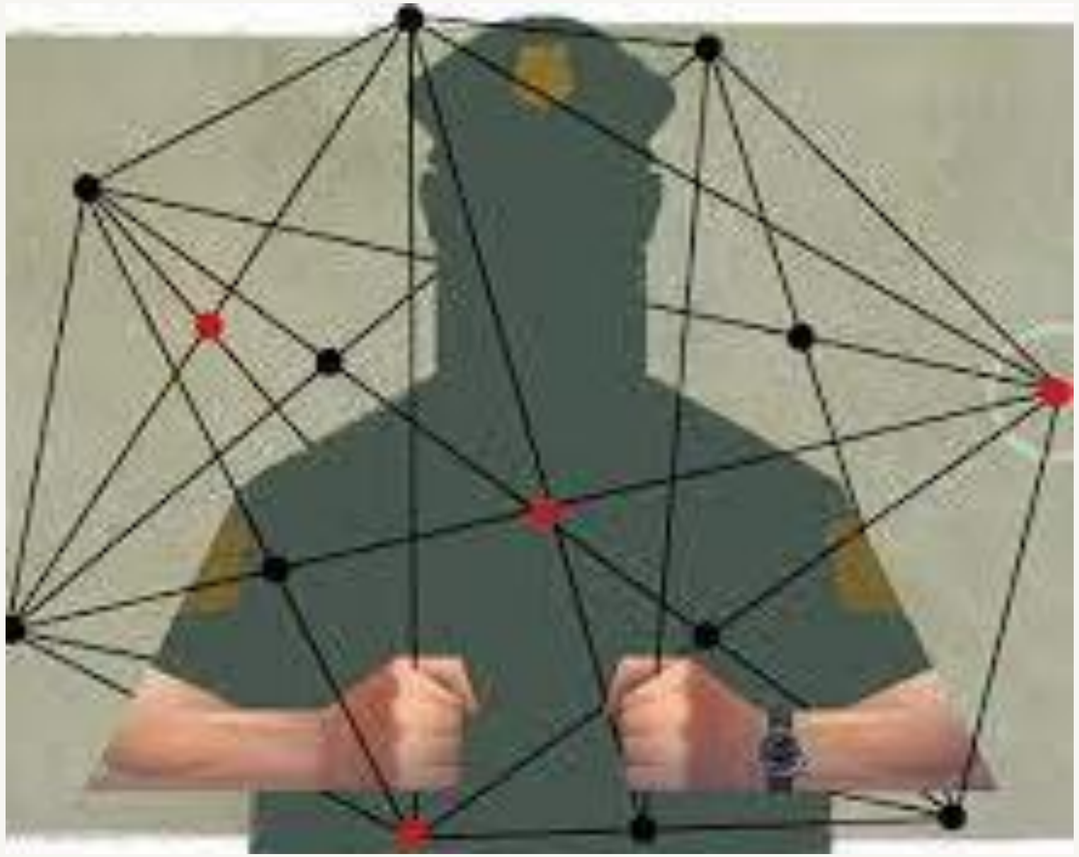
Power

Privacy

Praxis

Privatization

Power Problems



- New (and old) Targets
- Reifying Race
- Protecting Capital
- Private Platforms

Privacy Problems

Prosecution over Privacy

Narrowing of Privacy

Associational Privacy

Praxis Problems

The Pilot Problem

The Profit Problem

The Probability Problem

The Pressure Problem

The Way Forward

How do we approach the growth of new police technologies?

- How do we address the tensions?
- How do we minimize risks?

What do we do?

Judicial Responses

A “Smart” Fourth Amendment – Informational Security

Future-proofing the Fourth Amendment in an age of persistent surveillance

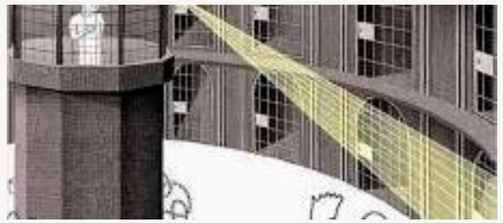
A Theory of Digital Rummaging

Legislative Responses

A weak statutory “WALL” – (Wiretap Act Like Law for Personal Data)

A strong statutory prohibition akin to a privilege for sensitive digital communications.

Individual/Community Responses



See the trap

Support secure devices

Strengthen community

Select representatives

Sabotage your data

Support journalism

Discussion/Questions?