

Connective Tissue: Governance Over Law Enforcement Technology Use in Washington and Elsewhere

Cameron Cantrell
Zoe Wood

UW School of Law



Catalyst

Law enforcement bodies at every level of government rely increasingly on technology to replace or aid analog work.

Most uses are hidden from the public eye, making regulation and accountability difficult.

The least is known about technology uses that arise when law enforcement (LE) interacts with an individual **one-on-one**.

Solution (1/2)

Our work is a response to this gap in knowledge. Seven types of technologies are especially prevalent:

- 1. Cell site simulators,**
- 2. Automated license plate readers,**
- 3. Predictive policing,**
- 4. Facial recognition,**
- 5. Unmanned aerial vehicles,**
- 6. Body-worn cameras, and**
- 7. Mobile device forensics.**

Solution (2/2)

We surveyed and assessed the landscape of 50 states' and DC's regulation + law enforcement agency (LEA) use of these seven technologies.

Today we will present some of our findings, with a focus on where WA's governance leaves room for **judicial discretion to promote equitable technology use and where **legislative growth** is necessary.**

We will also explain how the collaborative nature of police technology use puts even the strongest regulations in WA at risk of being undermined by weaker regulations in other states.

Value

Technology **compounds and amplifies** biases that already exist. It can also introduce its developers' biases.

Compounding biases, amplified and left unregulated, pose complex and substantial **risks to individual rights and liberties**.

Groups historically marginalized by white cispatriarchy are disproportionately subject to LE interactions, so they are also **disproportionately subject to the risks of LE technology use**.

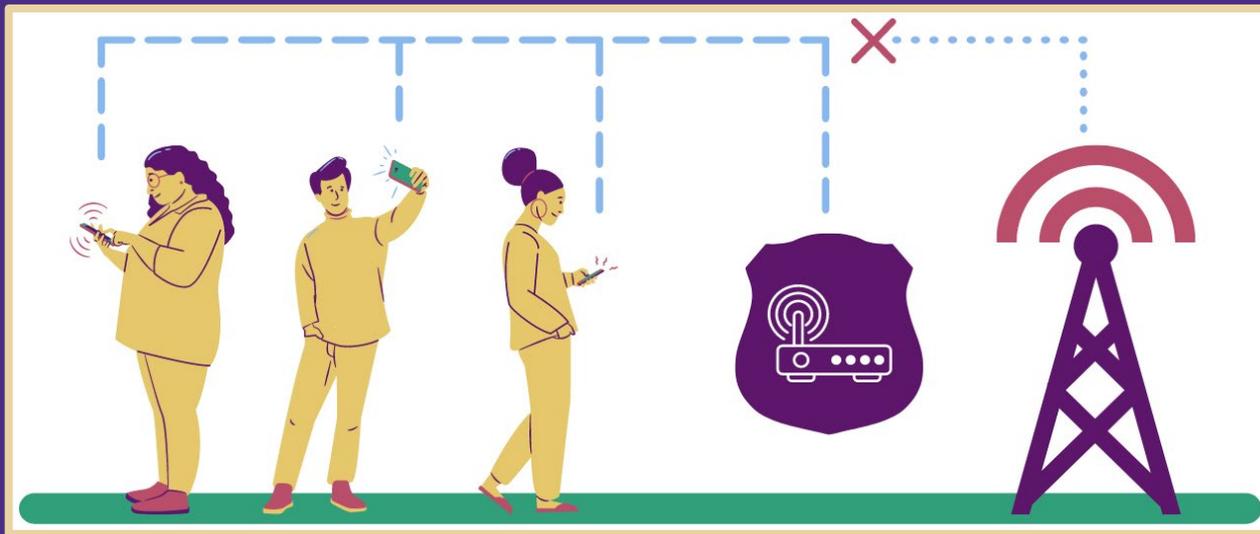
WA's Governance is Relatively Good

All technologies are in use in WA.

- > Cell site simulators: **B+**
- > Automated license plate readers: **D-**
- > Predictive policing software: **N/A**
- > Facial recognition software: **A**
- > Unmanned aerial vehicles: **D-**
- > Mobile device forensics: **A**
- > Body-worn cameras: **C**

Cell Site Simulators (CSSs)

A CSS emits a very strong, but phony, network signal so **all nearby phones** on a given cell provider network connect to it instead of to a real cell tower.



In WA: Tacoma PD uses CSSs.

Cell Site Simulators

WA is one of 13 states with a controlling LE-CSS authority (RCW § 9.73.260, .270).

WA law

Judicial discretion for equity

Subject only notified of CSS use if court orders

Order notice within 10 days of use ending, unless court finds good cause for delay (MD)

Initial authorization & each renewal can last up to 60 days

Authorize in 30-day increments, reserving 60 days for extraordinary facts (AZ, CT, VA)

Mandated LEA → Court Admin. monthly reports, but not shared publicly

Court Admin. publicly reports annual summary of reports, e.g., aggregate use numbers (MN)

CSS can collect content *and* location data

Request separate justifications in court order application for location vs. content data sought (IL, MD, MN)

Automated License Plate Readers (ALPRs)

ALPRs capture pictures of **every license plate that passes by**. The pictures are automatically stored in a database, which can often be accessed by multiple, out-of-state LEAs.



In WA: 12 LEAs (including WA State Patrol) use ALPRs.

Automated License Plate Readers

ALPRs come up **just once** in WA law, which provides a definition and no further regulation (WAC § 478-116-024). **19 states** regulate more comprehensively.

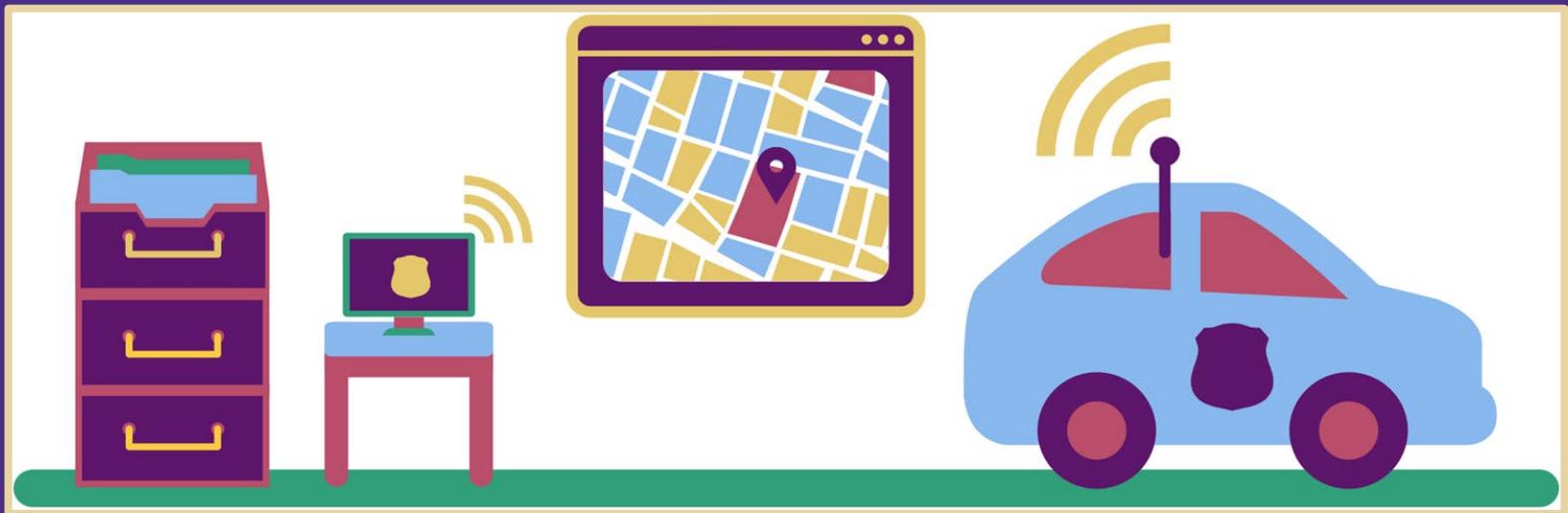
WA law

Some examples of stronger protections

(Unregulated use of device)	Restrict use to DPS, DoT, State Police (ME); local, county, and state LEAs (NH); “law enforcement purposes”
(Unregulated data retention)	Limit data retention to 21 days (ME); average is about 6 months
(Unregulated access to data)	In accordance with disclosure requirements for protected records, or pursuant to a state or federal warrant or a state disclosure order (UT)
(Unregulated use of data as grounds for a stop)	ALPR data ≠ reasonable suspicion as grounds for law enforcement to stop a vehicle (MT, NH)

Predictive Policing Software (predpol)

Predpol learns from past crime data to make **statistical predictions** about future crimes. These predictions direct LE to crime **“hotspots”** and intervene, preventing the crime’s occurrence.



In WA: Tacoma PD uses predpol.

Predictive Policing Software

LE predpol use is **fully unregulated at the state level**, nationwide (including DC).

Even at the local level, only one jurisdiction has acted: **Santa Cruz, CA.**

- > 2020: City council **adopts ban on use** because it is “disproportionately biased against people of color”
 - + Exception: showing, among other things, that use “will not perpetuate bias.”

Judicial discretion for equity: when faced with the RS/PC analysis for a seizure, use a critical eye to the extent predpol informed the encounter.

- > Complexities: *Wardlow's* “high-crime areas”

Facial Recognition Technology (FRT)

FRT helps LEOs identify individuals by matching an **unidentifiable** image, like CCTV video, to an identified image, like a mugshot or driver's license.



In WA: Pierce County Sheriff's Office uses FRT.

Facial Recognition Technology

12 states, including WA, regulate FRT; WA's protections are among the strongest (RCW § 43.386.010).

WA law

Comparison shows some stronger, some weaker protections elsewhere

Use = identifying or persistently tracking by collecting data

Use = identifying subject by collecting data and comparing it with other data (VA) (TX)

Can use for surveillance, id, or persistent tracking if authorized by warrant or exigent circumstances

Can use if expressly authorized by a warrant (MN); always, by default, to investigate criminal conduct (MO) (NH) (OR) (PA) (TX); if expressly authorized by statute (VA)

FRT results cannot serve as sole basis to establish probable cause in criminal investigation

-

LEA must write own policy regarding access

FRT data may only be accessible by a search, administrative, or inspection warrant (VA)

Unmanned Aerial Vehicles (UAVs)

UAVs speak for themselves: remotely-controlled aircrafts (with degrees of autonomy). They feature **cameras**, which are often enhanced with further technology like night vision or FRT.



In WA: 25 LEAs (including WA State Patrol) use UAVs.

Unmanned Aerial Vehicles

WA is one of 30 states with a controlling LE-UAV authority (WAC § 200-250-030, 040). But of those 30, WA is one of 4 states where **the only regulation is to exempt LEAs** from the civilian-facing restrictions.

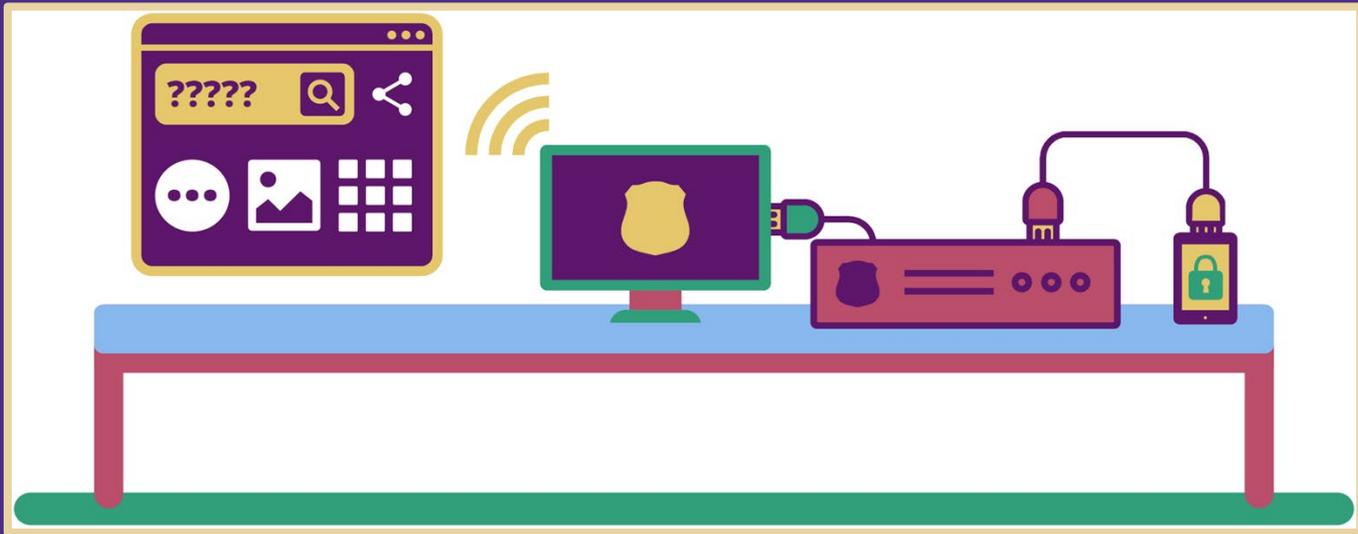
- > This means WA judiciary has no guaranteed role in UAV use.
- > 17/30 states require a warrant for LE-UAV use.

Judicial discretion for equity: when faced with claims/evidence related to UAV use, undergo analysis considering any offensive facets of use and WA's greater privacy protections.

- > Complexities: *Florida v. Riley's* no-warrant plurality

Mobile Device Forensics (MDFs)

MDFs extract a **complete copy of a phone's data**, then sort the data into searchable, filterable, organized categories (e.g., photographs). MDFs can also analyze the data to create timelines, maps, and contact networks.



In WA: 9 LEAs (including WA State Patrol) use MDFTs.

Mobile Device Forensics

WA is one of 17 states with a controlling LE-MDF authority (State v. Keodara, 191 Wash. App. 305 (2015)). Of those 17, WA is one of 5 states where the authority **only concerns warrant standards** for MDF-assisted searches.

WA law

Judicial discretion for equity

Limit phone search warrants to topics, and/or data generated close in time to incidents, for which LEOs had PC.

Request that warrant return include search protocol undertaken; generally use heightened vigilance in issuing phone search warrants. (DE)

(Unregulated: additional barriers to assisting searches with MDFs)

Request search warrant application specify whether MDF will assist search. (MT)

(Unregulated: consent to search as warrant exception)

In analyzing if consent to phone search was meaningful, consider subject's probable knowledge about MDFs. (no state reference, by one measure, consent authorized 1/3 of SPD's MDF-assisted searches)

Body-Worn Cameras (BWCs)

BWCs also speak for themselves: small cameras, mounted to LEO's bodies or helmets, record the LEO's point of view and can easily be turned on and off.



In WA: 6 LEAs use BWCs.

Body-Worn Cameras

BWCs are the most famous police technology, regulated in 28 states. Like the majority, WA does not mandate their use (RCW § 10.109.010–100).

WA law

Some examples of stronger protections

Policy required, but left up to the agency	LEAs must adopt a model policy established by an advisory board (VT)
Must retain for 60 days; then can destroy per applicable schedule	Retain until end of criminal investigation (MI); retain for 3 years if recording captures deadly force/restraint, discharge of firearm (NH) (TX); subject of complaint (NH); <u>has evidentiary value</u> (WI)
Presumption against disclosure; party seeking footage must “prevail”	Can be used as evidence of misconduct, if it depicts force, or as evidence in <u>any proceeding</u> (IL); on request, must be given to state LE division, AG, or circuit solicitor for <u>any criminal justice purpose</u>
Unregulated accountability	Permissive inference against LEO who fails to activate (CO); if LEO fails to activate, LEO must document why (NH) (TX) (UT)

Connective Tissue Between LEAs (1/2)

A given LEA collaborates with intra-state, inter-state, and federal LEAs. This results in:

- > inter-LEA technology hardware sharing (CSSs, MDFTs)
- > inter-LEA data sharing (ALPRs, FR, UAVs, BWCs)

Inter-LEA collaboration, coupled with lack of robust governance, enables WA LEAs to readily:

- > Borrow technology from other LEAs, **without going through public procurement**, and
- > Share data gathered from the technology with other LEAs, **without guarantee the data is safe from abuse.**

Connective Tissue Between LEAs (2/2)

Our findings are descriptive. We do not assert that WA LEAs or LEOs *will* borrow technology or share data in this manner. But the open possibility is too large to ignore.

Further: even where technology use by WA LEAs is appropriately regulated, inter-LEA collaboration means **WA's safeguards can be undermined by LE practices in other states.**

Judicial discretion for equity is **key** to ensuring not only that an individual's rights and liberties in WA are not undermined by LEA practices elsewhere, but also that WA's laws are given **maximum protective effect.**

Thank you for your time.

Cameron Cantrell (ctrell@uw.edu)

Zoe Wood (zoewood@uw.edu)

UW School of Law

