

Privacy in DSRC connected vehicles

Defcon 21 – August 3, 2013

whoami

- BSEE, digital communications
- Many years as a network engineer
- Santa Clara University Law student
- Research assistant providing technical expertise on privacy audits and reviews
- Contracted by auto consortium to review privacy of proposed vehicle to vehicle safety network

Standard Disclaimer

IANAL (Yet)

But if you know anyone looking for summer interns....

Non-Standard Disclaimer

A current NDA covers some of my work here (but not very much)
The focus will be on published information and standards.

What is This Project?

- DSRC: Dedicated Short Range Communications
 - (Where “short” == 380m)
 - Vehicle to Vehicle
 - Vehicle to infrastructure
 - Not having to wait for a light on an empty street again.
 - Better traffic planning for better cities and roadways.

Why is It being Developed?



Safety



How the safety features work

Non-trivial Impact on Auto Deaths

- World Health Organization estimates 25% of vehicle deaths each year can be prevented.
- Fatigue and distracted driving accidents reduced.
- Blind Corners, fog and limited visibility accidents reduced.



Photo: Public Domain

Will This really Happen?

IT ALREADY IS

How Soon?

- Hardware is already being shipped.
- Software issues still entirely in the air
 - More is being done in software these days.
- The US Dept. of Transportation is considering mandating this for all new cars. (Decision to come later this year.)
- Has already deployed in trucks in Europe

What is DSRC

- Basic safety messages sent out every 1/10 seconds.
- All message carry a standard glob: values for pre-defined vehicle trajectory and operational data.
- Cars process data and warn driver.
- Equipment integrated into vehicle



Photo Credit: US Dept. of Transportation

AfterMarket Installation



Photo Credit: NIST

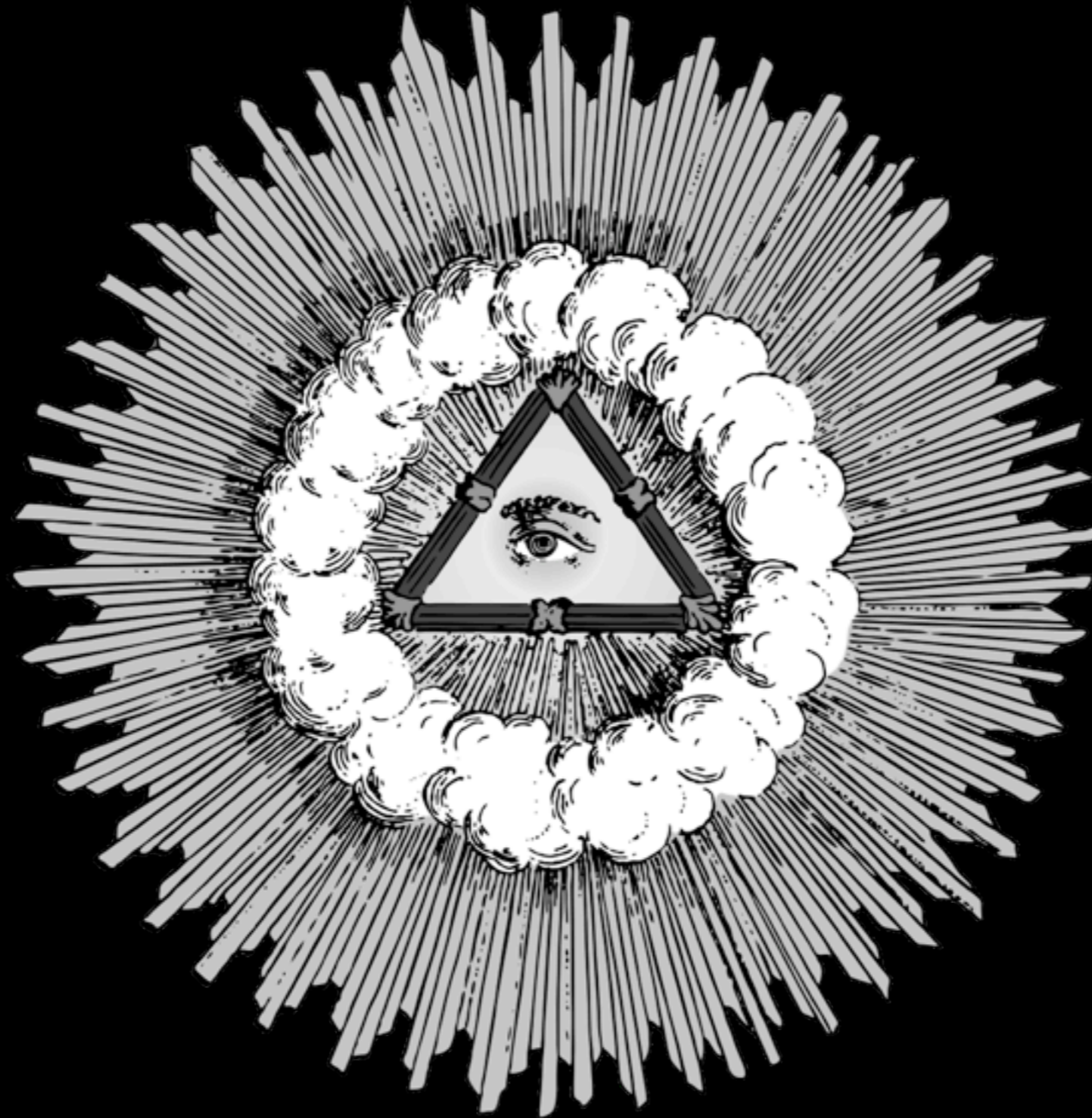
A little cumbersome

What DSRC is not



- CANbus
- OnStar (or any other remote service)
- (Direct) support for autonomous driving mechanisms.

Photo Credit: US Dept. of Transportation



Technical details

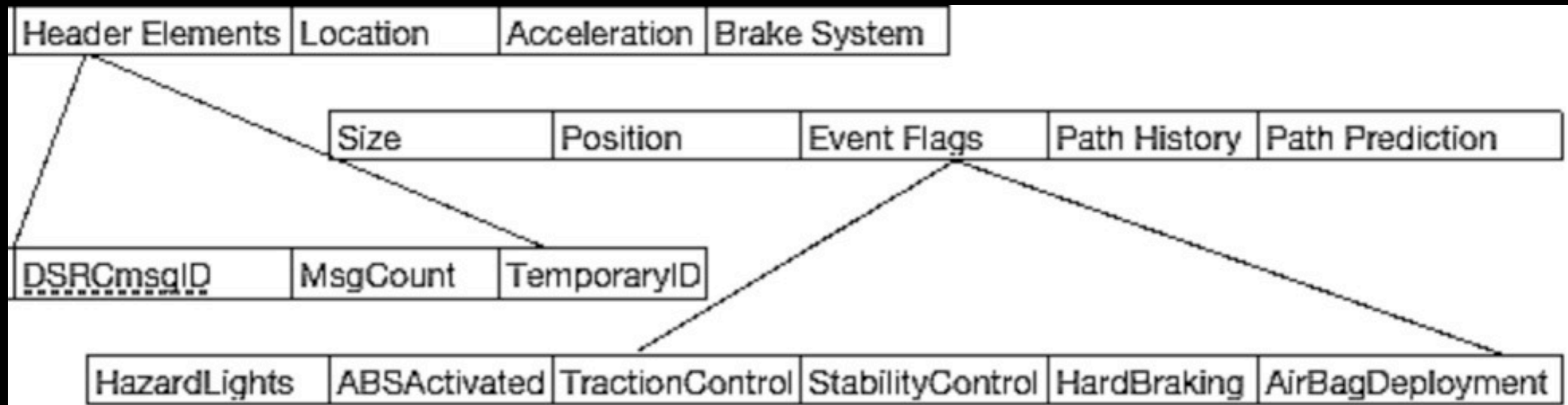
Radio protocol

- 5.9GHz reserved in US and Europe
- Signaling standard: IEEE 802.11p / 1609.4 / 1609.3
- Channels reserved for specific functions
- Protocol does not require source address for vehicles
- Recommendations include using certificates
- Privacy challenges at each layer



Photo Credit: NASA

Basic Safety Message



- Standard: SAE J2735
- ~50 fixed data elements
- “only” interface to radio (on this channel/band)

Parameters for effectiveness

- Density
 - Benefit derived from other vehicles' use
 - Greater usage means greater effectiveness
- Confidence
 - Most messages must be trustworthy

Validity?

- All messages are cryptographically signed
- Signing certificates issued by central authority
- Issued based on system fingerprint
- Revocation for “malfunctioning” equipment
- System should invalidate itself if internal checks fail

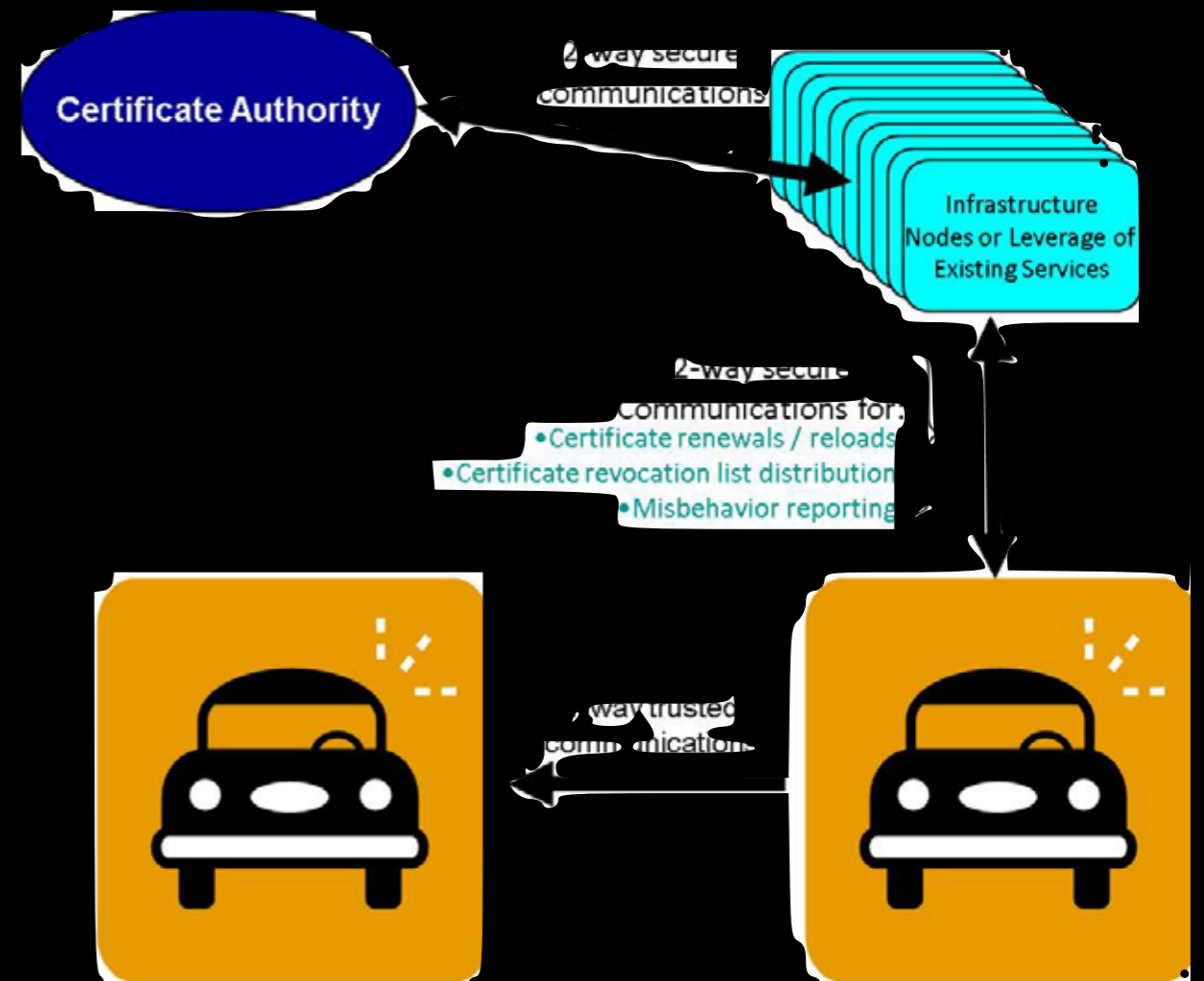
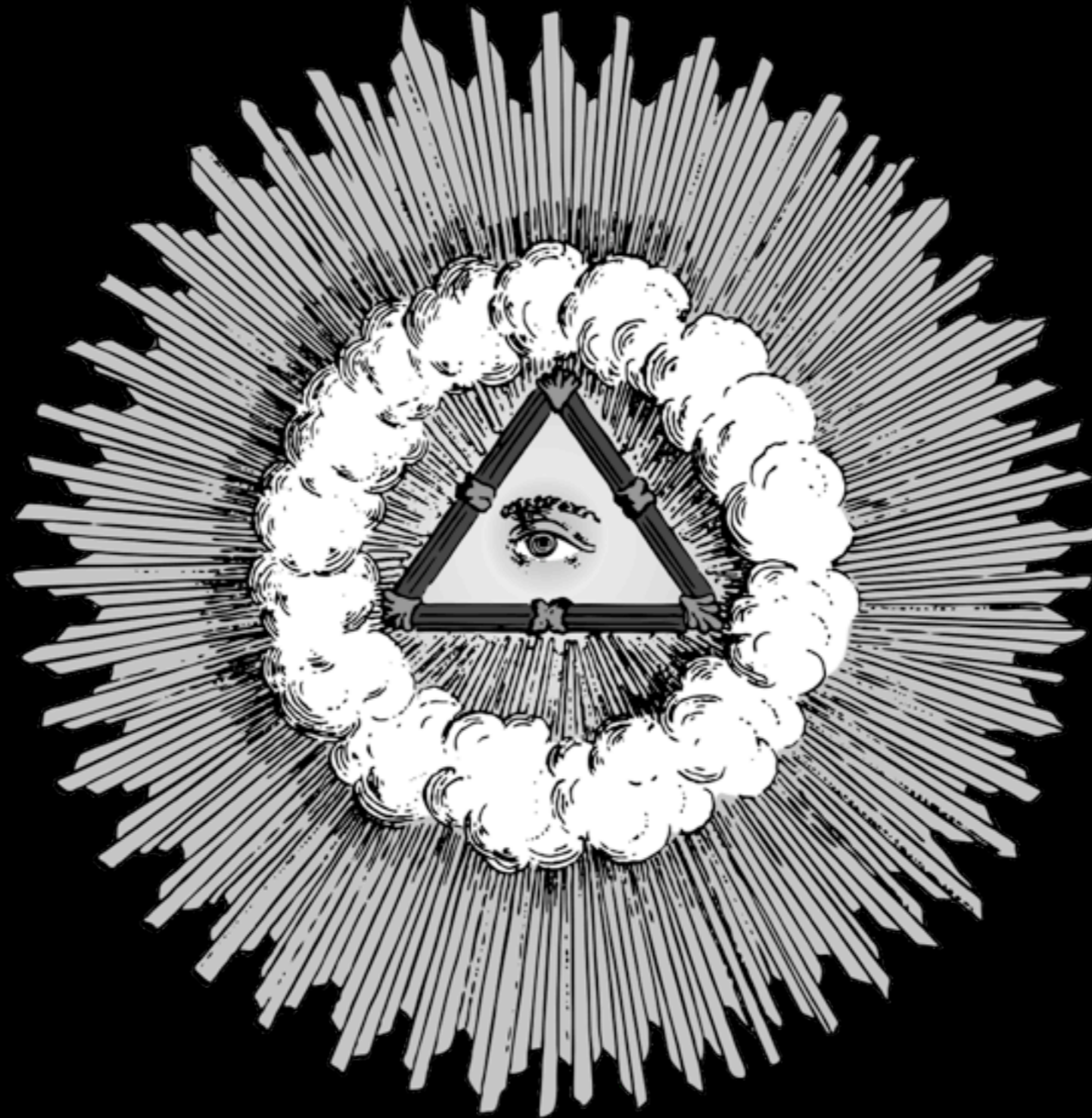


Image source: US Dept. of Transportation

Certificates

- Limited time use to prevent tracking
 - Reused?
- Periodically refreshed (and malefactors reported)
 - How often?



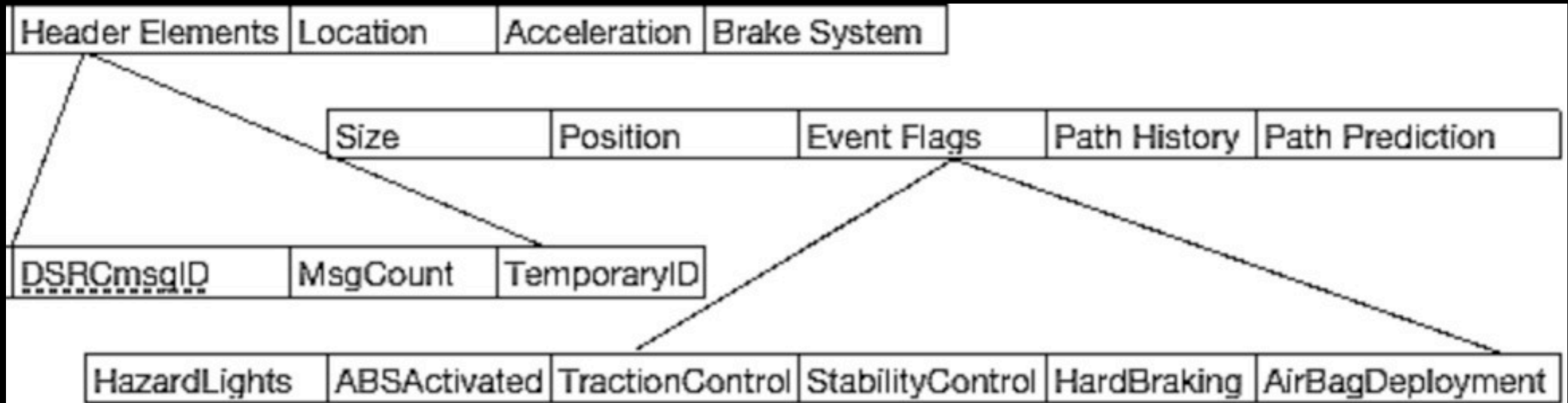
Privacy?

MAC Layer



- Changeable source (for vehicles) / no destination
- Unrouteable! (mostly)
- No significant privacy concern *as is*.
- **Any** algorithm to make network routeable will make vehicles trackable.

BSM



- “Temporary” ID could become persistent with bad app
- Open source apps suggested for processing and acting on message data

Certificates



- Identity/Validity conflict
 - Solution: constantly changing certificates
 - Revocation by fingerprint
- Issuing authority?

Fingerprints

- “No” correspondence between fingerprint and car
- “hard coded” into device
- If revoked, entire unit must be replaced to function

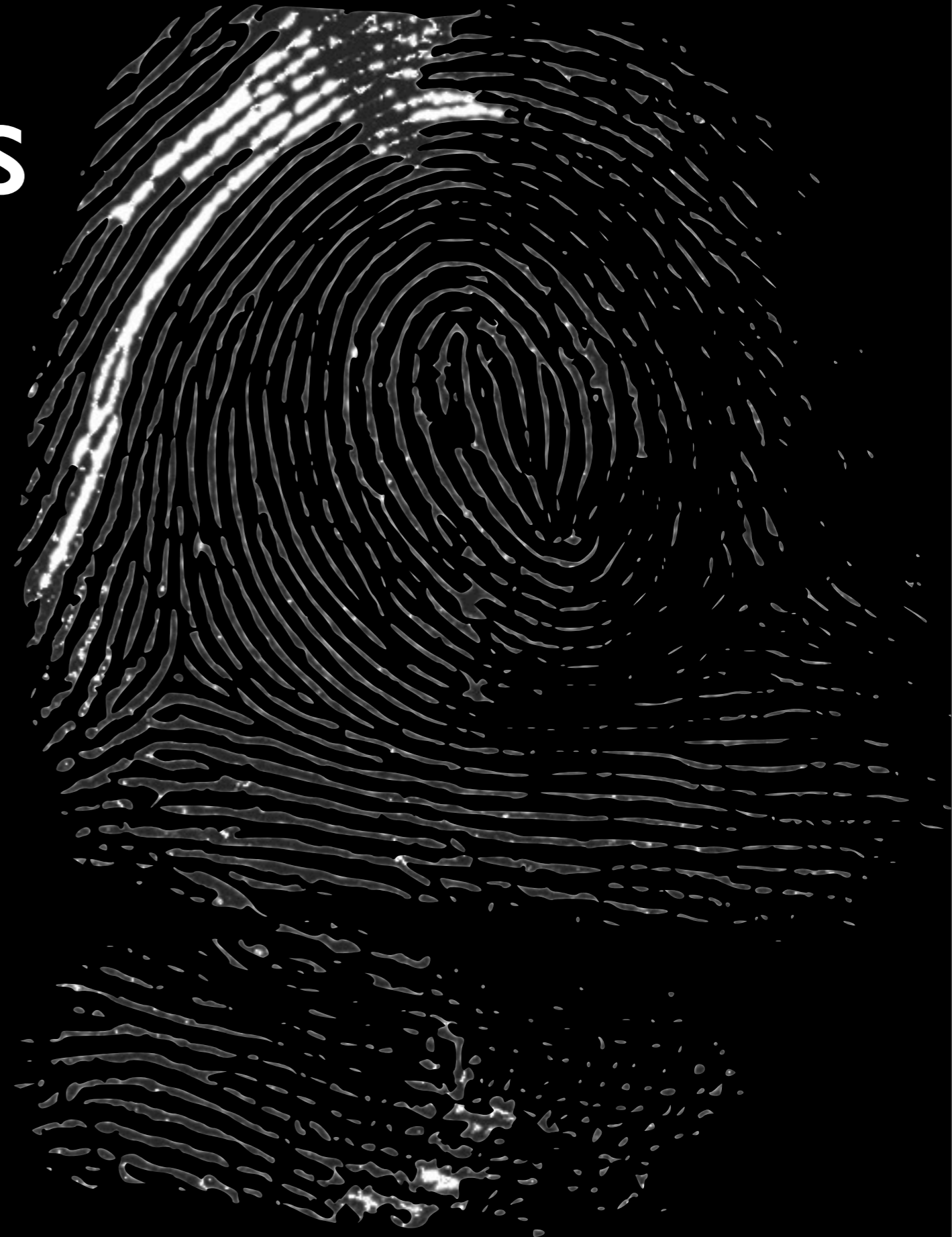


Photo Credit: NIST

Certificate Delivery



- Haven't figured out how certificates are delivered to vehicle
- Proposals include cellular, wifi, infrastructure links
- So many opportunities for failure

Worrisome Noise



- Manufacturers want to use this system for commercial apps
- Advertising and other “funding” schemes to pay for CA
- Fixed infrastructure potentially operated by data brokers

Problem: Law Enforcement

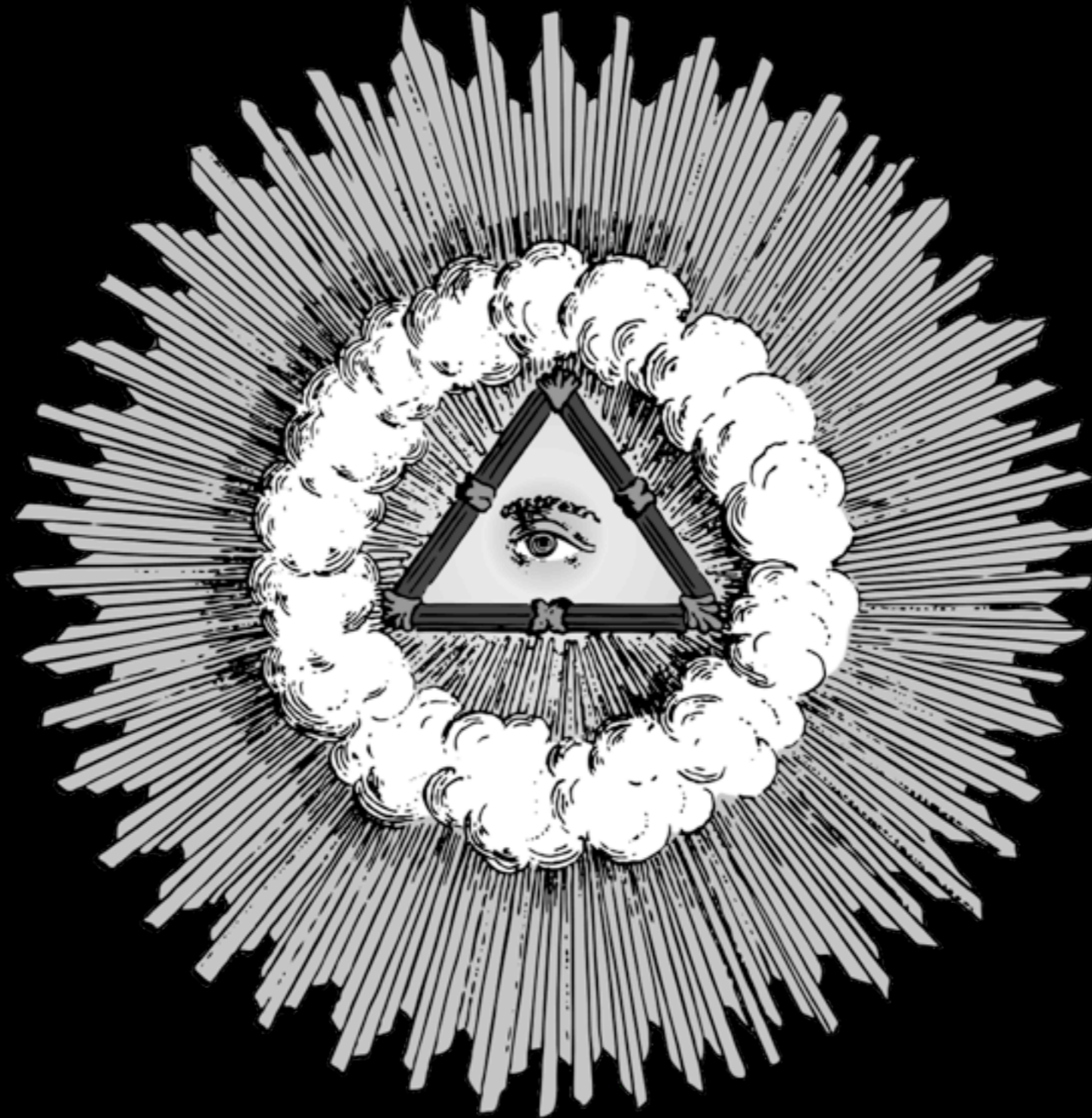
- What can they do with this?
- Correlate location, speed to independent identification? (cameras?)



Photo Credit: Alex E. Proimos

What you Can Do

- Hack the radios
 - Commercially available now
- Hack the protocols
- Become politically engaged
 - Most decisions are not being made by elected officials
 - Help find a way to fund the infrastructure without selling out!



Thank you

Acknowledgements

- Professor Dorothy Glancy, who requested my help on this project
- DC 650 (especially Charles Blas) who gave me a reality check with current security and privacy capabilities

Contact

- Christie Dudley
- @longobord
- cdudley@scu.edu