PRIVACY PROTECTION IN TRAFFIC SURVEILLANCE SYSTEMS

Professor Dorothy Glancy
Santa Clara University School of Law

WISE 2010: Women's Institute in Summer Enrichment
Team for Research in Ubiquitous Secure Technology (TRUST)
June 23, 2010 Vanderbilt University, Nashville, TN

Roadmap

- Traffic surveillance technologies
- Privacy Interests on the open road
- Privacy Audit of Traffic Watch
- Proactive Privacy Strategies for Future Ubiquitious Traffic Surveillance Systems
  - Vehicle Infrastructure Integration (VII)
  - IntelliDrive

International Comparative Study of Interactions

Privacy ⇦⇨ Traffic Surveillance

Japan

Smartway

United Kingdom

Congestion Charging & ANPR

Automated Number Plate Recognition

United States

IntelliDrive

Vehicle Infrastructure Integration (VII)

How to assure privacy protection in advanced traffic surveillance systems

1. Privacy Audit of a traffic surveillance system

2. Proactive Framework for building privacy into an even more advanced system.

Advanced Traffic Surveillance Systems

Multifunctional networks that may collect personal information and affect driver behavior

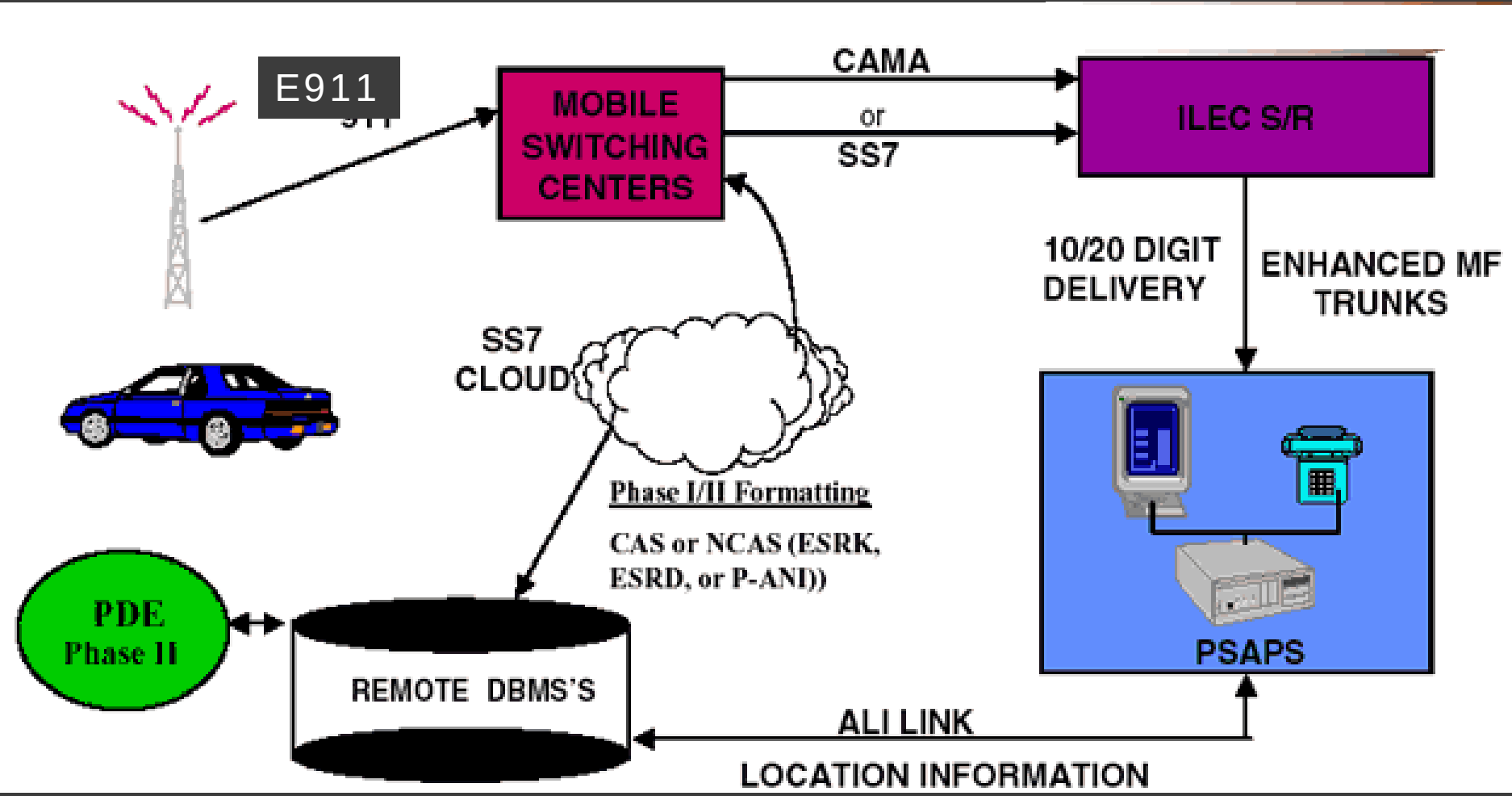
- Multi-purpose
- Interconnected
- Multiple technologies
  - Remote sensing
  - Information technologies
  - Wireless communications
- Mass surveillance

Traffic Surveillance Technologies

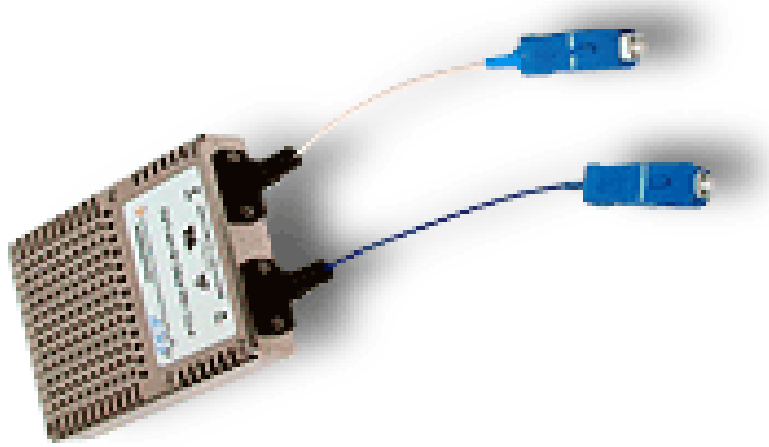
- Wireless communications (Telematics)
- Beepers & GPS tracking devices
- Traffic cameras
- Radar and photo radar (human and automatic)
- Toll tags (FasTrak, EasyPass, etc.)

Wireless Network Telematics

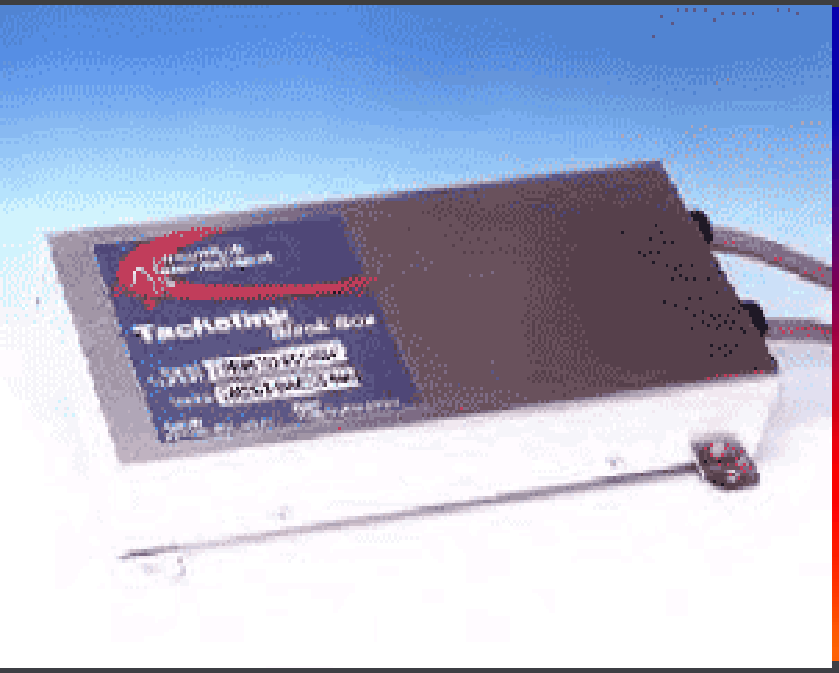
e.g. OnStar

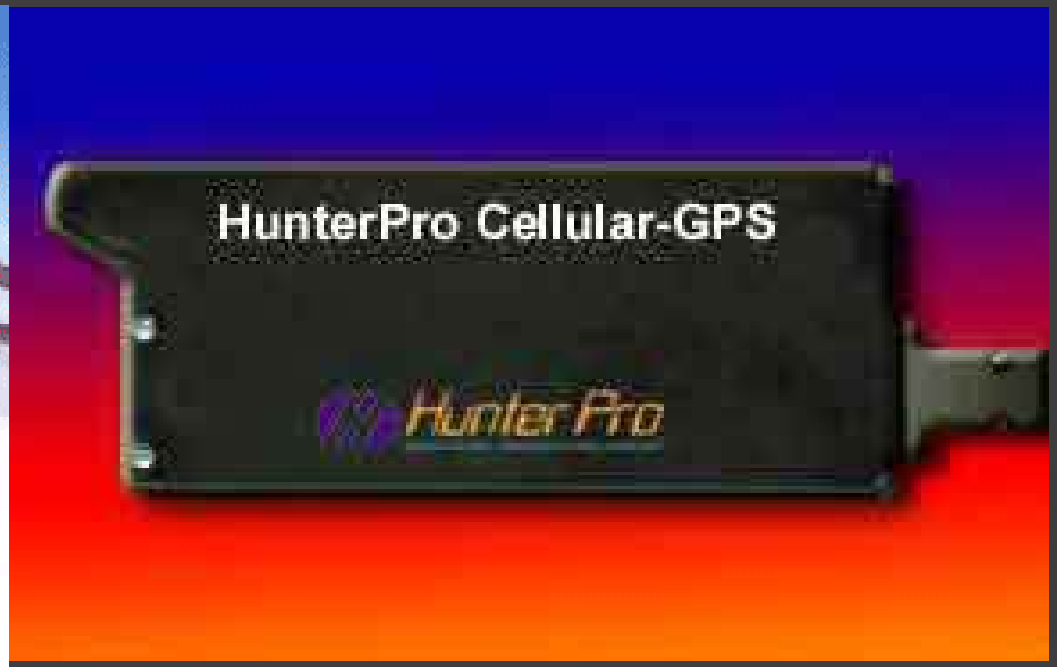


Beepers



GPS Tracking Devices





Traffic Cameras

Photo Radar

Photo Radar Systems

Automated Law Enforcement

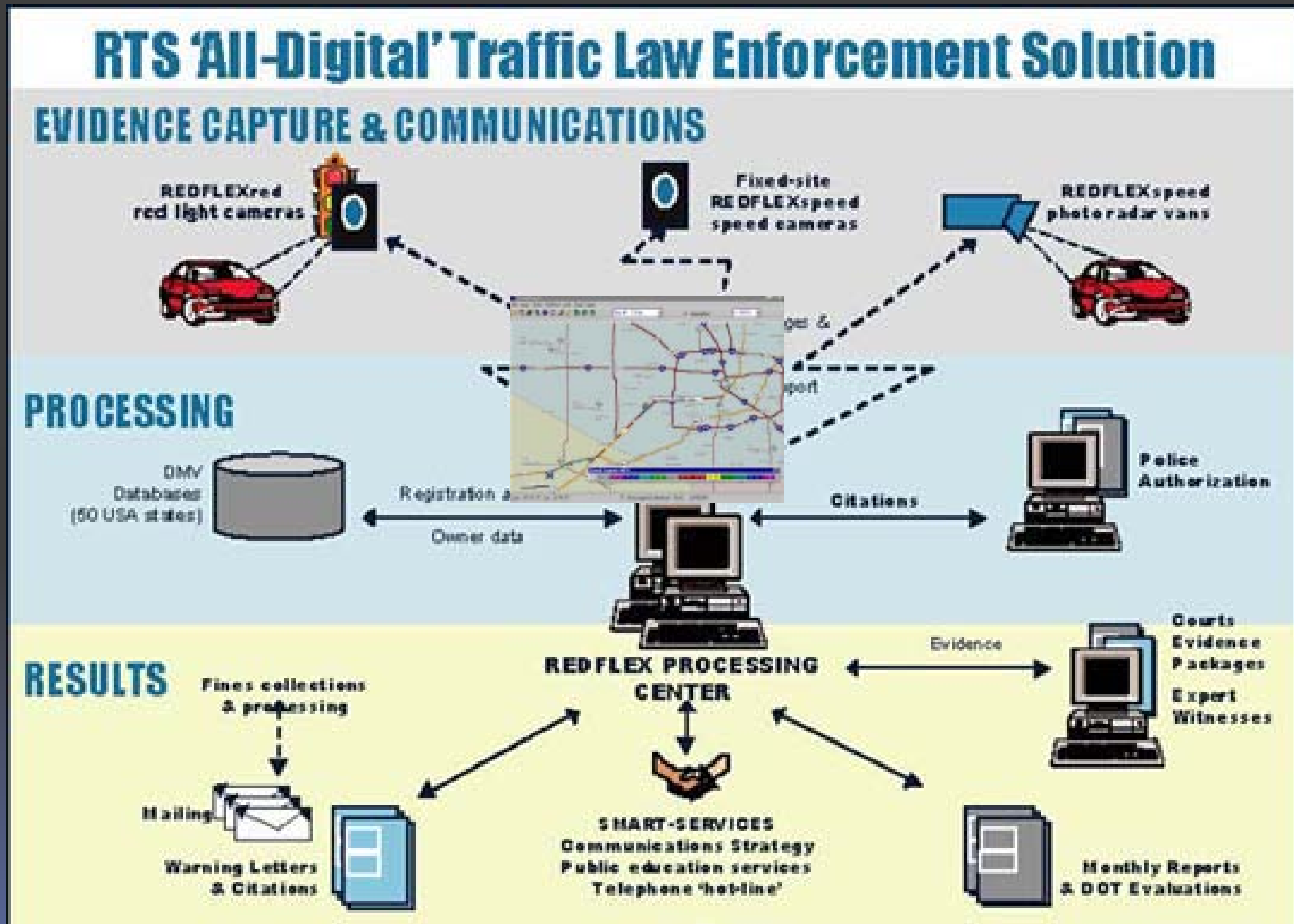
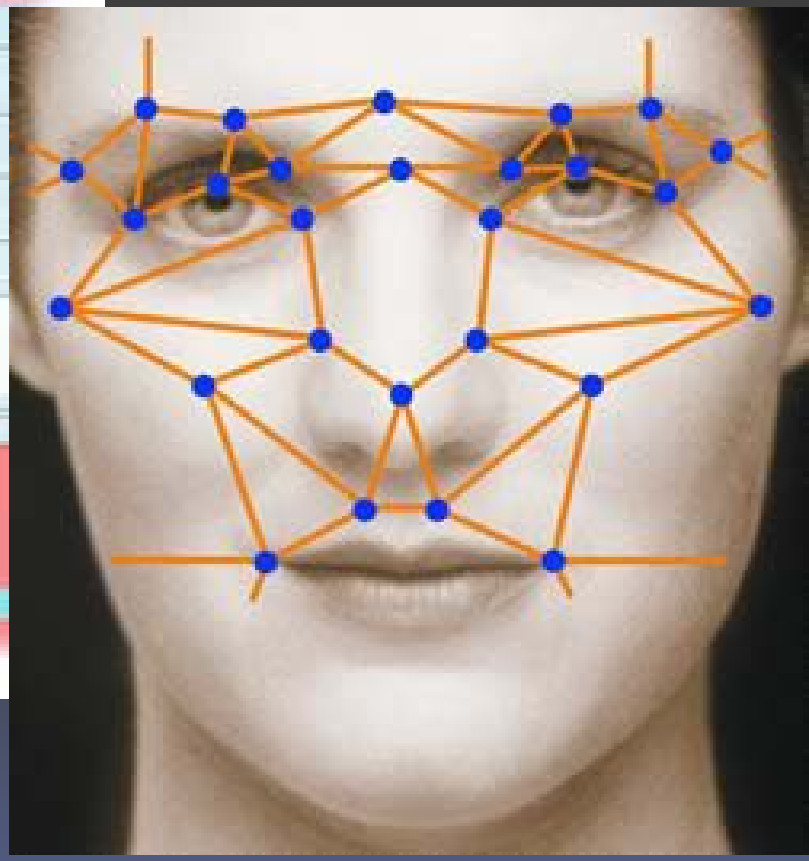


Photo Radar Ticket

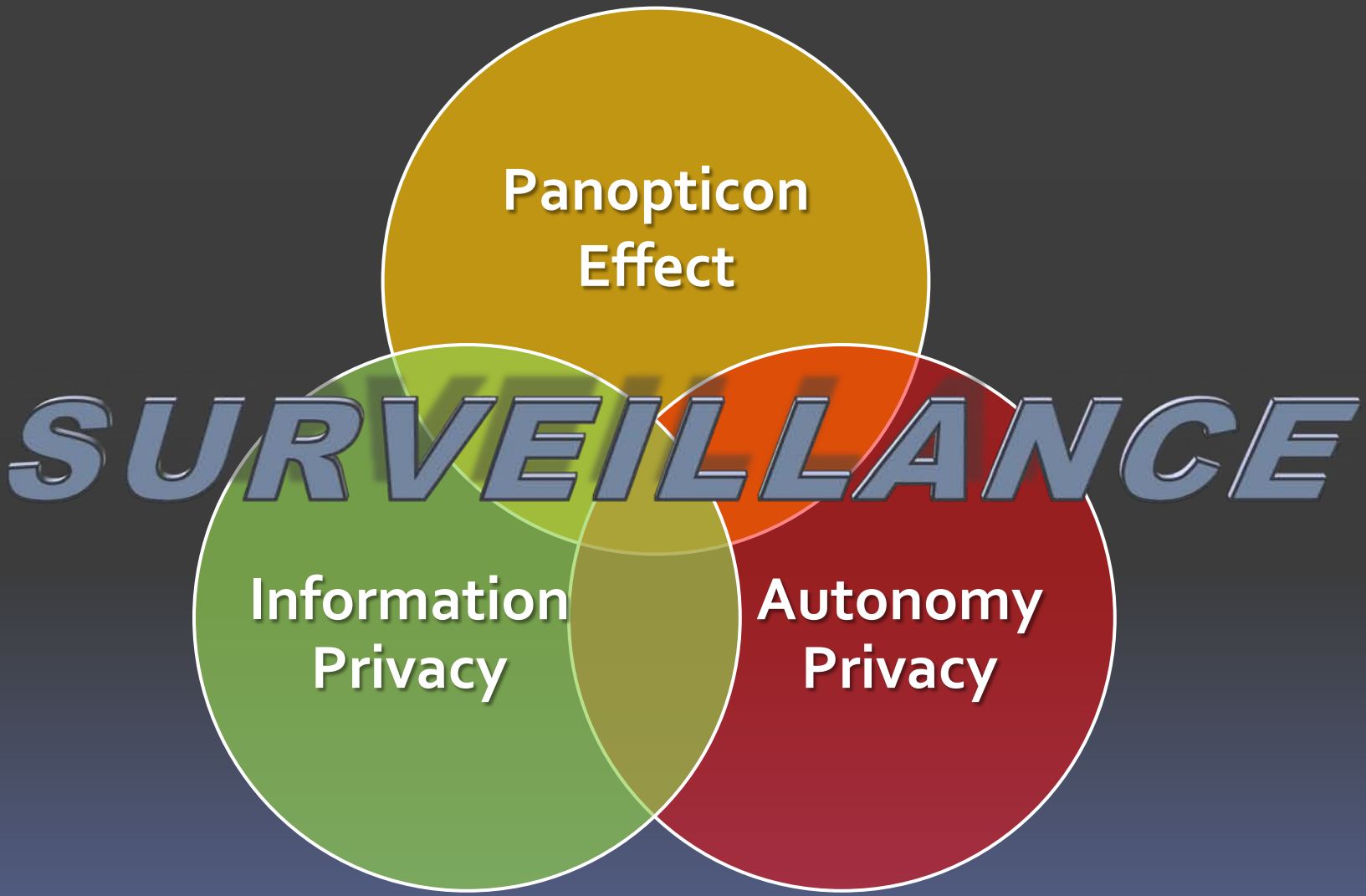
Facial Recognition



Toll Tag Transponders

Professor Dorothy Glancy - Santa Clara University School of Law
WISE 2010: Women's Institute in Summer Enrichment - Team for Research in Ubiquitous Secure Technology (TRUST)
June 23, 2010 Vanderbilt University, Nashville, TN

Privacy Interests



INFORMATION PRIVACY

Interests in precluding the collection, dissemination or misuse of sensitive and confidential information about an individual human person without that person's consent.

"informational privacy"

location, itinerary, personal travel routes

Origin-Destination (OD) data

AUTONOMY PRIVACY

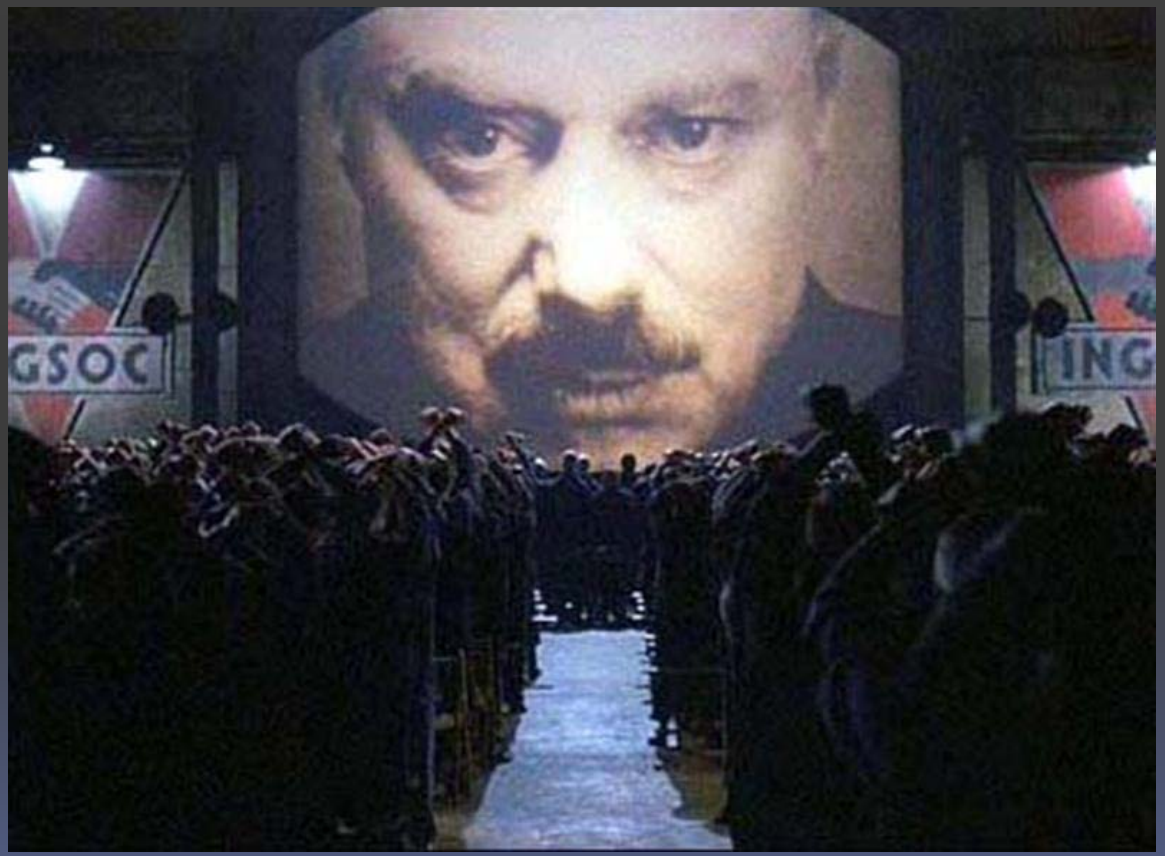
Interests in making intimate personal decisions or conducting personal activities without interference .

Individual self-determination regarding who will have how much access to that individual.

Decisions about where and when to drive.

PANOPTICON EFFECT

Big Brother



VOSA

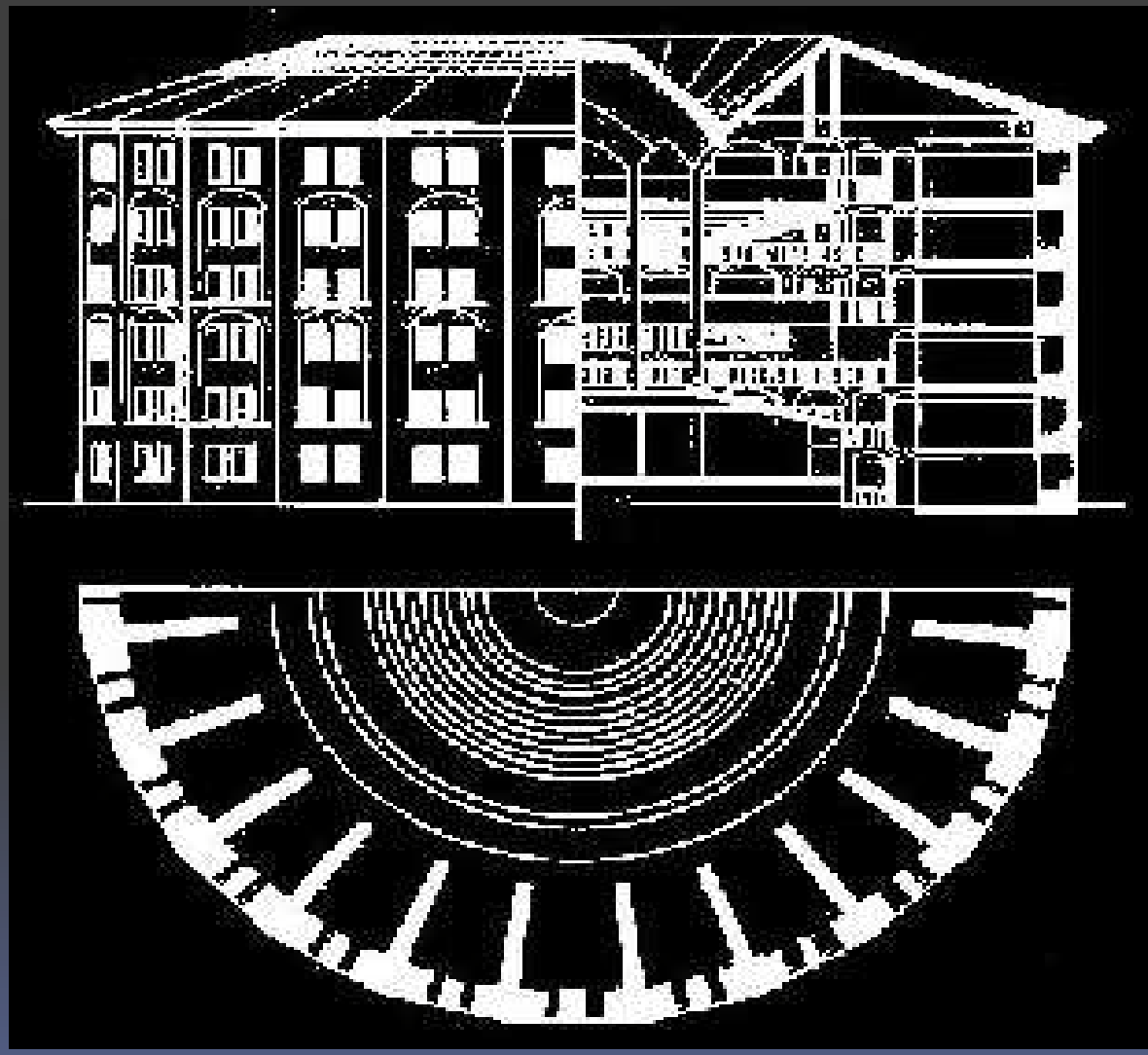
Vehicle and Operator Services Agency

"Saving lives, safer roads, cutting crime, protecting the environment"

The Panopticon Effect

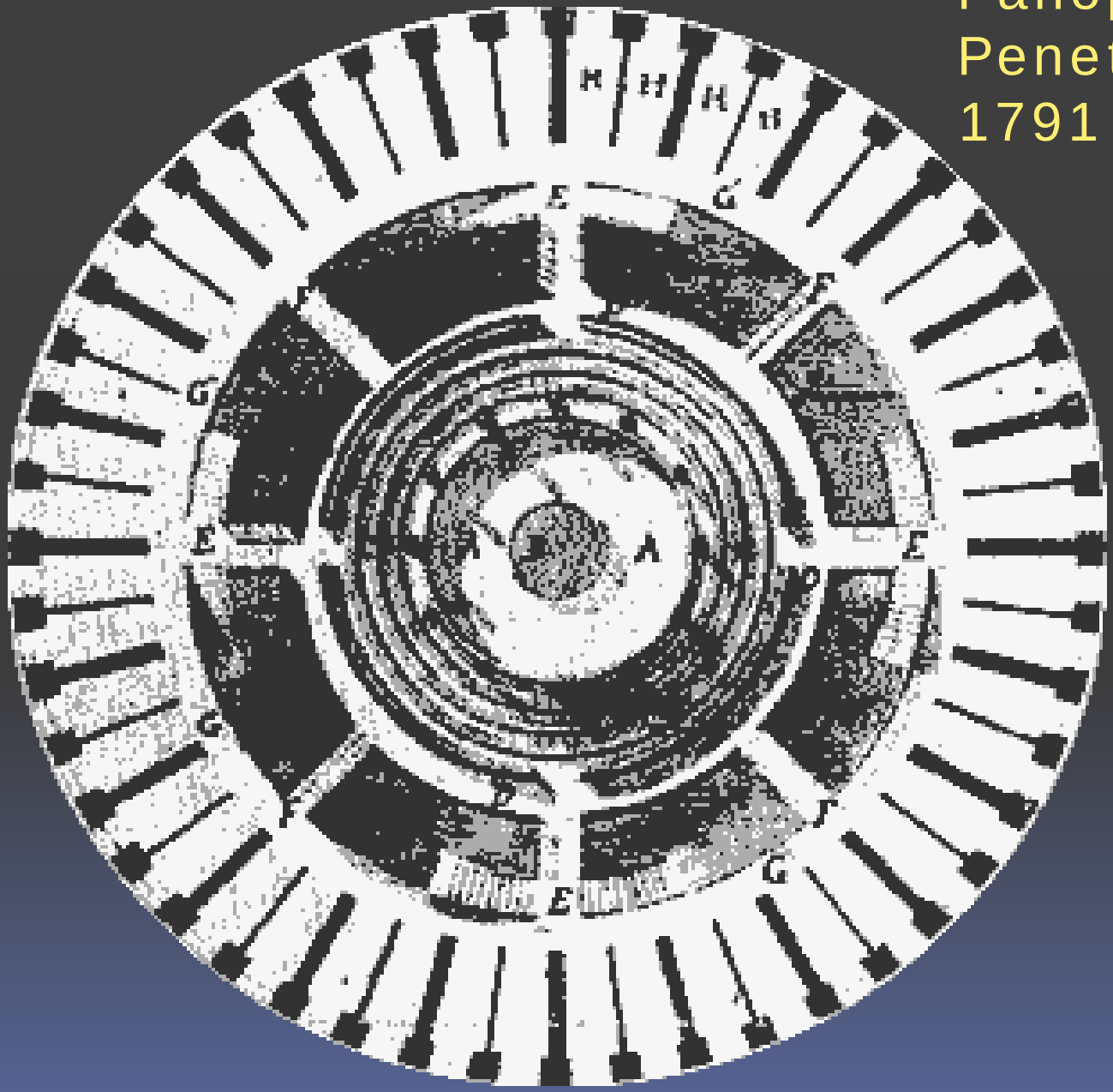
Jeremy Bentham's
Panopticon
Prison
(1791)

In the 20th Century
Michel Foucault
Discipline and Punish
(1978)



Floor Plan

Jeremy Bentham's
Panopticon
Penetentionary
1791

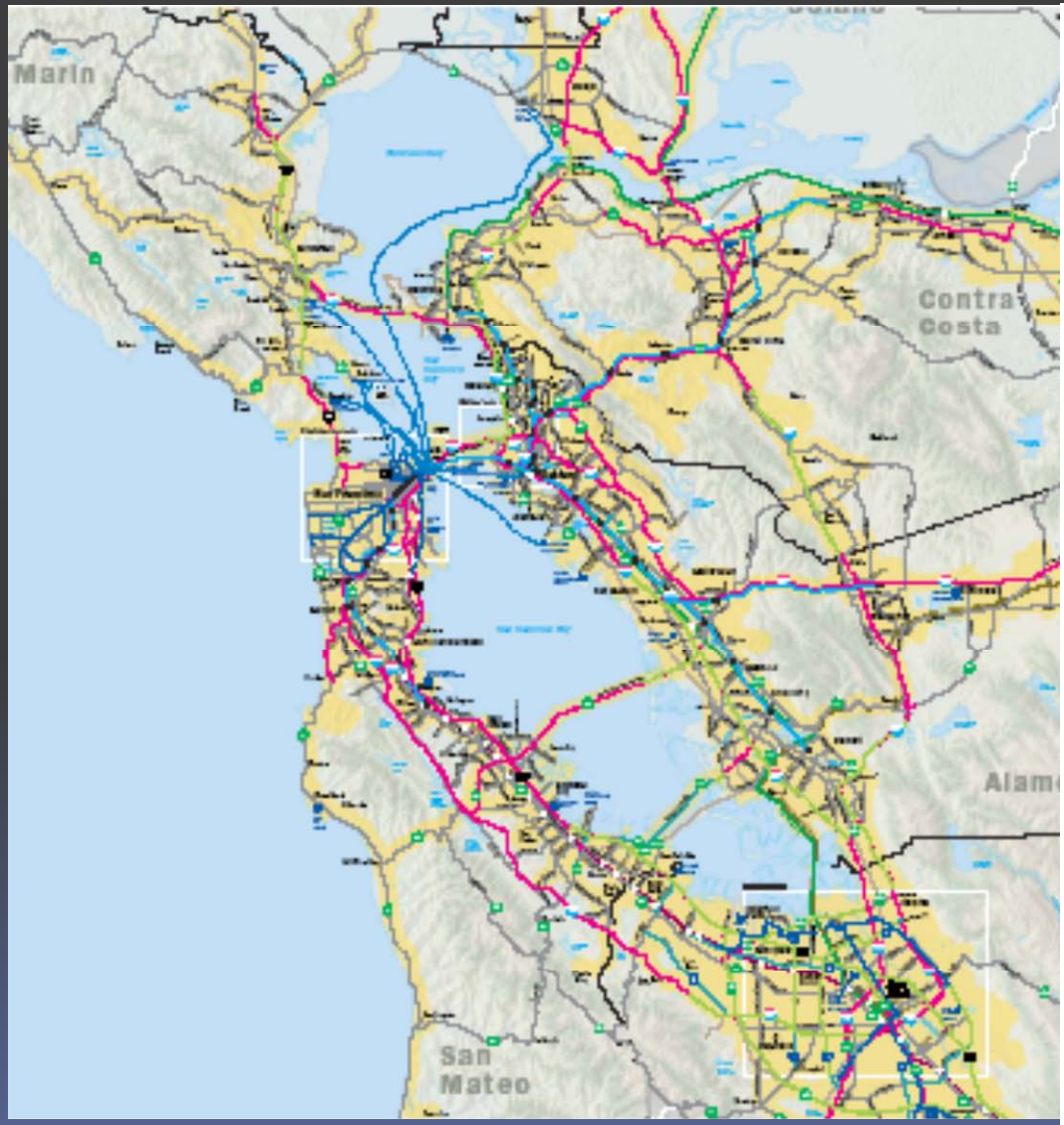


Total Information Awareness

Terrorism Information Awareness

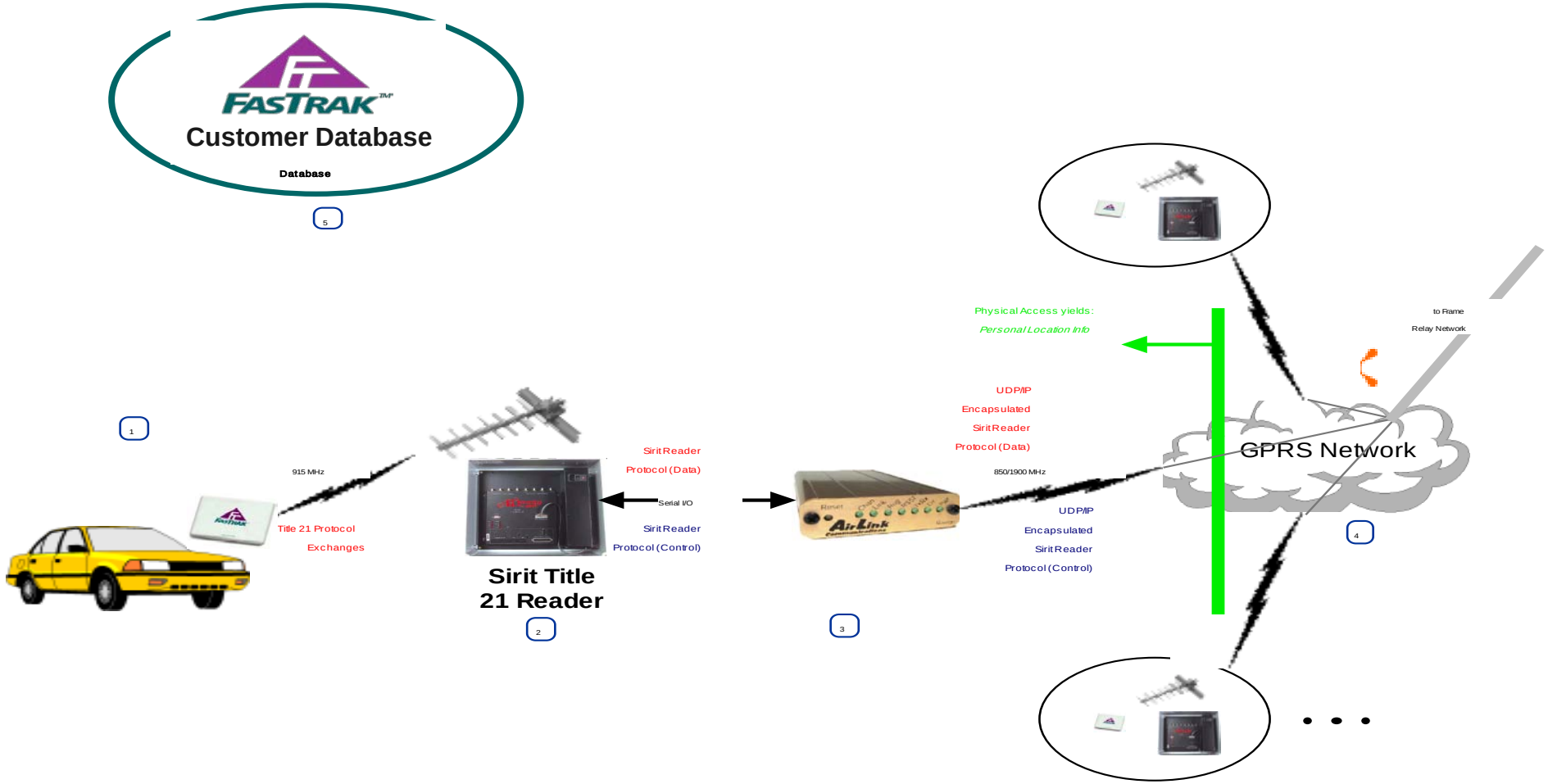
A Traffic Surveillance System Privacy Audit

San Francisco Bay Area Metropolitan Transportation Commission



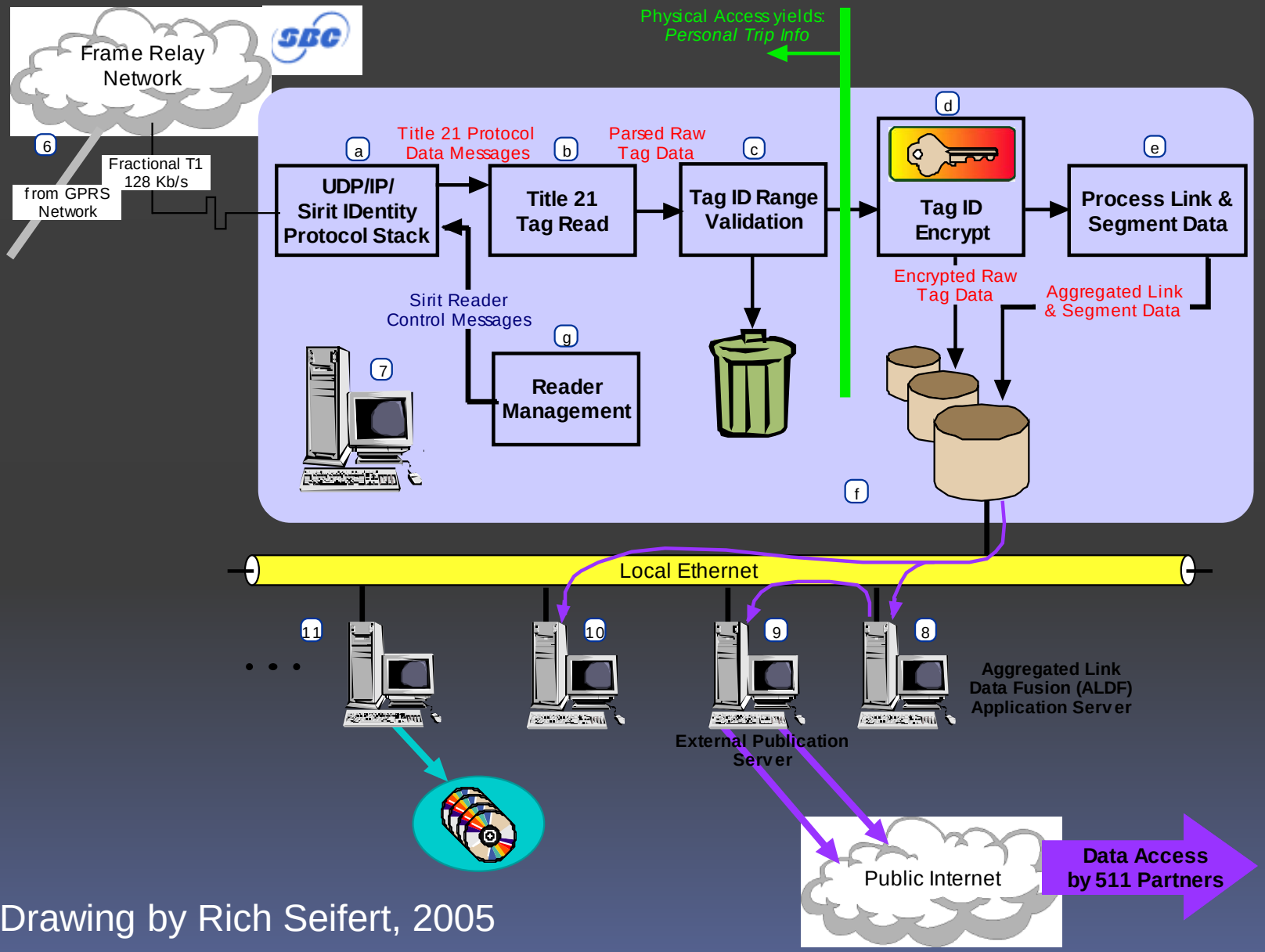
2004
Traffic Watch
Privacy
Assessment

Traffic Watch Privacy Assessment



Drawing by Rich Seifert, 2005

Traffic Watch Privacy Assessment



Drawing by Rich Seifert, 2005

CRITERIA FOR 2004 PRIVACY AUDIT

Federal Legal Requirements
18 U.S.C. § 2510/2511, 18 U.S.C. § 3117, CALEA, USA PATRIOT Act
18 U.S.C § 1029
47 U.S.C. § 222
Federal search/seizure law
California Law
Constitutional Privacy Guarantee, Art. I, § 1
California Event Data Recorder Statute: Cal. Vehicle Code § 9951
California Tracking Device Statute: Cal. Penal Code § 637.7
MTC Privacy Guidelines
1. All traffic data collection activities will be implemented in a manner consistent with Federal and California laws governing an individual's right to privacy.
2. The tag users' consent will be secured before the operation of any data collection system based on toll tags.
3. Encryption software in the central software system will mask each tag ID before any other processing is done to ensure that the toll tags are treated anonymously.
4. The encrypted tag IDs will be retained for no longer than twenty-four hours and then discarded. No historical database of the encrypted IDs will be maintained beyond that time period.
5. No information about, or that is traceable to, any individual person will be collected, stored, or manipulated.
6. Information on the data collection, aggregation and storage practices will be available at the 511 .org website, which will include traffic data collection methods, privacy policy, and full disclosure on the use of the data.
7. Members of the public will be given the ability to contact the program to discuss any privacy questions or concerns.
8. All recipients of the data shall comply with these privacy principles.
9. An annual evaluation will be conducted to assure that individual privacy is protected.

2004 Privacy Policy

1. All traffic data collection activities will be implemented in a manner consistent with Federal and California laws governing an individual's right to privacy.
2. The tag users' consent will be secured before the operation of any data collection system based on toll tags.
3. Encryption software in the central software system will mask each tag ID before any other processing is done to ensure that the toll tags are treated anonymously.
4. The encrypted tag IDs will be retained for no longer than twenty four hours and then discarded. No historical database of the encrypted IDs will be maintained beyond that time period.
5. No information about, or that is traceable to, any individual person will be collected, stored, or manipulated.
6. Information on the data collection, aggregation and storage practices will be available at the 511 .org website, which will include traffic data collection methods, privacy policy, and full disclosure on the use of the data.
7. Members of the public will be given the ability to contact the program to discuss any privacy questions or concerns.
8. All recipients of the data shall comply with these privacy principles.
9. An annual evaluation will be conducted to assure that individual privacy is protected.

FasTrak Privacy Policy as of 2008

How Personal Information is Used

Personal information will only be used by BATA, the Golden Gate Bridge, Highway and Transportation District (GGBHTD), and the California Department of Transportation (Caltrans) for the purpose of administering a FasTrak user's account and managing the FasTrak operations. In the course of administering FasTrak accounts, BATA may disclose personal information to third party service providers for the purpose of operating the FasTrak program (e.g., DMV, municipal courts, account processors or collection agencies); otherwise, personal information will not be disclosed to third parties, except as required by law or ordered by a court of competent jurisdiction. Information about a FasTrak user's use of the system, but which does not personally identify a user, may be disclosed to others to generate statistical reports for the purpose of managing the FasTrak operation.

FasTrak Privacy Policy as of 2008

Other Uses of Toll Tag Data

The Metropolitan Transportation Commission (MTC)/511 operates a data collection system based on FasTrak toll tags to provide better information about the transportation network to Bay Area travelers, transportation managers, and transportation planners through the 511 Driving Times^{SM} service. Encryption software is used to mask each toll tag identification number to ensure that toll tag information is treated anonymously in the data collection process. For more information on the 511 Driving Times^{SM} service and how customer data is protected, please refer to MTC 511's Privacy Notice.

FasTrak Privacy Policy as of 2008

Security

BATA will take all reasonable steps to safeguard personal information through physical, electronic and procedural means. BATA will treat FasTrak user information confidentially and require third party service providers to treat it in the same manner.

FasTrak users retain the right to review and edit all of their personal information pertaining to their accounts, whether stored electronically or on paper. Personal information can be reviewed and edited online at http://www.bayareafastrak.org/dynamic/accounts/index.shtml. Any inquiry or request to obtain information, in accordance with the above provisions, should be directed in writing to the FasTrak Customer Service Center or to BATA. BATA may adopt procedures for review of such information, including but not limited to charging a fee for processing requests for access to personal information.

Effective Date

The effective date of this privacy policy is May 25, 2005, as amended on September 24, 2008. If BATA makes changes to this privacy policy, BATA will post the revised policy on its FasTrak website, including the date of any amendments.

Current 2010 Privacy Notice

511 Driving Times℠

In the 511 Driving TimesSM service, MTC/511 operates a data collection system based on FasTrak® toll tags to provide better information about the transportation network to Bay Area travelers, transportation managers, and transportation planners.

In matters concerning traffic data collection, MTC/511 will take the following steps to ensure the protection of personal information:

- The tag users' consent will be secured via a FasTrak® toll tag license agreement before the operation of any data collection system based on toll tags.
- Encryption software in the central software system will mask each tag ID before any other processing is done to ensure that the toll tags are treated anonymously.
- The encrypted tag IDs will be retained for no longer than twenty-four hours and then discarded. No historical database of the encrypted IDs will be maintained beyond that time period.
- Every two years, or the year following any major change in the 511 Driving Times system (whichever occurs first), a comprehensive assessment of privacy protection will be performed.

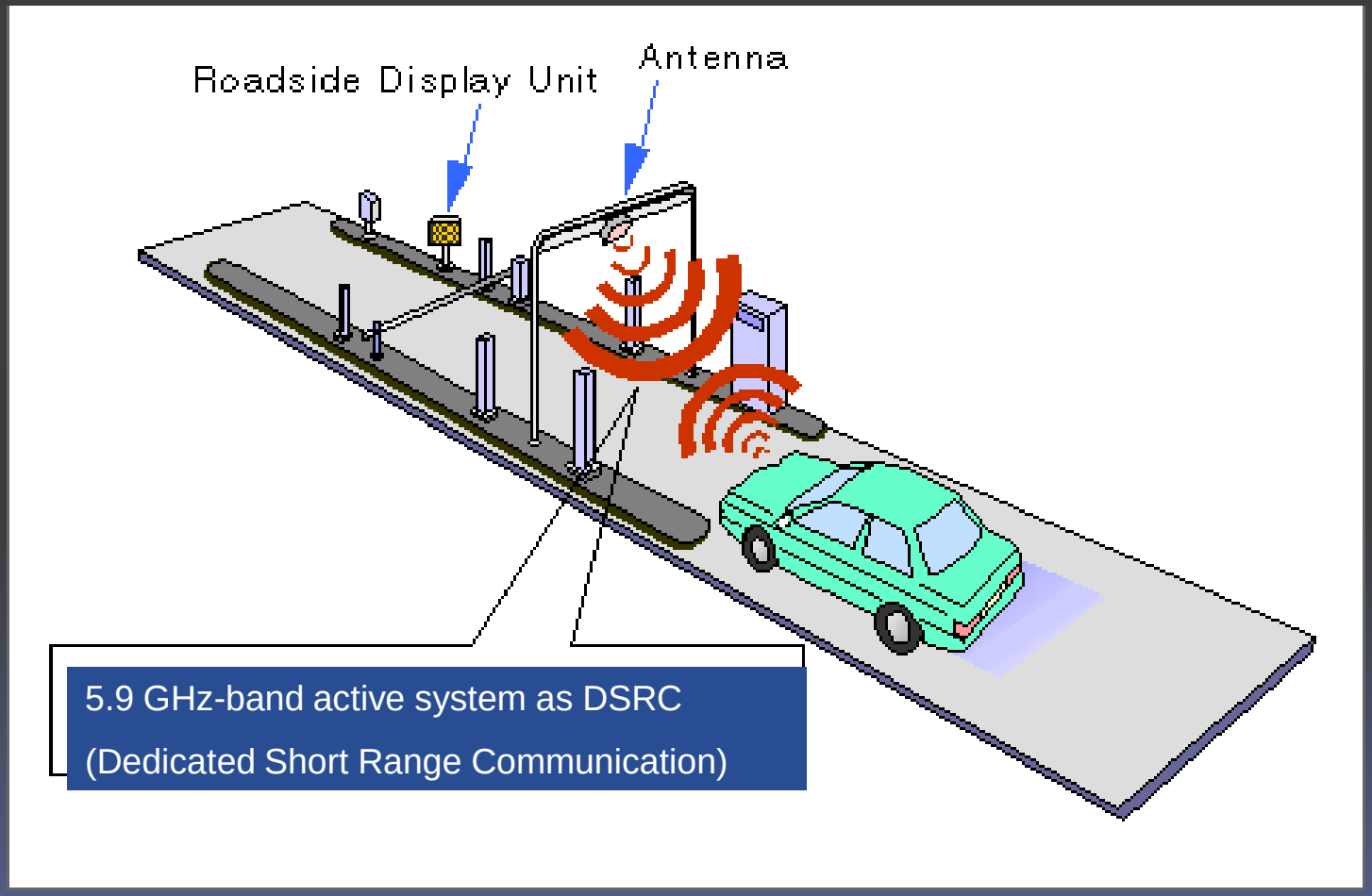
Being Proactive about Privacy in a nationwide mass surveillance system

Vehicle Infrastructure Integration (VII)

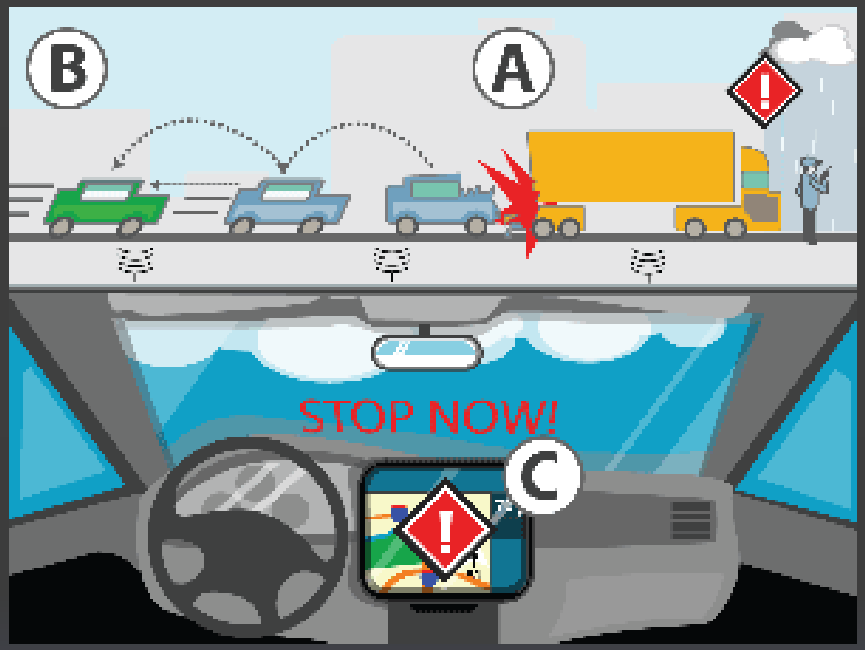
- National system, decentralized
- Combined purposes: safety, mobility, convenience
- Embedded in vehicle
- VII Privacy Policies Framework

Vehicle Infrastructure Integration (VII)

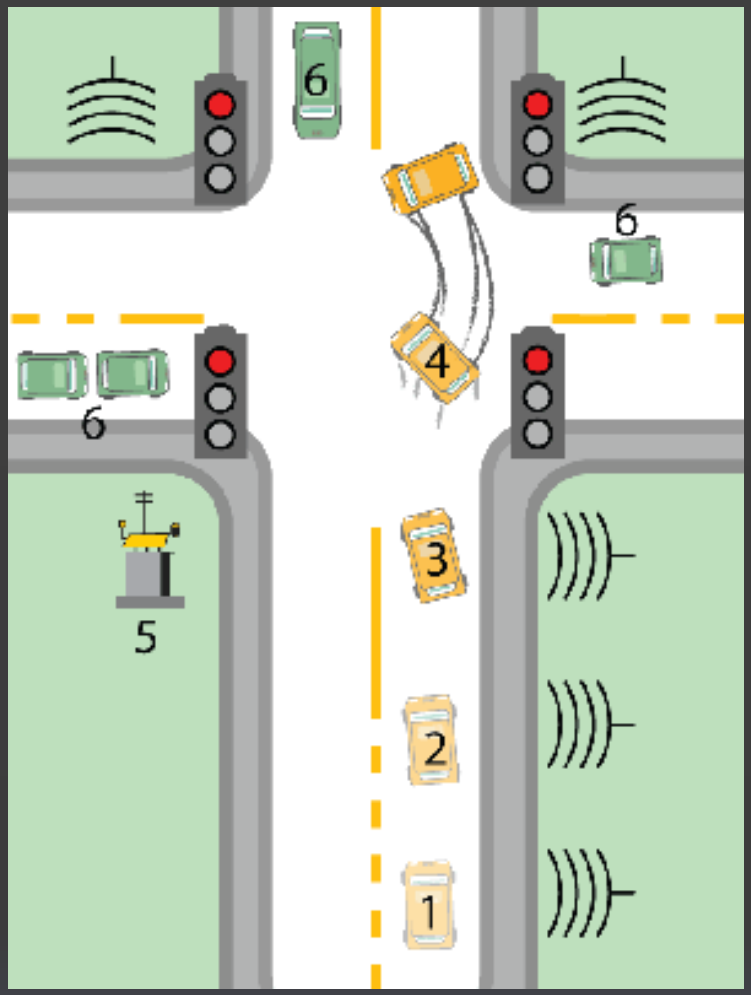
Using Dedicated Short Range Communications (DSRC) 5.9 GHz



FCC Report and Order, Release-Number FCC 03-324 (released Feb. 10, 2004).



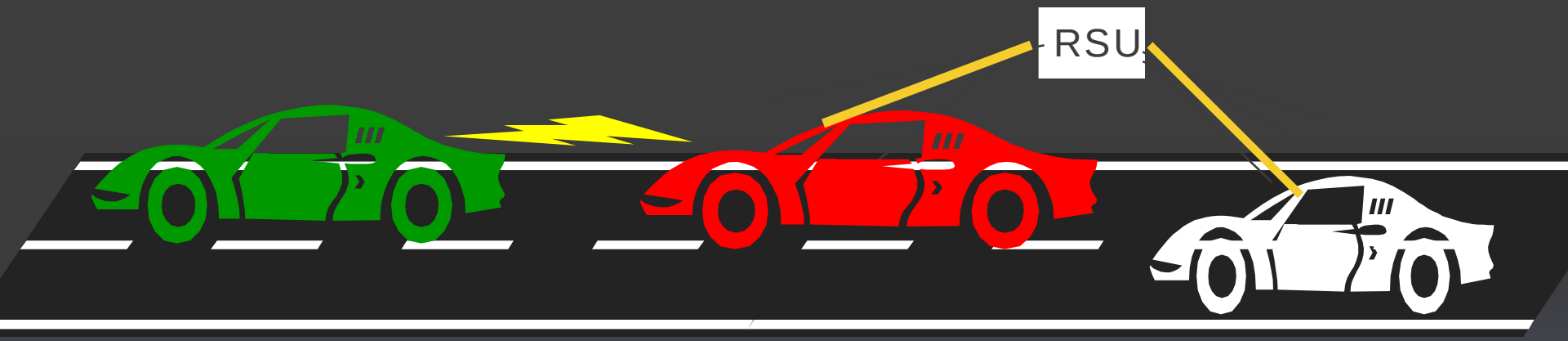
A. **Incident occurs upstream.**
B. **Incident alerts/warnings transmitted vehicle to vehicle and vehicle to roadside.**
C. **Vehicle-based safety systems activate.**



1. Potential red light violator approaches intersection.
2. Potential red light violator receives in-car warning.
3. Potential violator stops in time; or if not,
4. Violator crosses into intersection.
5. Roadside infrastructure detects violator.
6. Warning sent from roadside to other cars.

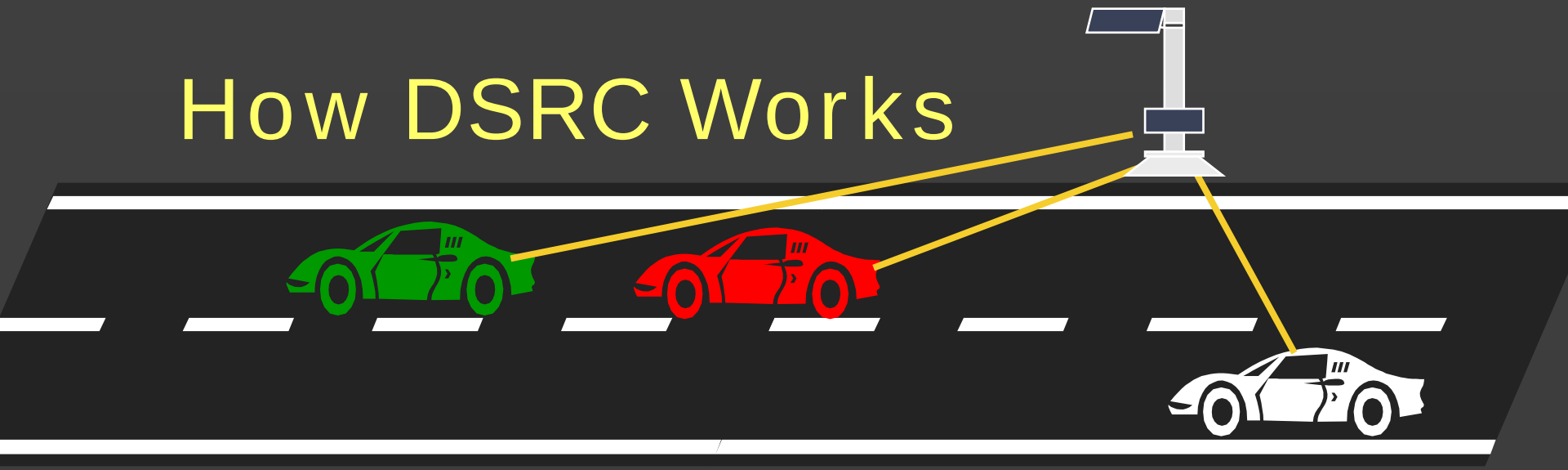
What Is VII?
Vehicle Infrastructure Integration

- An "Enabling Communication Infrastructure" to support real time vehicle-to-vehicle And Vehicle-to-Infrastructure Communications



Supporting Safety AND Mobility Applications

How DSRC Works



- RSE announces applications (AID)
  - up to 10 times a second
- When vehicle enters communications zone
  - Checks AID
- Executes Application
  - Sends message
- *AID must exist in both Vehicle & roadside*

On-Board Equipment / Unit

Sources of Privacy Protections in VII

- **Privacy Policies** articulating Industry and Government commitment to privacy protection
  - Privacy Policies Framework
  - Transparency
- **Technical Tools** protect communications and personal information
  - Encryption
  - Randomly Changing MAC addresses
  - Stripping IDs from traffic management information
- **Legal Requirements** protect personal information
  - Choice and Consent
  - Minimization
  - Anonymization
  - Data security requirements
    - Encryption
    - Data destruction and removal

See you on the highway!

Professor Dorothy J. Glancy
Santa Clara University School of Law
Santa Clara, California

dglancy@scu.edu