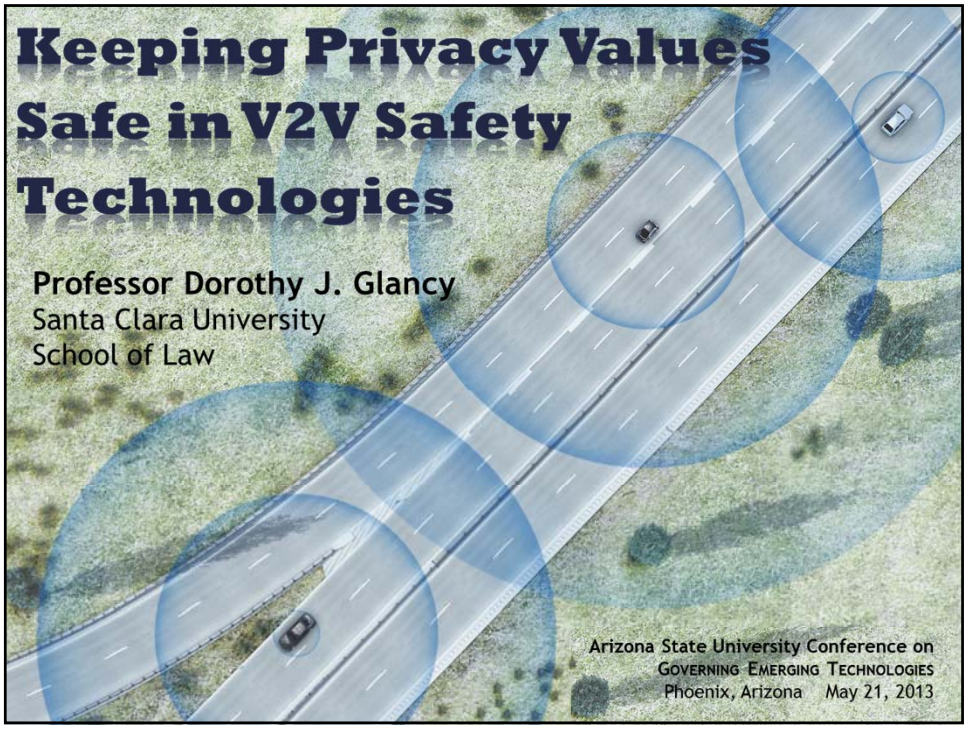
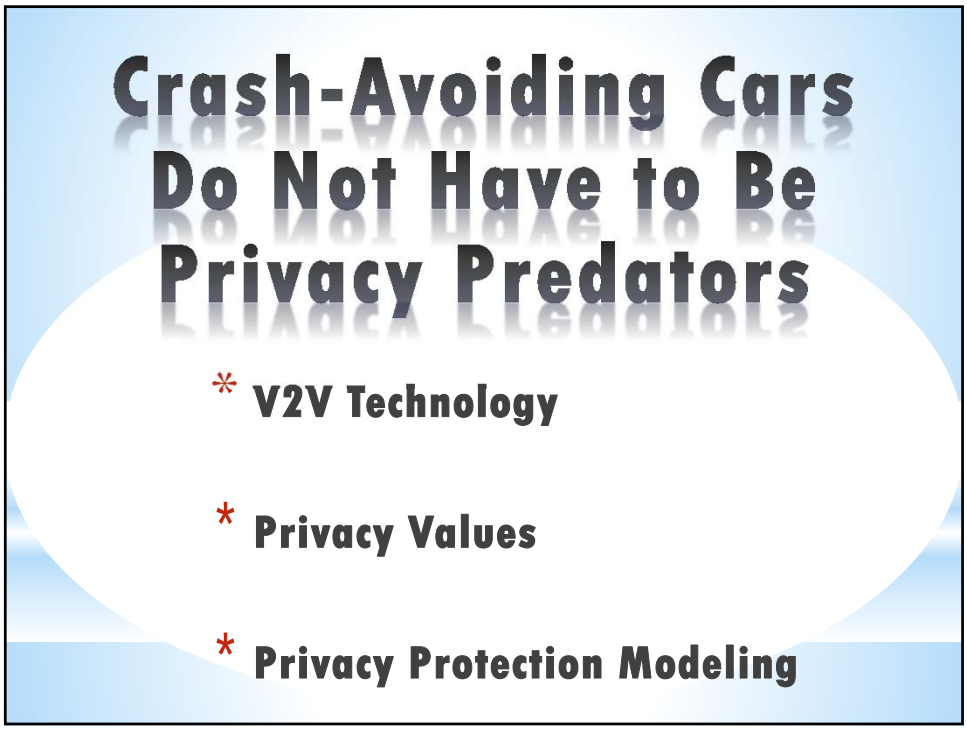
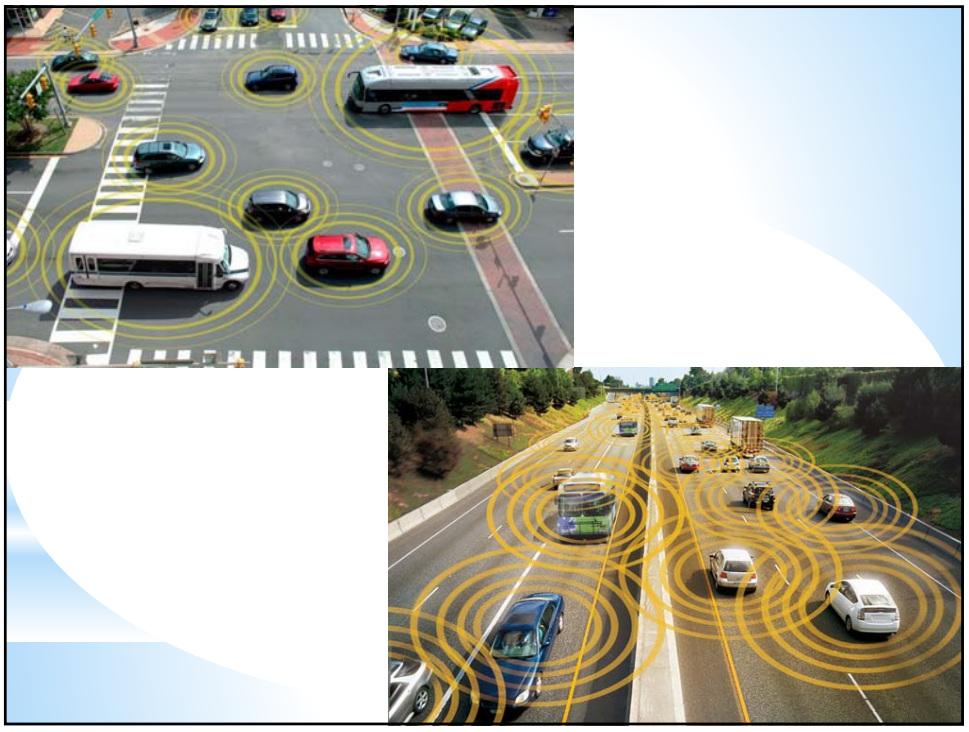

Keeping Privacy Values Safe in V2V Safety Technologies
Professor Dorothy J. Glancy
Santa Clara University
School of Law
Arizona State University Conference on
GOVERNING EMERGING TECHNOLOGIES
Phoenix, Arizona May 21, 2013

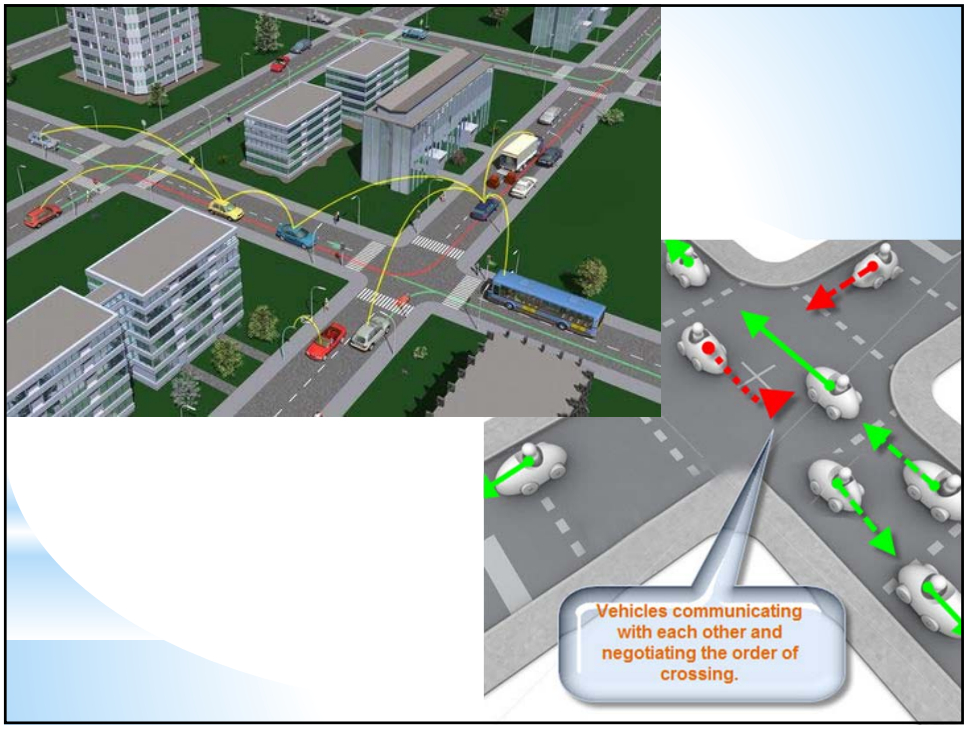

Crash-Avoiding Cars Do Not Have to Be Privacy Predators
* V2V Technology
* Privacy Values
* Privacy Protection Modeling

V2V Safety Technology

* Interoperable (all makes, models, etc.)
* Ad hoc vehicle networks nationwide

* Basic Safety Data Exchange
  * 5.9 GHz DSRC wireless
  * GPS
  * Vehicle diagnostic data
* Goals
  * Safety
  * Trustworthiness
  * Anonymity





Two–Part Communication
Transmitted ten times every second

IEEE Standards 802.11p and 1609

Certificate — PKI encrypted Identifier, including Link ID that connects certificates used by a specific device

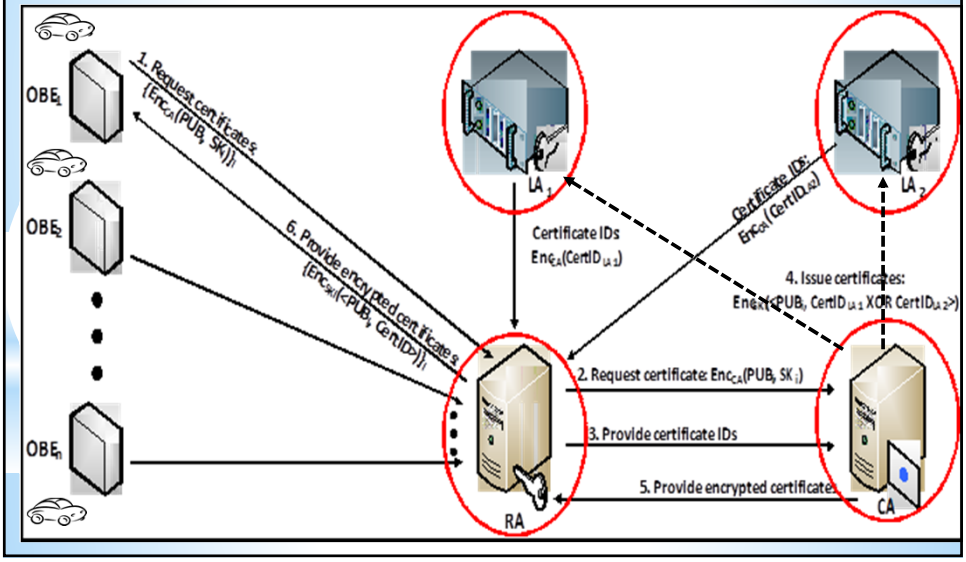
V2V Basic Safety Message

SAE J2735 Standard

- **GPS Position**
- **Speed**
- **Acceleration**
- **Heading**
- **Transmission State**
- **Steering Wheel Angle**
- **Brake Status**
- **Path History**
- **Path Prediction**

Transmitted in the clear (Unencrypted) 10 x second

Prototype Certificate Issuance
Security Credential Management System



Types of Privacy Values
Types of Privacy Challenges

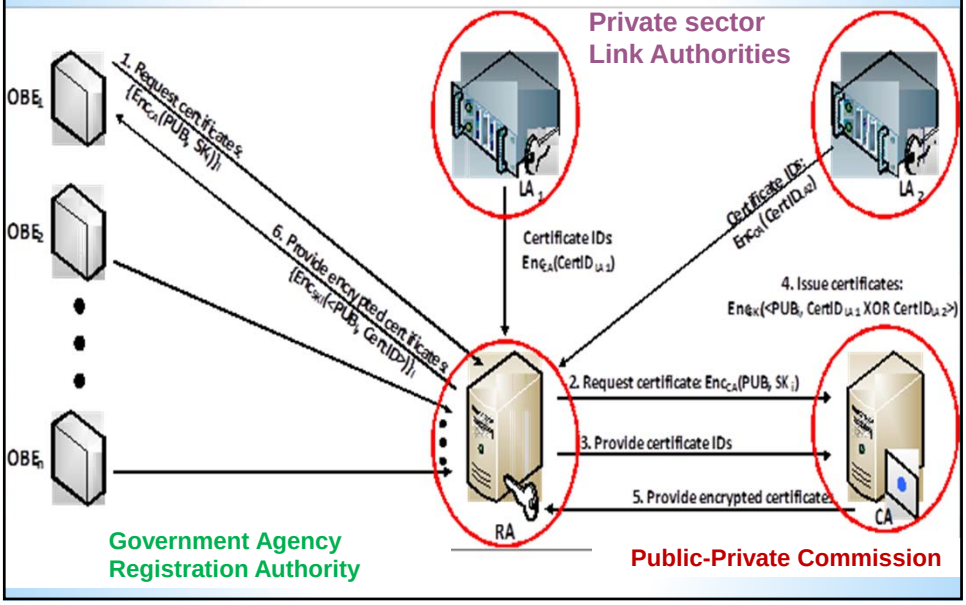
* Ethical
* Legal
* Political

* Anonymity
* Personal Information
* Surveillance

Privacy Model

* **Technological** – PKI for Certificates
* **Security Credential Management**
  - Random bundles of certificates
  - New certificate every 5 minutes
* **Governance**
  - Separate types of separated entities

Security Credential Management System Distributed Governance



Thank you!

Safe travels !

Professor Dorothy Glancy
Santa Clara University School of Law