Security and Privacy-Aware Cyber-Physical Systems: Legal Considerations

Christopher S. Yoo
University of Pennsylvania
July 12, 2018
Overview of Research

- Tort and products liability for CPS
- Privacy and cybersecurity regulation
  - NHTSA (autonomous vehicles)
  - HIPAA (personal health information)
  - FDA (medical devices)
Key Design Elements for Law

- Accountability-based detection
- Fusion-based detection of sensor attacks
- Bounded-time recovery
- Provenance-based forensics
- Differential privacy

- The standard for determining sufficient security
- Ways to minimize privacy liability
Standard for a Well-Designed Product

- Previous standard: consumer expectations
  - Actually reflects judicial notions of fairness
  - Risks collapsing into a perfection standard
  - Often driven by industry standards

- Emerging standard: risk-utility calculus (ALI ‘95)
  - Weighs cost-benefit tradeoffs between alternative designs
  - In some states, shifts burden of proof to manufacturer

- Current law – one third of states follows each, the other third combines the two
Scope of Duties under Tort Law

- Duty to protect against foreseeable vulnerabilities
- Duty to protect against foreseeable misuse/attacks
- Duty to warn of dangers (even if no duty to redesign)
- Duty to mitigate damage in case of an accident
- Duty to disclose later-discovered vulnerabilities
- Personal injury/damage vs. economic harm
Complex Causation

- Interactions among multiple components
- Foreseeable user misconduct
  - Failure to use safety measures
  - Aftermarket modification
- Hackers as a potential intervening cause
- Presence of learned intermediaries
- Need for forensic evidence
Other Tort Liability Issues

- Complexities from mixing CPS & non-CPS devices
- Reliance on contracts instead of general duties
- Shift from driver liability to manufacturer liability
- Role of insurance
  - Insurance may potentially allocate liability
  - But insurance cannot spread correlated risks
Federal Preemption

- **NHTSA**
  - Ambiguous scope of future preemption
  - Potential interest in preempting on security/privacy
  - Questionable capacity to regulate the details

- **FDA**
  - Express preemption for certain medical devices
  - Cumbersome nature of approval process
  - Potential for reliance on alternative compensation schemes
Implications

- Basic design: cost-benefit analysis
- Potential importance of industry standards
- Duty to anticipate foreseeable failures
- Limits to availability to validate software
  - Inherent incompleteness of validation
  - Unboundedness of state generated by the physical world
- Forensics as a potential two-edged sword
- Potential benefits from preemption
Privacy/Security for AVs

- NHTSA Federal Automated Vehicles Policy (Sept. 2016)
  - Encourages data recording/sharing (after de-identification)
  - Prioritizes privacy, cybersecurity, crashworthiness, consumer education
  - Encourages states to create “technology-neutral” competitive environments
Privacy/Security for AVs

  - Encourages cybersecurity best practices
    - Cybersecurity by design
    - Rapid detection and remediation
    - Information sharing among industry members
    - Self-audits, risk assessments, workforce education
  - Leaves privacy to FTC and Congress
Privacy/Security for AVs

- NHTSA has put V2V communication standards on the back burner
- California now allows driverless AV testing
- States will continue to experiment
Scope of HIPAA – Covered Entities

- Do not handle protected health information (PHI): no liability
- Handle limited datasets: reduced liability
  - Fewer than 18 identifiers present, not fully de-identified
  - Agreement to return/destroy data, creation of data use agreement
- Provide services to health care providers and handle PHI: full liability
- Act as business associate: full liability
HIPAA Privacy Rule

- Patient authorization for use/disclosure of PHI
- Procedures for PHI return, destruction, protection
- Minimization of PHI use
- Disclosure of PHI to HHS on request
- Process for individuals to make complaints
HIPAA Security Rule

- Develop and periodically review security measures
- Adopt policies, procedures, and a training program that address security issues, including:
  - Data transfer and disposal
  - Threat detection and containment
- Establish contingency plans (data backup, disaster recovery, emergency mode operation)
- (Also Breach Notification Rule, Unique Identifiers Rule, and Enforcement Rule)
HIPAA Enforcement

- Authority
  - HHS Office of Civil Rights (OCR)
  - State Attorneys General (2009 HITECH Act)—infrequent but possible

- HHS OCR enforcement actions
  - Initial negotiations
  - Settlements (e.g., $3.5 million for prohibited disclosures and failed risk analysis in Feb. 2018)
  - Civil money penalties (e.g., $4.3 million for encryption failures in June 2018)
Key HIPAA Design Issues

- Need for access to identifiable data
- Storage of information in patient homes
- Sharing of health information across devices
- Impact of differential privacy
- Need for processes (including training and documentation)
FDA Classification

- Class III devices include those which sustain life, are implanted, or present unreasonable risk of illness or injury

- Medical CPS will almost certainly be Class III devices—the riskiest, most-regulated class
  - Quality system
  - Pre-market approval
  - Post-market regulation
FDA Quality System

- Start design control during development; continue indefinitely
- Develop software validation and verification system
  - Verify output conforms to input
  - Validate that device meets intended needs
FDA Quality System

- Submit complete description of design controls to be eligible for pre-market approval
  - Use of consultants/subcontractors
  - Device and clinical evaluations
  - Device reliability, durability, serviceability
  - Cybersecurity
  - Risk management
FDA Pre-Market Approval

- Requires significant documentation, including clinical trials
- Requires a risk analysis report that
  - Identifies threats and vulnerabilities
  - Determines the likelihood of exploitation
  - Determines strategies for cybersecurity
- Recommends additional document describing cybersecurity software updates and patches
FDA Post-Market Regulation

- Adverse event reporting
- Yearly post-approval reporting on:
  - System updates
  - Defects and cybersecurity issues
- Surveillance reporting that addresses questions from clinical trials, depending on pre-market approval results
FDA Device Modification

- Pre-market approval amendments required for:
  - Different intended uses
  - New patient populations
  - New generations of a device

- Post-approval supplements required for:
  - Changes in performance or design specifications
  - Changes that may affect safety of efficacy
FDA Enforcement

- **Authority:** FDA Center for Devices and Radiological Health Office of Compliance

- **Penalties**
  - Warning letters, injunctions
  - Criminal prosecutions
    - Misdemeanors for first offenses; felonies for additional offenses
    - Fines up to $500,000; imprisonment up to a year
    - E.g., 46 months in prison, forfeiture of $1.2 million in profits
Thank you!