Privacy Regulation in the US and the EU

Jan. 28, 2019

Overview

- Privacy Principles
  - Fair Information Practices (FIPPs)
  - Privacy by Design
  - Contextual Integrity
- Comparison of US and EU privacy laws and regulation
- Civil Society Responses
- Privacy by Design

Privacy Principles

- Fair Information Principles (FIPPs)
  - Transparency
  - Individual participation
  - Purpose specification
  - Data minimization
  - Use limitation
  - Data quality and integrity
  - Data security
  - Accountability and Auditing

Privacy Principles

- Seven Foundational Principles of Privacy by Design (Cavoukian 2009)
  - Proactive not reactive; preventative not remedial
  - Privacy as the default setting
  - Privacy embedded into design
  - Full functionality—positive-sum, not zero-sum
  - End-to-end security—full lifecycle protection
  - Visibility and transparency
  - Respect for user privacy

Privacy Principles

- Contextual Integrity: Privacy in Context (Nissenbaum 2010)
- Contexts:
  - Data subject
  - Sender of the data
  - Recipient of the data
  - Information type
  - Transmission principle

EU vs. US

	EU	US
Regulatory Source	Supranational and national	Federal and state
Major Regulatory Authority(ies)	European Commission	Depends on industry or sector Federal Trade Commission (FTC) for consumer privacy
Regulatory Approach	Precautionary	Reactionary
Organizational Coverage	All organizations that deal with the data of EU citizens	Mainly public-sector plus some specific private industry sectors
Major EU-wide/ Federal Privacy Laws	European Convention on Human Rights EU Charter of Fundamental Rights 1995 EU Data Protection Directive (replaced by GDPR) 2002 Privacy and Electronic Communications Directive (ePrivacy Directive) 2018 General Data Protection Regulation (GDPR) ePrivacy Regulation (proposed)	4th Amendment Federal Privacy Act of 1974 Federal Trade Commission Act of 1914, Section 5 Electronic Communications Privacy Act of 1986 (ECPA) Title II of ECPA: Stored Communications Act Computer Fraud and Abuse Act of 1986

EU vs. US

		EU	US
Smart Meters	Major regulatory authority(ies)	European Commission	State-level Public Utility Commissions National Institute of Standards and Technology (NIST)
	Major EU-wide/Federal Privacy Laws	GDPR 2006 Energy Service Directive 2009 Electricity Directive 2012 Energy Efficiency Directive 2016 Clean Energy Package	The Energy Independence and Security Act of 2007 NIST has developed some guidelines
CAVs	Major regulatory authority(ies)	European Commission	National Highway Traffic Safety Administration (NHTSA) Federal Trade Commission (FTC)
	Major EU-wide/Federal Privacy Laws	GDPR	Driver's Privacy Protection Act of 2015 Not yet well developed; have suggested guidelines
UAVs	Major regulatory authority(ies)	European Commission European Aviation Safety Agency (EASA)	Federal Aviation Administration (FAA)
	Major EU-wide/Federal Privacy Laws	GDPR 2008 Basic Regulation Proposed 2018 EASA regulation	Fourth Amendment Not yet well developed; have suggested guidelines

GDPR vs. U.S. Data Protection

- Wider scope
  - Data of all EU citizens
- More specific data protection requirements
  - Right of access
  - Right of data rectification
  - Right to erasure (right to be forgotten)
  - Right to restriction of processing
  - Right to data portability
  - Right to object
- Harsher penalties for noncompliance
  - Fine of up to €20 million or 4% of global annual turnover

Civil Society Responses

Ralph Nader:

“Pushing the driver out of any kind of control of the vehicle with **software that is fallible** — how many times has your computer failed? — and that is **extremely vulnerable to hacking for which there’s no known solutions**, is going impede any kind of substantial, quantifiable vehicle fleet that’s driverless.”

Civil Society Responses

Electronic Privacy Information Center (EPIC):

"NHTSA should remove references to 'data privacy notices/agreements' in order to restore substantive rights to consumers and limit carmakers' ability to hide behind **incomprehensible privacy policies**. Most importantly, NHTSA should promulgate mandatory, legally enforceable privacy rules for automated vehicle manufacturers. **Voluntary codes of conduct and industry self-regulation simply cannot provide realistic privacy protections when they are not supported by enforceable legal standards**."

Privacy by Design Ideas for Smart Meters

- Anonymization
- Cryptographic computation/Encryption
- Perturbation
- Battery approaches
- Aggregation
- Sampling interval