Privacy by Design
Principles vs. Reality

Peter A. Kiss SFC USA (Ret)

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

Eric Schmidt, Google CEO, CNBC interview, December 3, 2009

"The makers of our Constitution … conferred against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."

Louis Dembitz Brandeis, US Supreme Court Associate Justice, *Olmstead v. United States* (1928)

Workplace Privacy
Relative value

- balanced against employer's interests
  - full day's work for full day's pay
  - professional, physical & health qualifications
  - conduct on & off the job
- balanced against statutory requirements
  - qualifications
  - tax information
- balanced against public interest
  - public health
  - positive/negative influence

Privacy Violations

- reasonable expectation of privacy
- implied/expressed consent
- intentional and inadvertent violations
  - data loss through negligence
  - data loss through hacking
  - data sharing with third parties
- both at work and elsewhere

Privacy Enhancing Technologies (PET)

- technology-based solutions
- applications or tools with discrete goals
- address single dimension of privacy
  - anonymity
  - confidentiality
  - control over personal information
- bolt-ons to existing systems

Privacy by Design

- "total design" – information eco-system
- integrate privacy into the design of
  - technology
  - operational systems
  - work processes
  - management structures
  - physical spaces
  - networked infrastructure
- far broader than workplace privacy
- does not cover all workplace privacy issues

Possible Areas of Application

- access authorization systems
- pay as you drive
- pay per view
- smart electricity metering
- health insurance cards
- public transport payment

Principles

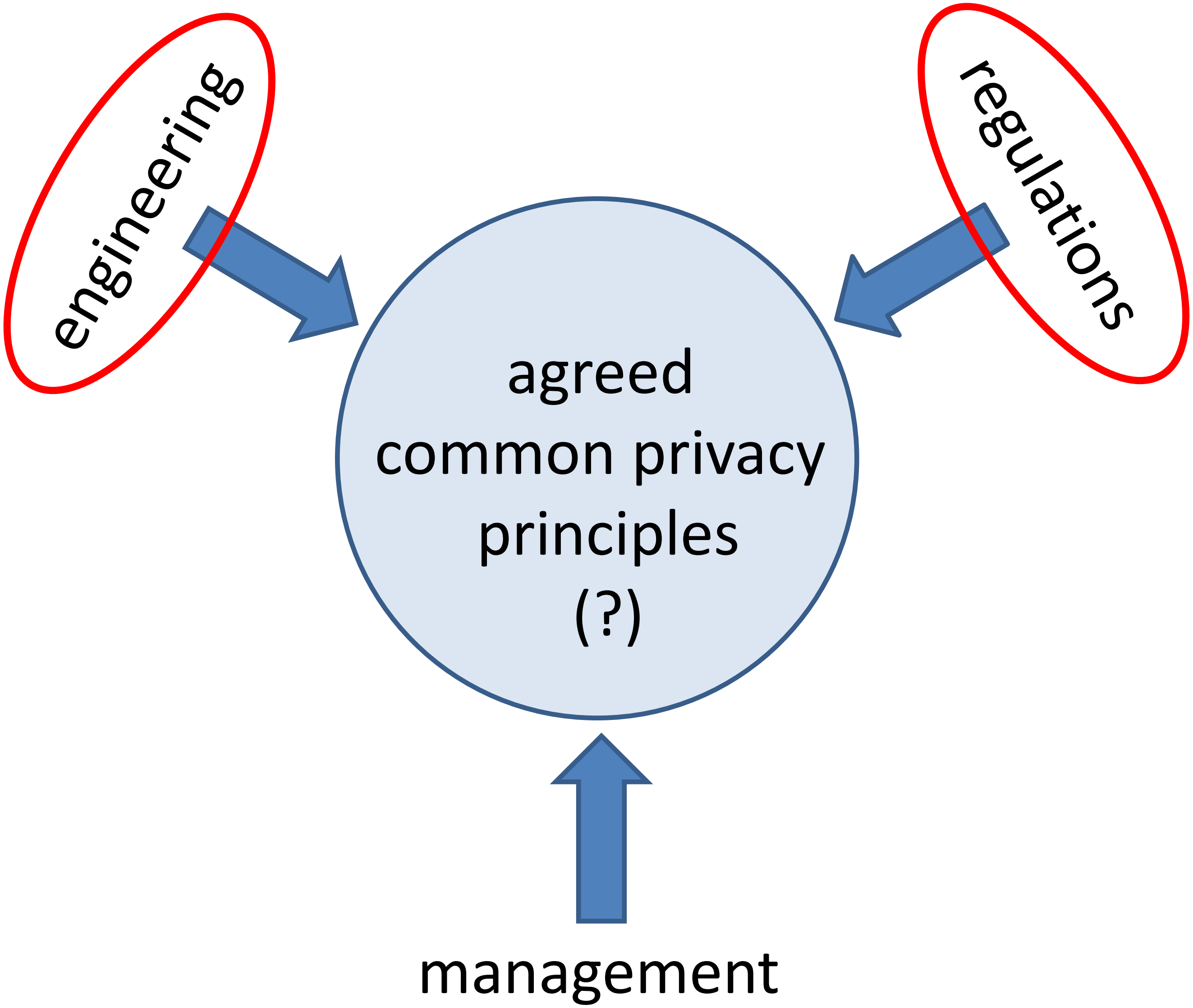
1. Proactive and preventative
2. Privacy the default setting in IT systems
3. Privacy embedded into IT system design and architecture
4. Positive-sum rather than zero-sum approach
5. Privacy embedded from end to end within IT security systems
6. Visibility and transparency
7. Respect for user privacy

Privacy by Design – Concept so Far

- no standards or benchmarks
- few true models (SDG&E)
- some agreement on challenges
- no common solutions
- may turn into gimmick

situation similar to information security in 1980's

Three Factors – Two Drivers



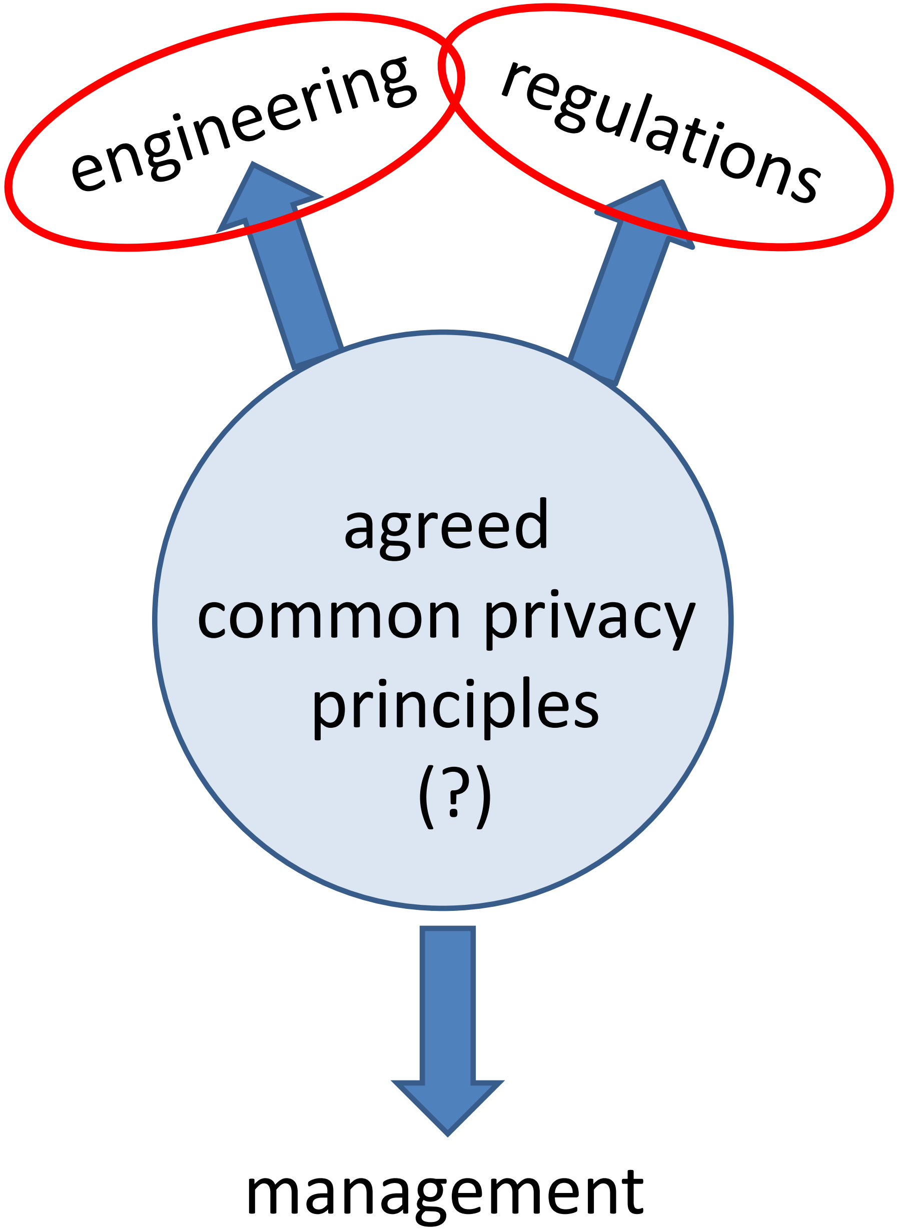
engineering

regulations

agreed common privacy principles (?)

management

Three Factors – Two Drivers



Regulation

- cognitive dissonance
- little or no guidance to engineering
- little or no concern for business efficiency
- potential to become rigid "letter-of-the-law"
- potential to set global standards & benchmarks

Engineering

- focus on specific challenges
- potential to become fragmented
- isolation from decisonmaking
- isolation from business model
- no common language with management

Management

- no clear guidance on what is expected
- clearly identifiable loss of revenue to PbD
- clearly identifiable costs to PbD
- no clear benefits to adopting PbD principles
- no clear risk in NOT adopting PbD principles
- engineers will take care of it
- no common language with engineers

How can we Make it Happen?

guidance – incentives – coercion – control

- apply lessons of "security by design"
- engage executive management
  - demonstrate benefits
  - create common language
- develop practical privacy standards
  - privacy metadata
  - data minimisation
  - information security
- transparency
  - Privacy Impact Assessment
  - Subject Access Request

Thank you for your attention!