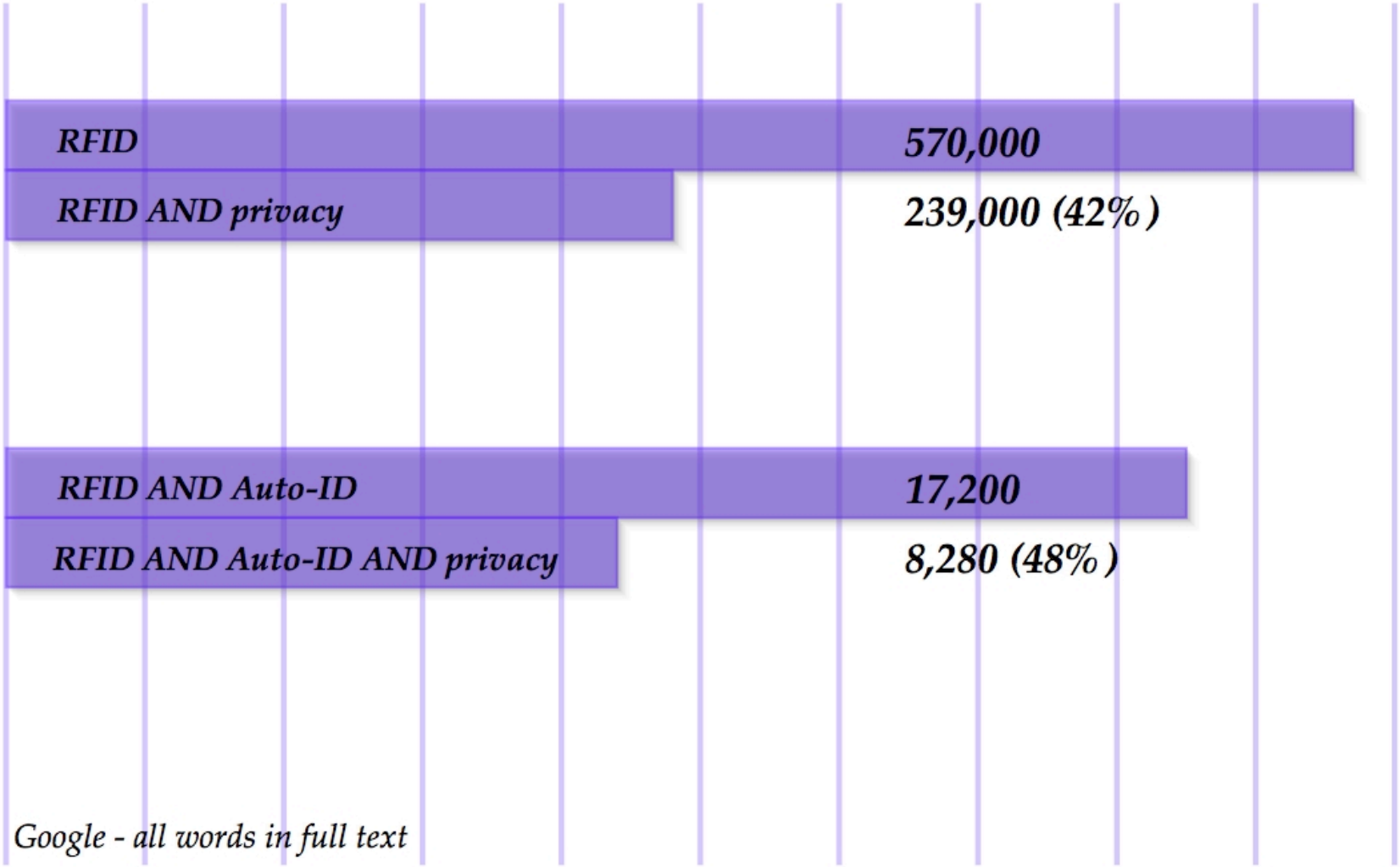
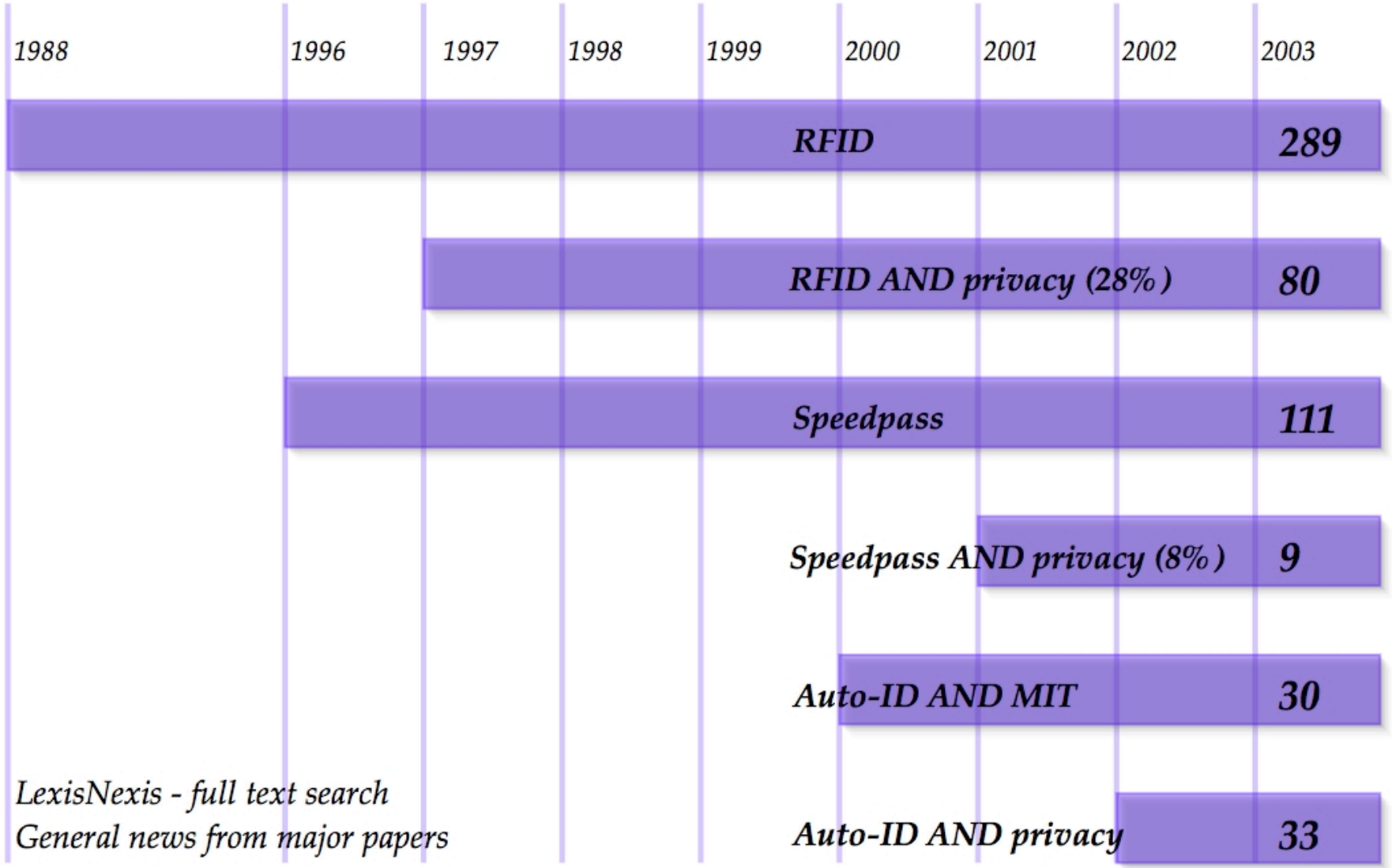
Privacy and Security in the EPC Network

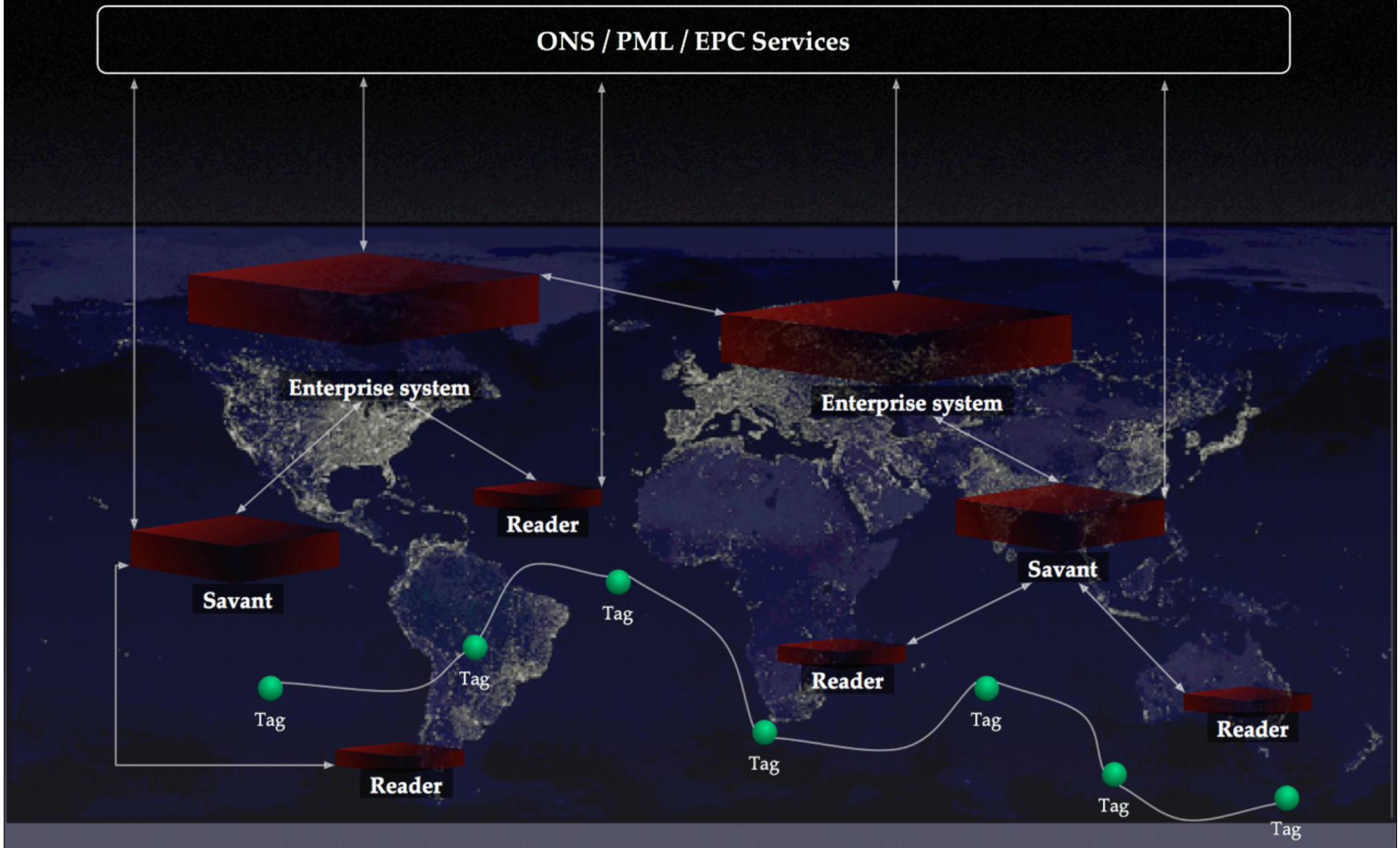
Ravi Pappu
Founding Partner
ThingMagic LLC

Privacy in the EPC Network is a growing and valid concern

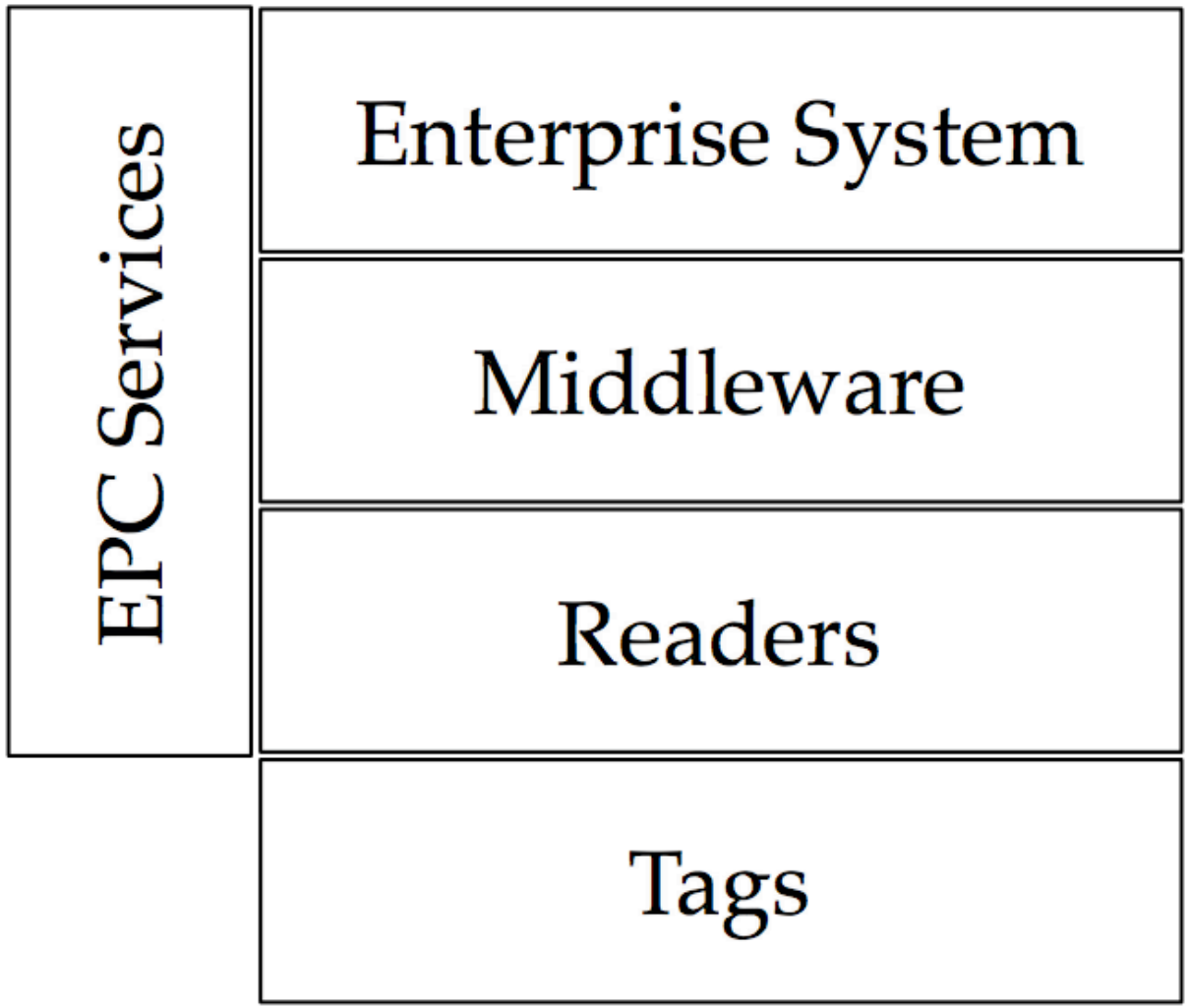

RFID
570,000
RFID AND privacy
239,000 (42%)
RFID AND Auto-ID
17,200
RFID AND Auto-ID AND privacy
8,280 (48%)
Google - all words in full text


1988
1996
1997
1998
1999
2000
2001
2002
2003
RFID
289
RFID AND privacy (28%)
80
Speedpass
111
Speedpass AND privacy (8%)
9
Auto-ID AND MIT
30
Auto-ID AND privacy
33
LexisNexis - full text search
General news from major papers

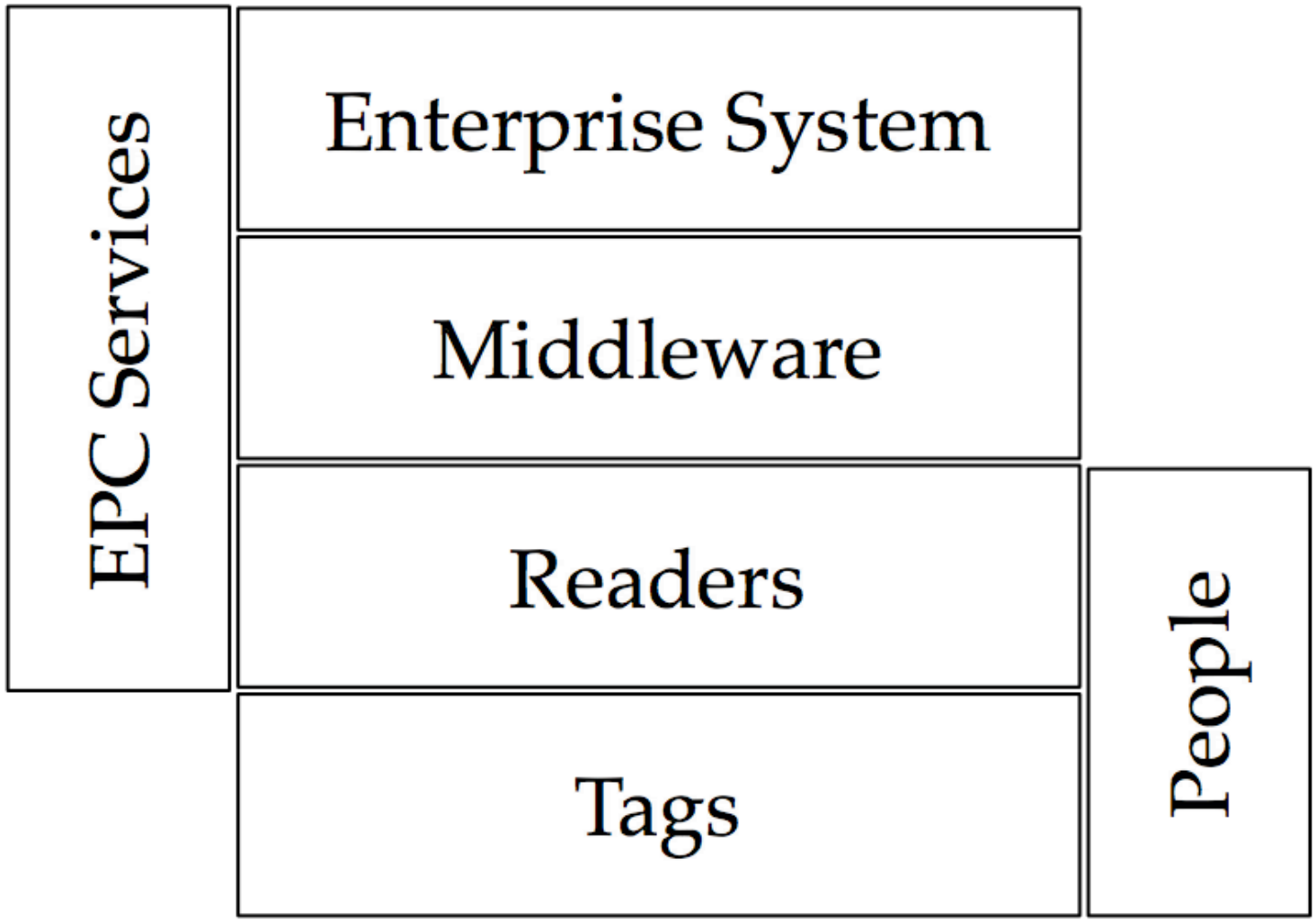
The EPC Network



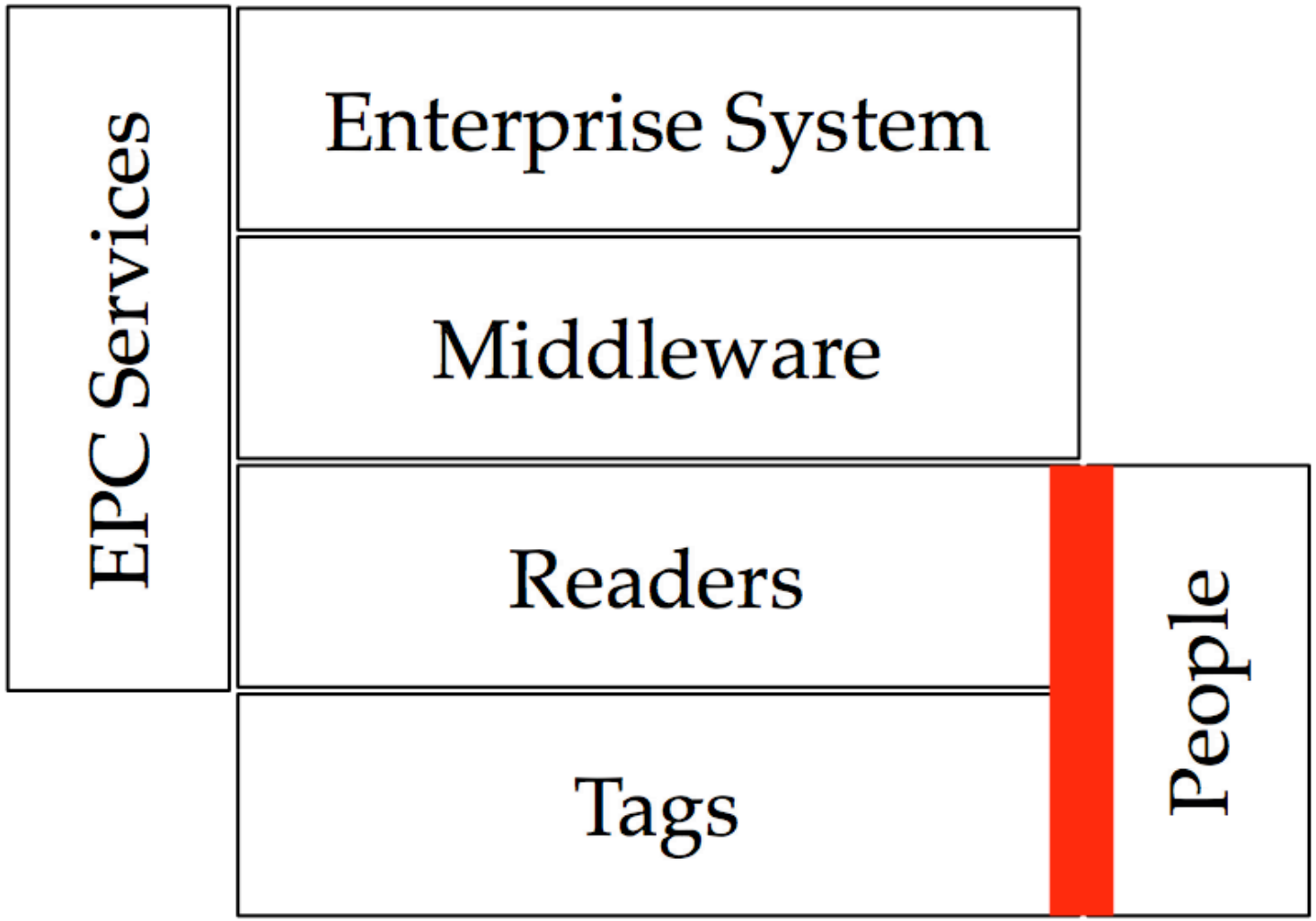
The EPC Network



The EPC Network



The EPC Network



What's different about the EPC Network?

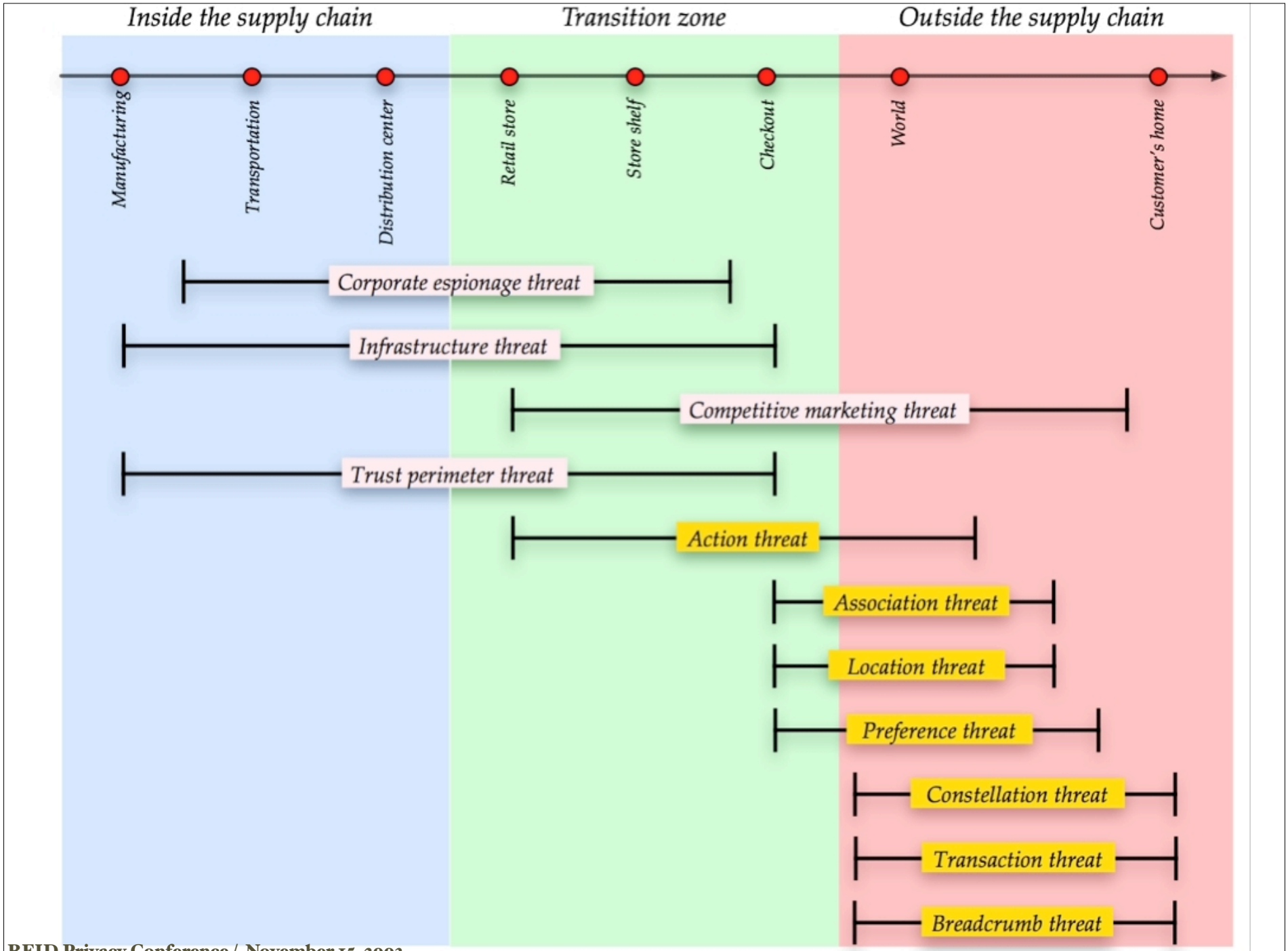
- Promise of *imminent*, *widespread* deployment
- *Unique* identity
- *Open* system - need to *trust* multiple entities with data
- Customers perceive *no choice* in adoption
- Customer benefit not articulated *clearly*

Threats to data security

- *Corporate espionage threat* - espionage via supply chain dynamics
- *Trust perimeter threat* - broadening of perimeter because of data sharing via networks
- *Competitive marketing threat* - customers are revealed to competitors
- *Infrastructure threat* - DOS, jamming, physical damage, counterfeit tags....

Threats to personal privacy

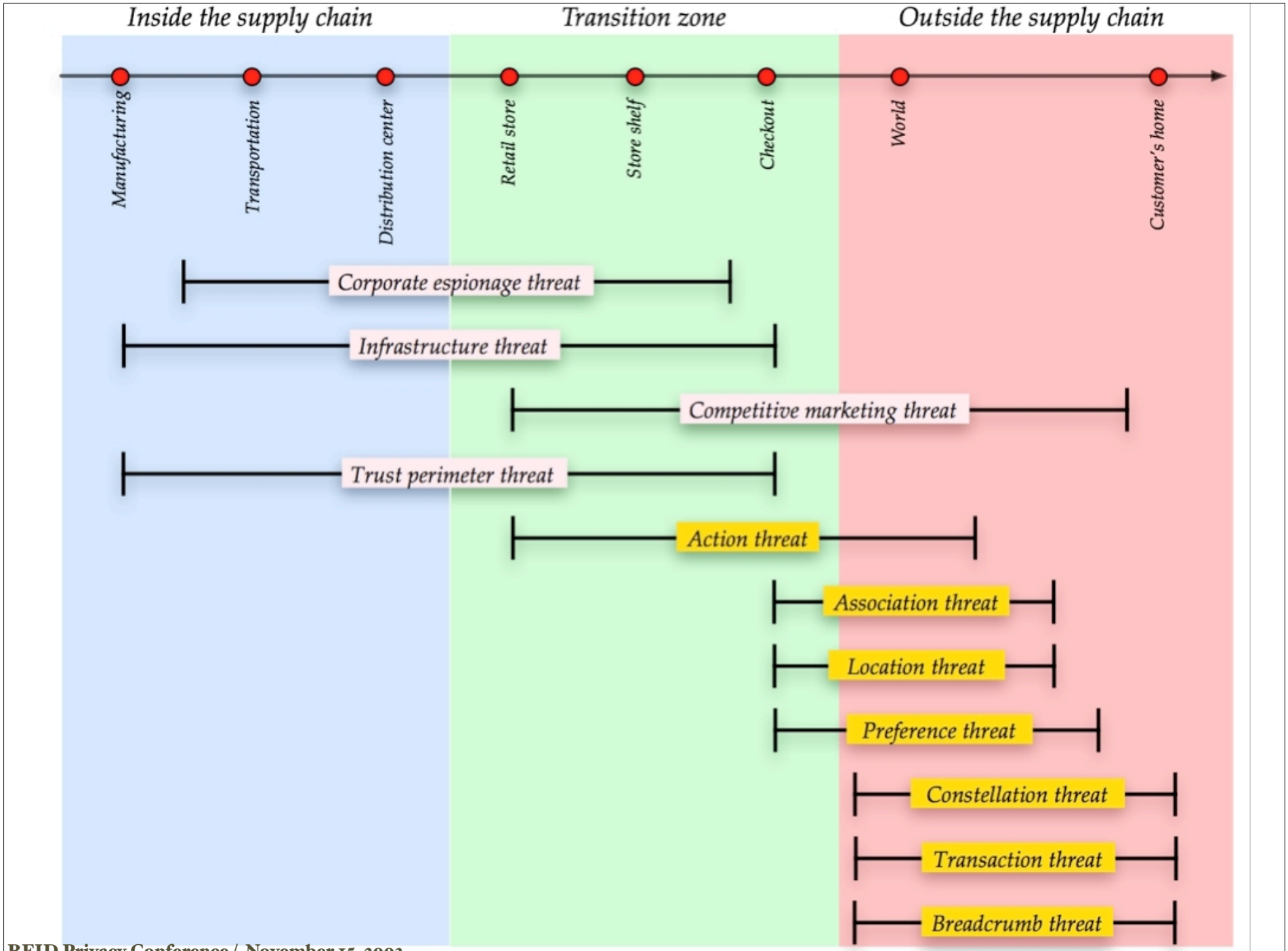
- *Action threat* - determining action based on tags
- *Association threat* - associating personal identity with tags
- *Location threat* - determining tag location
- *Preference threat* - revealing personal preferences
- *Constellation threat* - RFID "shadow"
- *Transaction threat* - determining transactional information
- *Breadcrumb threat* - No way of dissociating data from identity

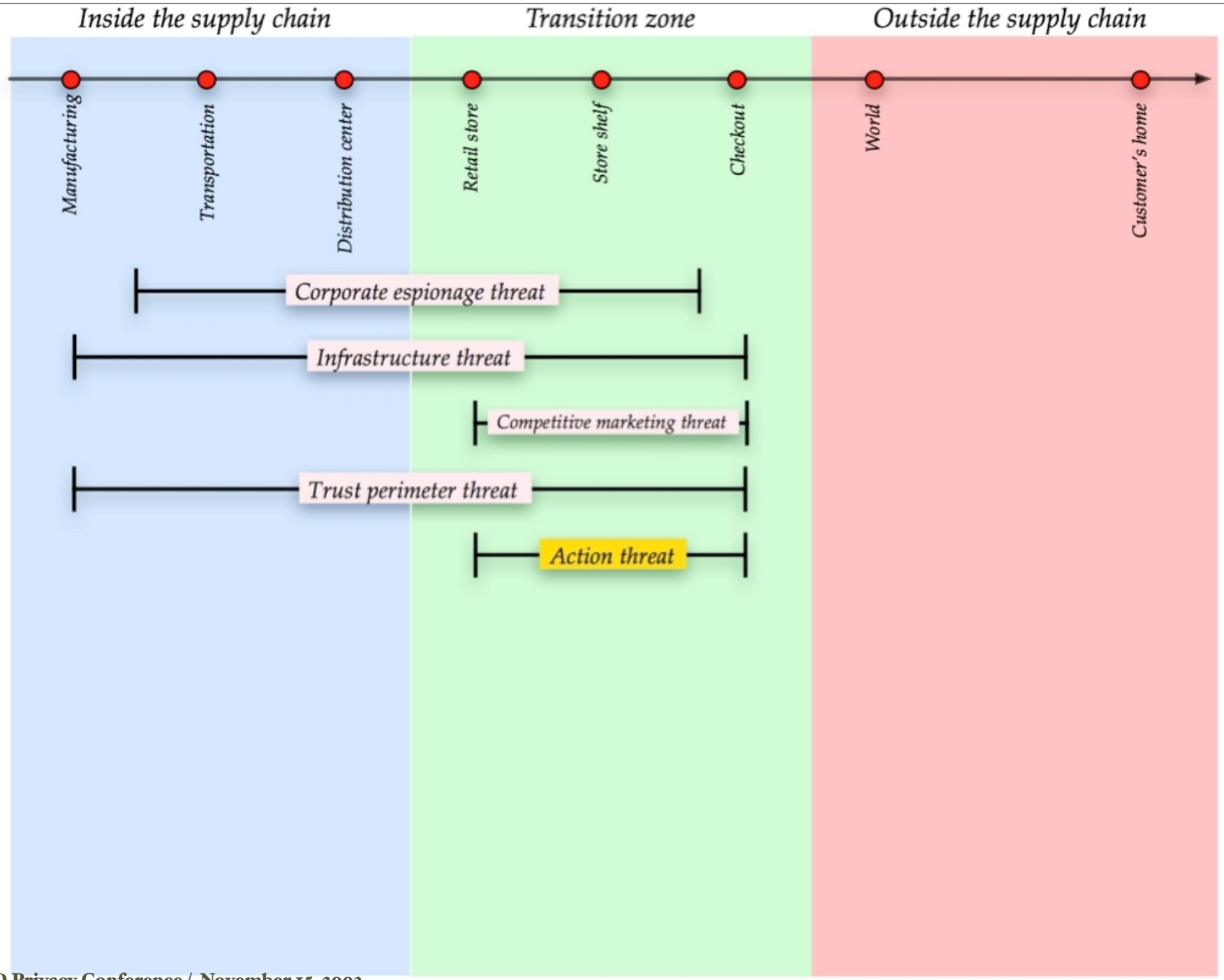

Inside the supply chain
Transition zone
Outside the supply chain
Manufacturing
Transportation
Distribution center
Retail store
Store shelf
Checkout
World
Customer's home
Corporate espionage threat
Infrastructure threat
Competitive marketing threat
Trust perimeter threat
Action threat
Association threat
Location threat
Preference threat
Constellation threat
Transaction threat
Breadcrumb threat

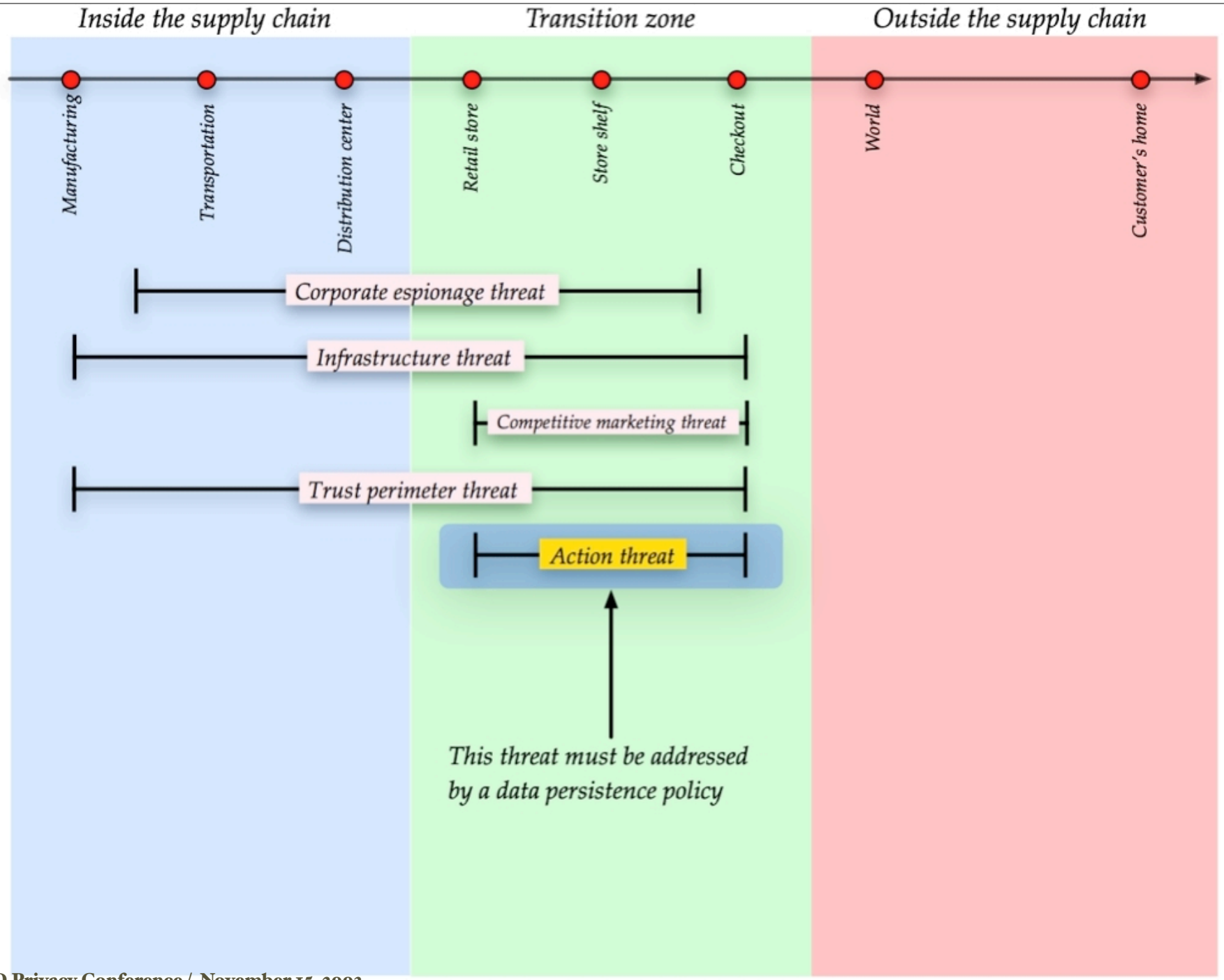
Consumers and companies have a *shared* interest in secure RFID systems

The *kill* command

- "This is kill in a Biblical sense" - *Sanjay Sarma*
- Implemented in all EPC air protocols
- Password required to kill tags
  - EPC Class 0 - 24 bits; EPC Class 1 - 8 bits; HF EPC - 24 bits
- Reader and authentication infrastructure being designed


Inside the supply chain
Transition zone
Outside the supply chain
Manufacturing
Transportation
Distribution center
Retail store
Store shelf
Checkout
World
Customer's home
Corporate espionage threat
Infrastructure threat
Competitive marketing threat
Trust perimeter threat
Action threat
Association threat
Location threat
Preference threat
Constellation threat
Transaction threat
Breadcrumb threat


Inside the supply chain
Transition zone
Outside the supply chain
Manufacturing
Transportation
Distribution center
Retail store
Store shelf
Checkout
World
Customer's home
Corporate espionage threat
Infrastructure threat
Competitive marketing threat
Trust perimeter threat
Action threat

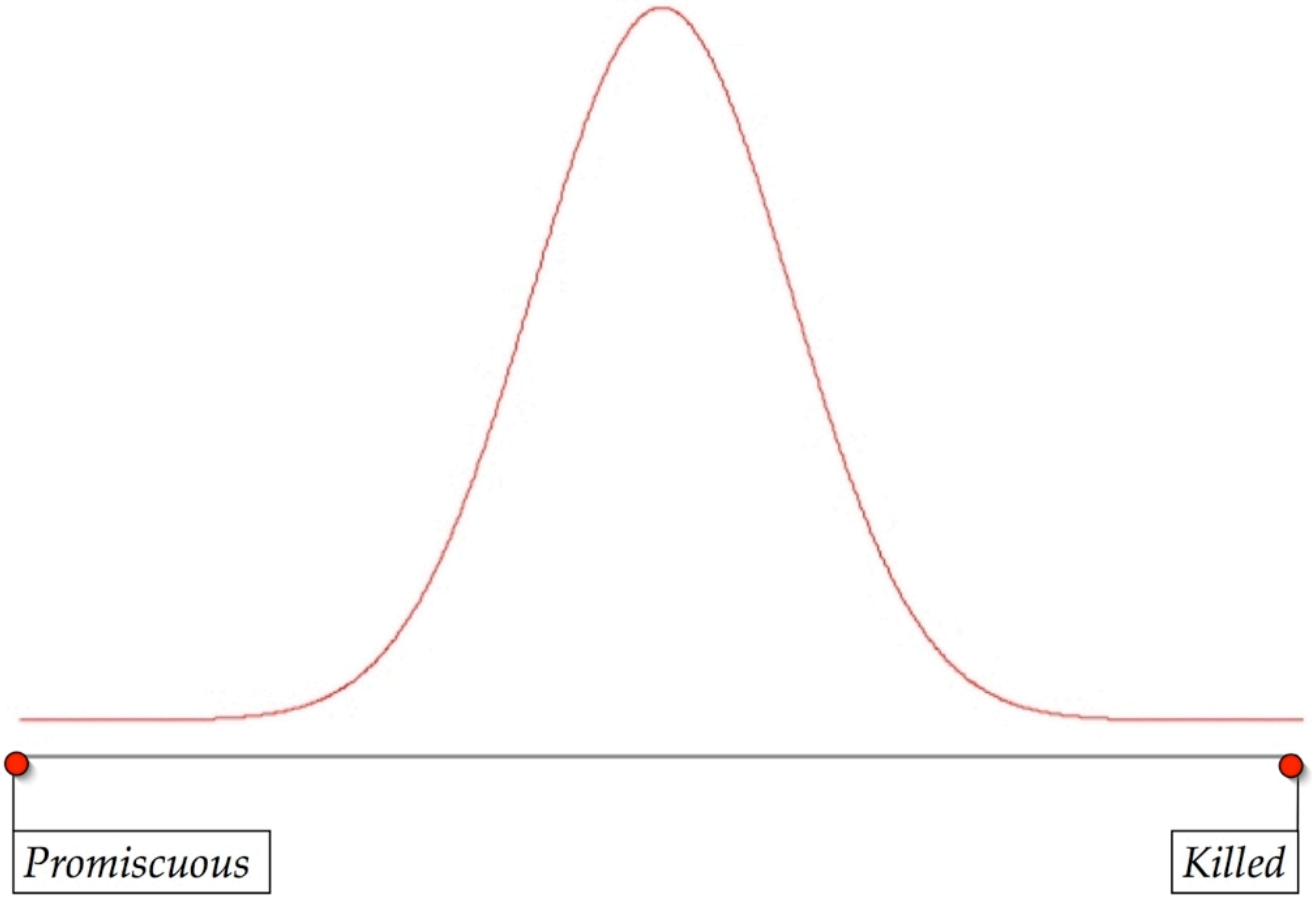

Inside the supply chain
Transition zone
Outside the supply chain
Manufacturing
Transportation
Distribution center
Retail store
Store shelf
Checkout
World
Customer's home
Corporate espionage threat
Infrastructure threat
Competitive marketing threat
Trust perimeter threat
Action threat
This threat must be addressed by a data persistence policy

Assertion

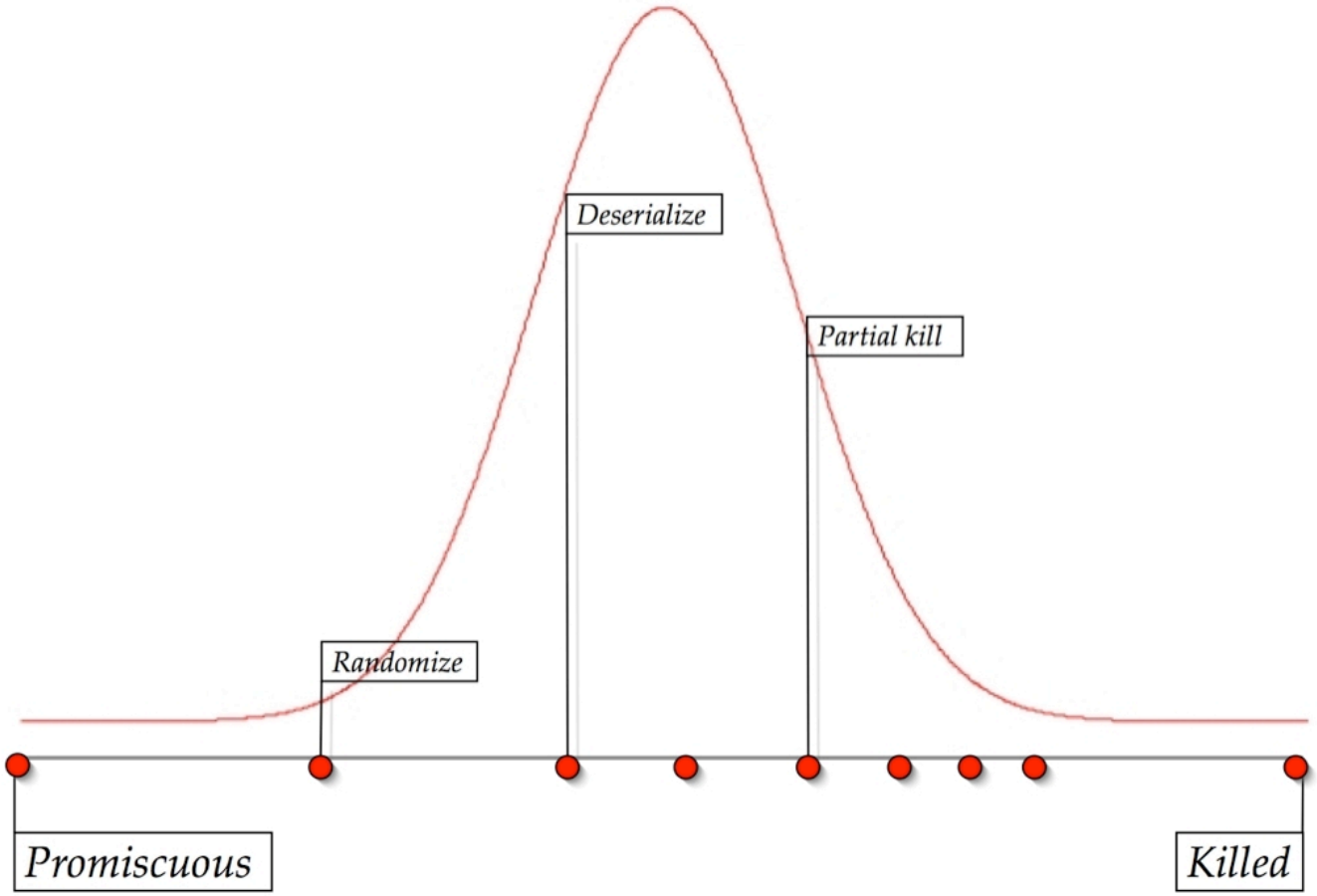
Personal privacy concerns can be made vanishingly small by

- Adopting a data persistence policy in the transition zone
- Killing tags at point of sale

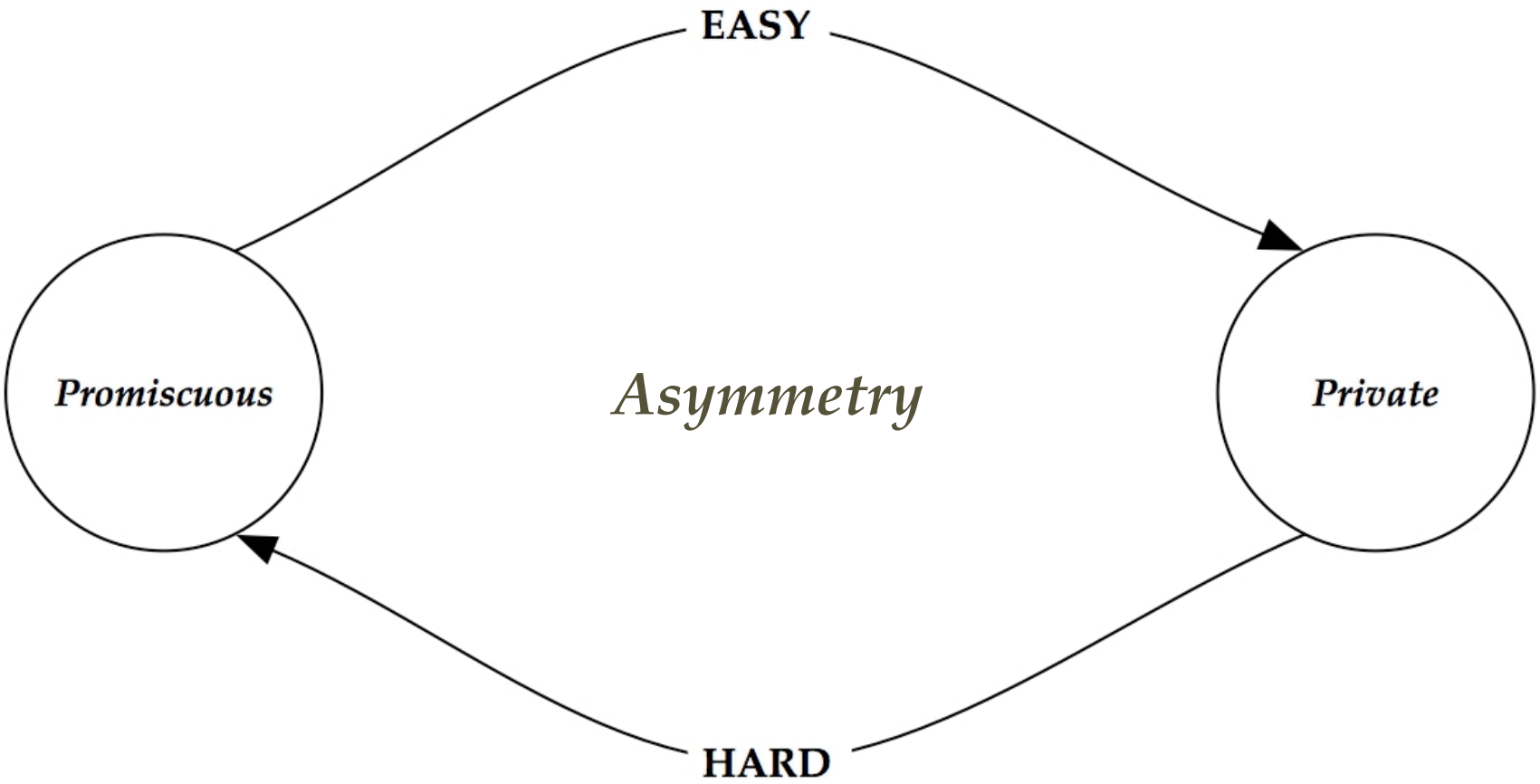
Spectrum of privacy options



Spectrum of privacy options



The philosophy of RFID privacy



Ongoing RFID privacy research

- Dual channel access + ID re-encryption
- Hash locking + silent tree walking
- Blocker tags
- Pseudonyms

Strong interest in academic research community

Short & long term challenges

- *Tags* - develop efficient implementations of *cryptographic primitives on tags*
- *RF protocols* - *evolve protocols* to leak as little information as possible about tag identity
- *Readers* - build readers with *reliable kill capability* and the ability to incorporate *evolving privacy and security policies*
- *System design* - reliable *security and authentication mechanisms*, secure databases...

PSAG Mission

- Assess threats to privacy and security stemming from RF protocols
- Promote mechanisms of maximizing privacy within the context of existing system
- Define next-generation privacy protection mechanisms in collaboration with other action groups in EPC ecosystem

Messages

- Privacy protection must continue to be *embedded into the DNA* of the EPC Network. The kill command is a good start.
- Consumers and companies have a shared interest in secure RFID systems
- EPC systems must be designed to accommodate evolving privacy and security policies

Questions?

Ravi Pappu

ravi@thingmagic.com