Physical Access Control

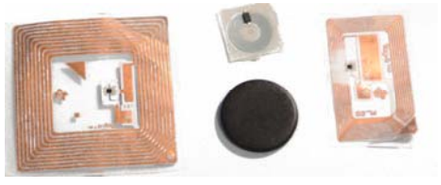
Information Disclosure in a Community-Oriented RFID Deployment

Travis Kriplean
Computer Science & Engineering
University of Washington

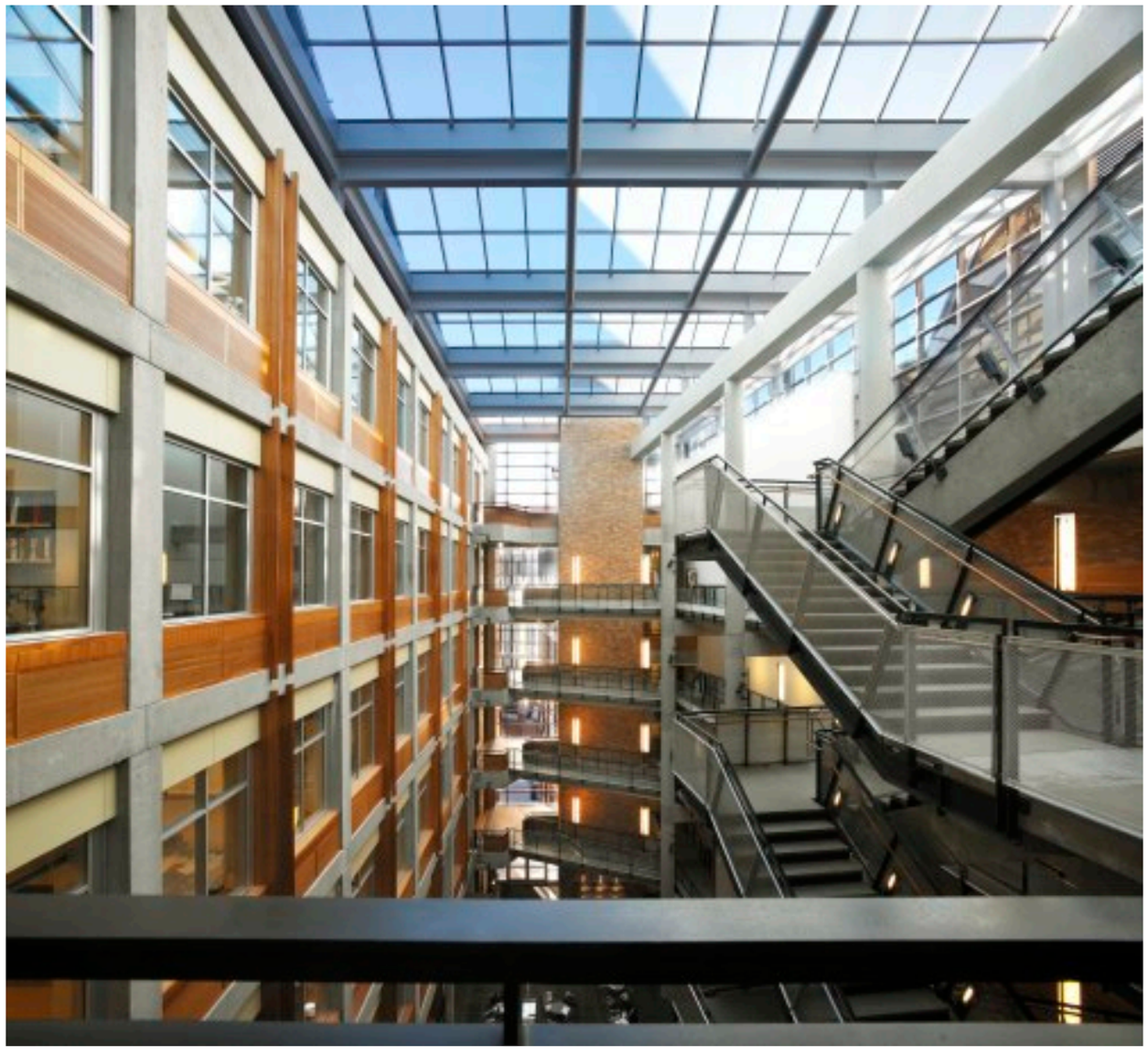
The RFID Ecosystem

- RFID allows tracking of tagged objects
  - tags and readers/antennas
  - readers communicate with a central database

RFID tags



RFID antenna

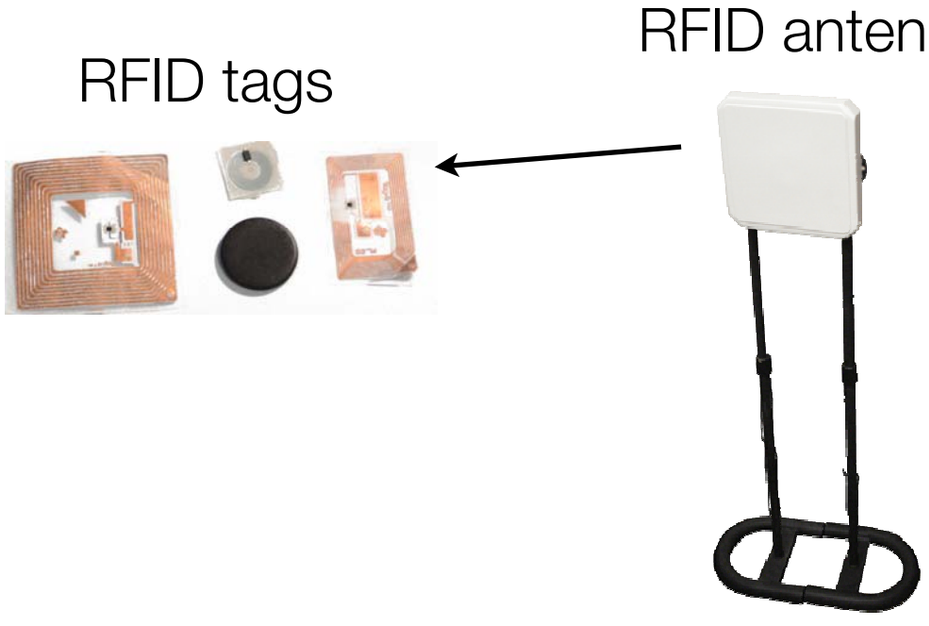


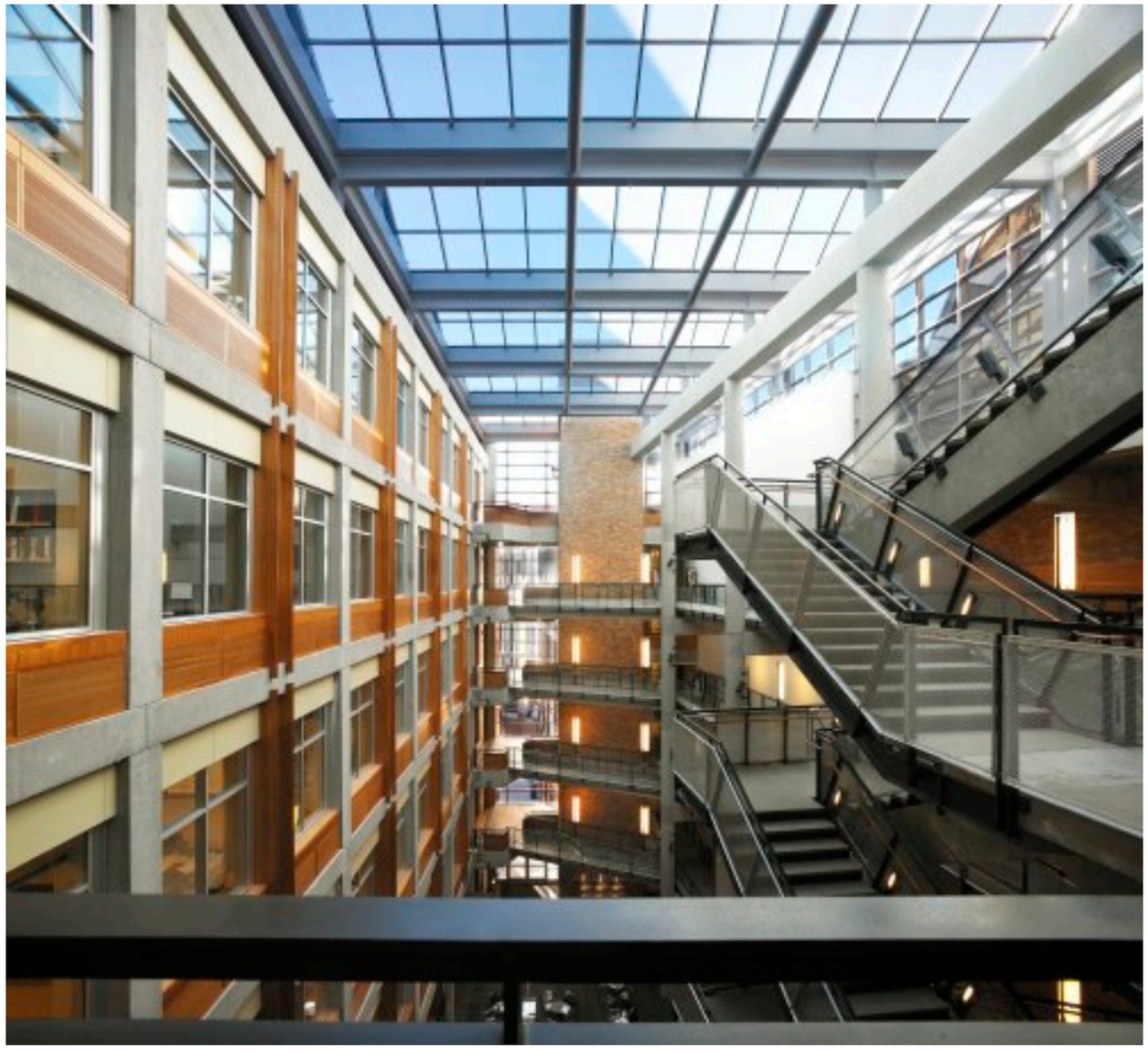
Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu

2

The RFID Ecosystem

- RFID allows tracking of tagged objects
  - tags and readers/antennas
  - readers communicate with a central database



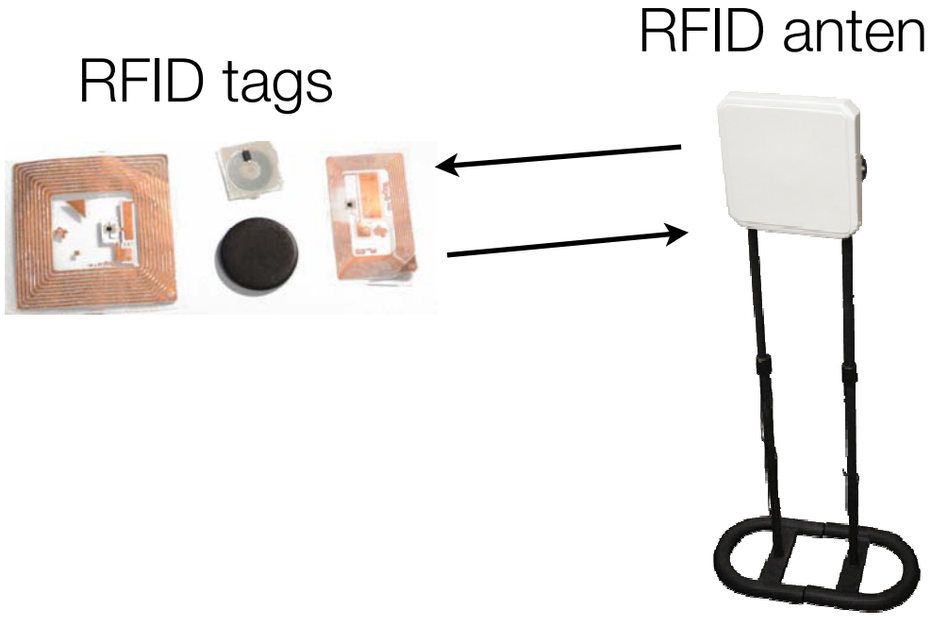


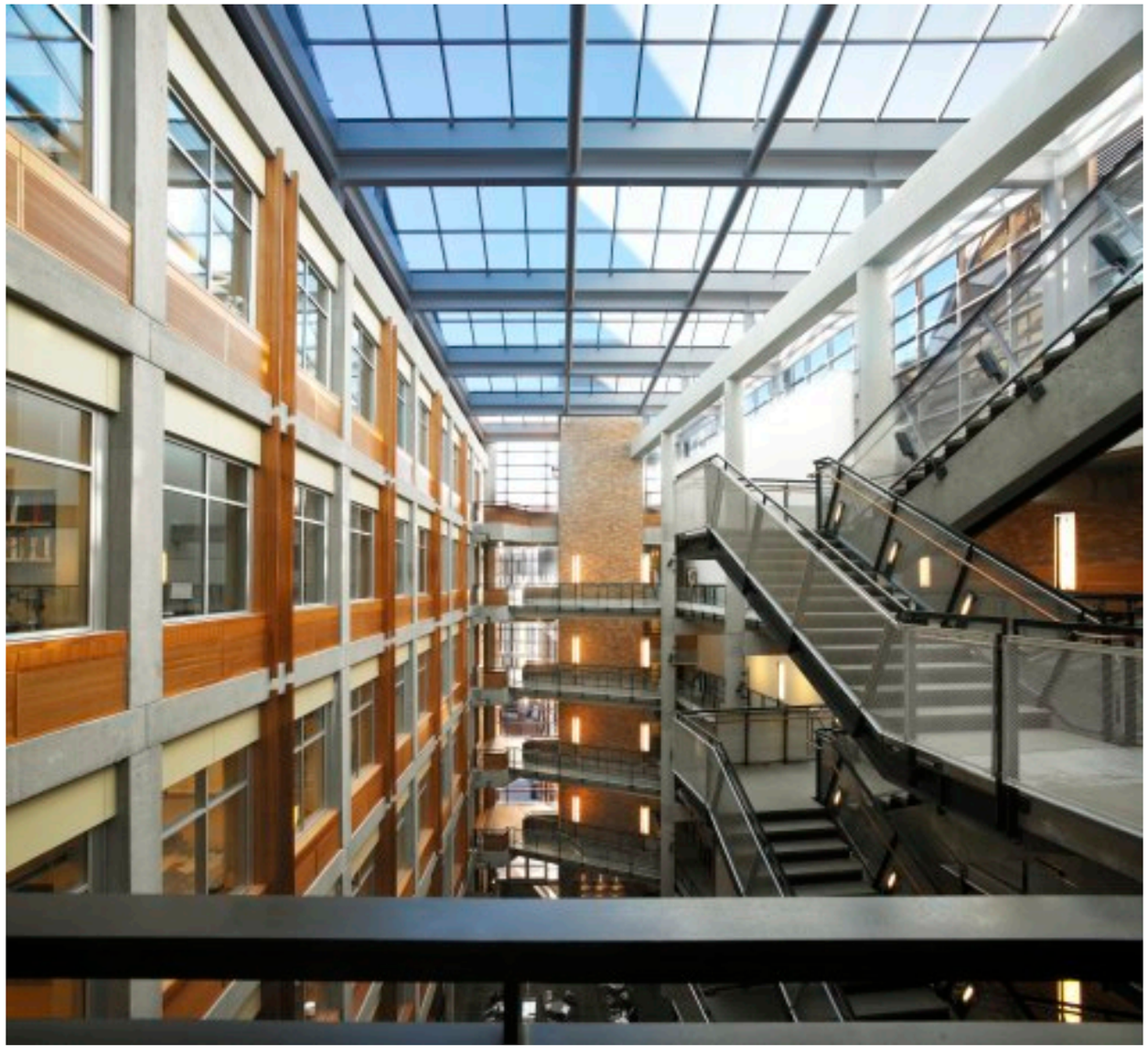
Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu

2

The RFID Ecosystem

- RFID allows tracking of tagged objects
  - tags and readers/antennas
  - readers communicate with a central database



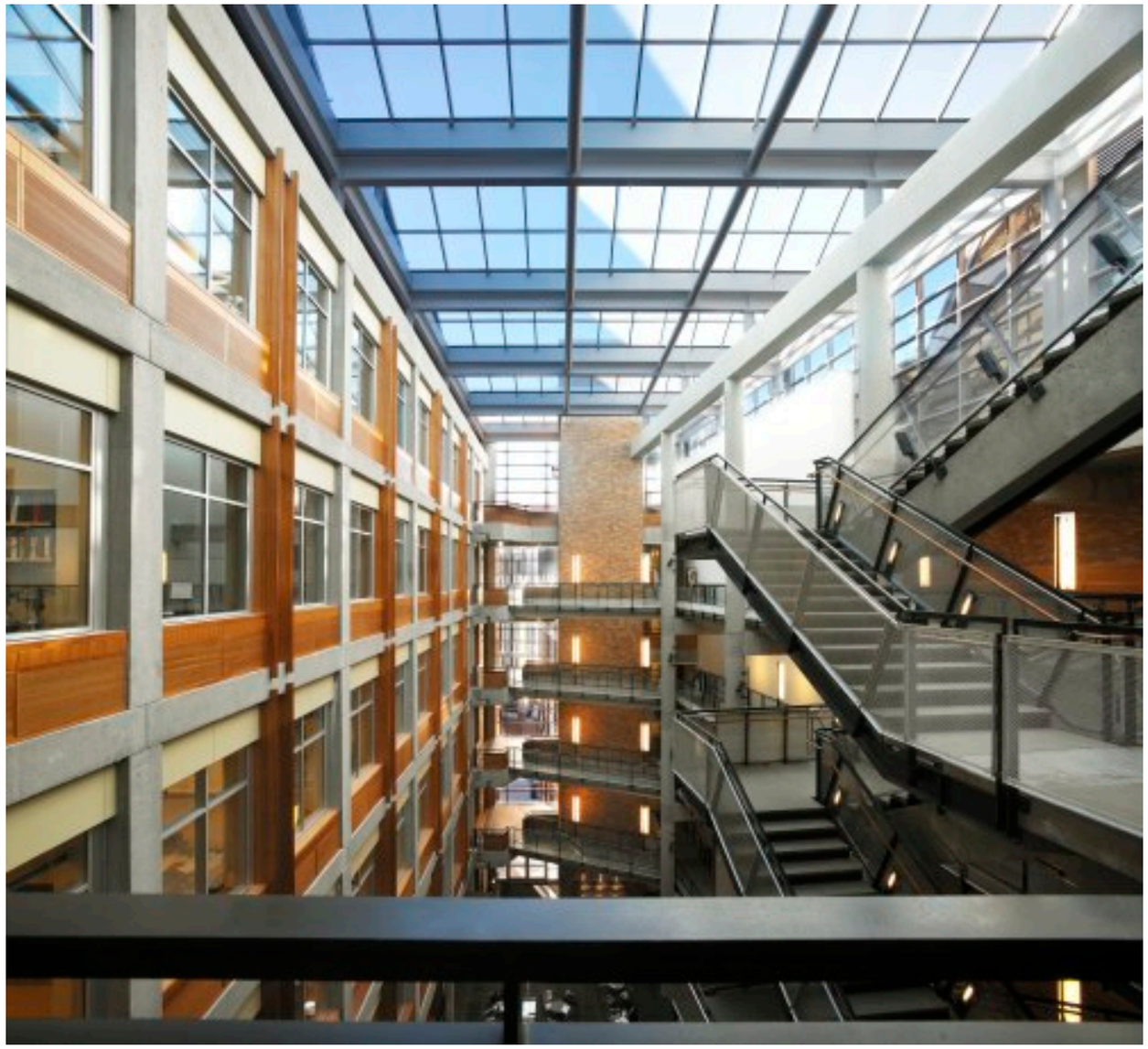


Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu

2

The RFID Ecosystem

- a building-wide RFID infrastructure
  - 300 RFID reader antennas
  - people carry personal tags
  - hundreds of tagged objects
- long-term research test bed

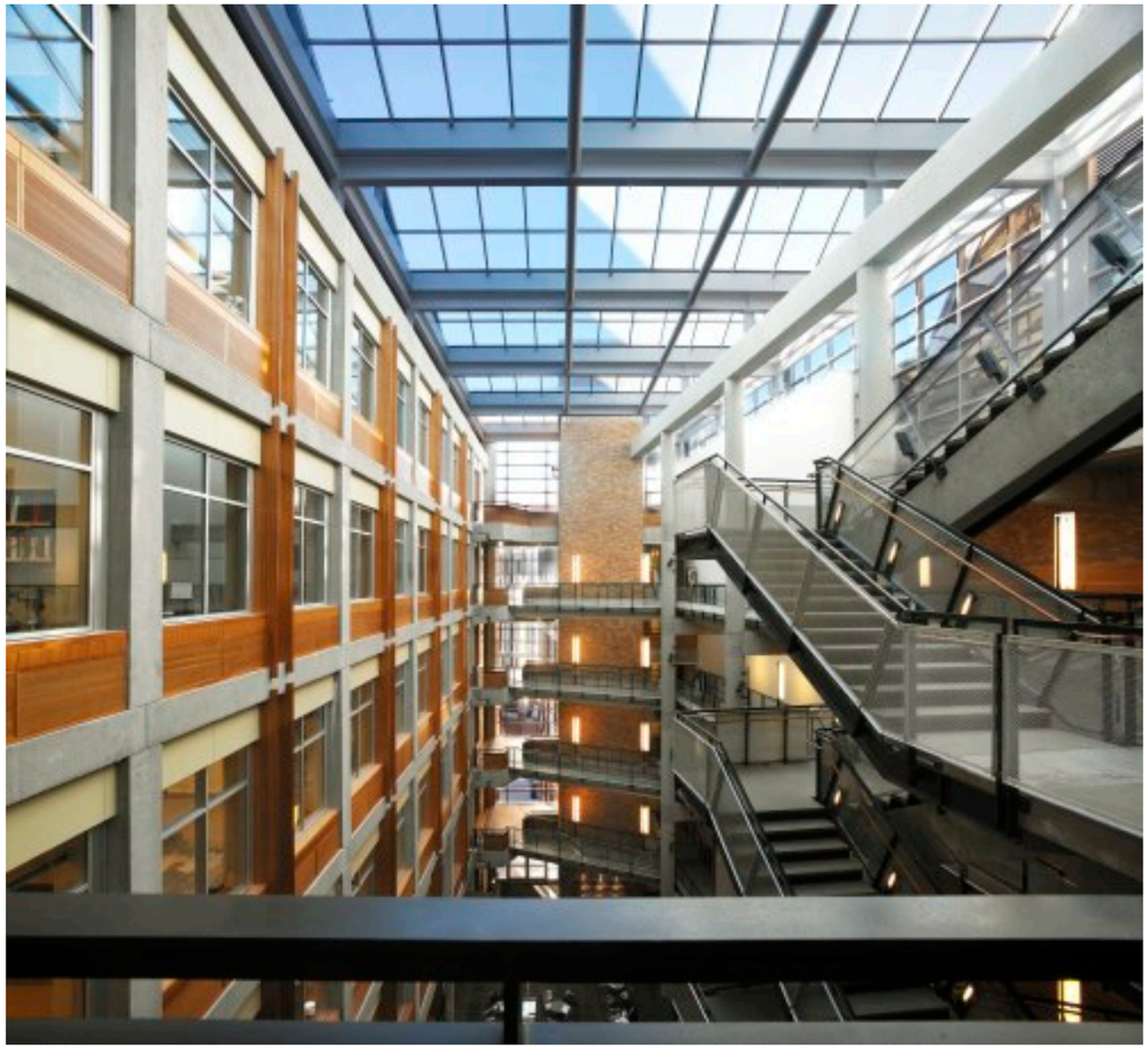


Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu

3

The RFID Ecosystem

- create information-rich environments that empower people
- allows applications such as an object or friend finder, personal reminders, and event notification
- complex social space
- useful applications require information to be disseminated
- information is actionable will likely impact social dynamics



Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu

4

A pervasive dilemma...privacy vs. utility

5

A pervasive dilemma...privacy vs. utility

divulge no information

perfect privacy, no utility

5

A pervasive dilemma...privacy vs. utility

divulge no information

perfect privacy, no utility

all phenomena recorded, indexed, and shared

no privacy, full utility

5

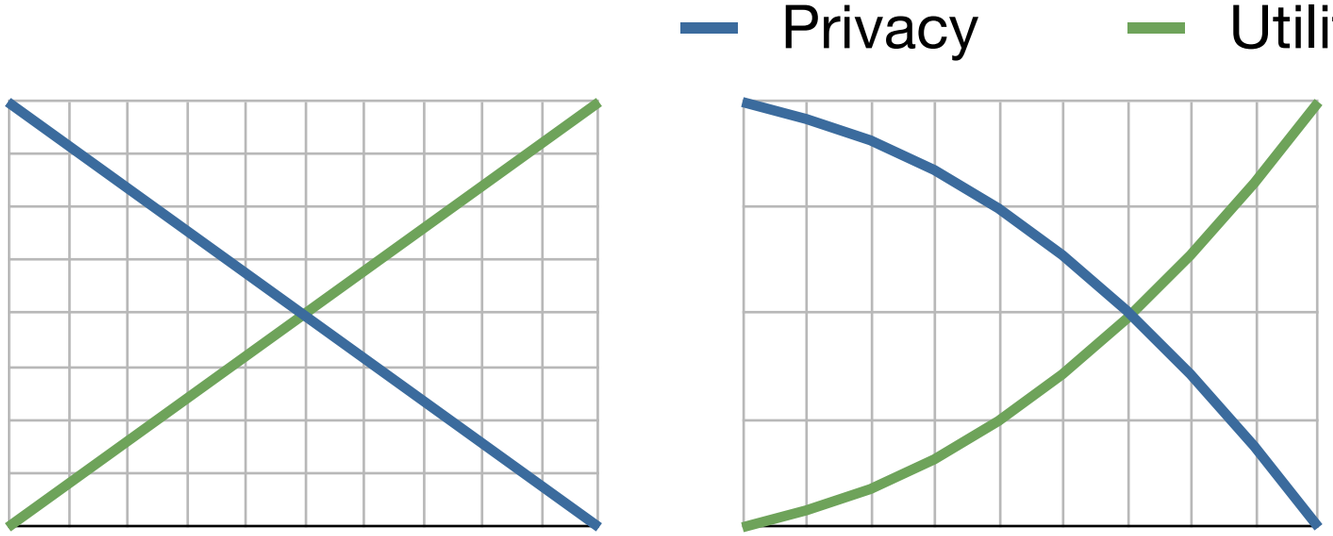
A pervasive dilemma...privacy vs. utility

divulge no information

perfect privacy, no utility

all phenomena recorded, indexed, and shared

no privacy, full utility

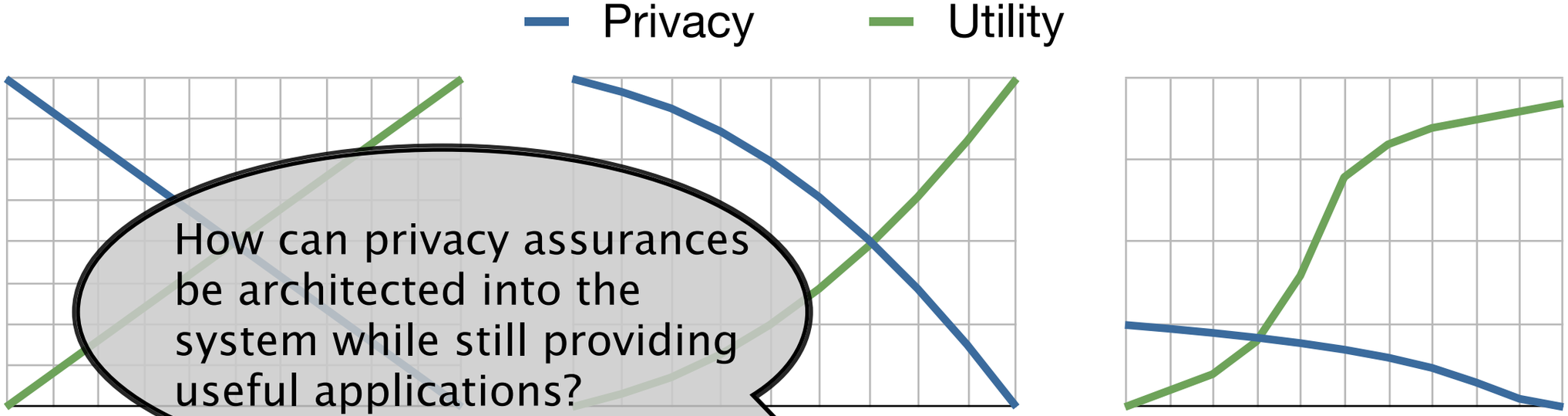


5

A pervasive dilemma...privacy vs. utility

divulge no information
perfect privacy, no utility

all phenomena recorded, indexed, and shared
no privacy, full utility



5

Prison building at Presidio Modelo, Isla De la Juventud, Cuba
image from Wikipedia

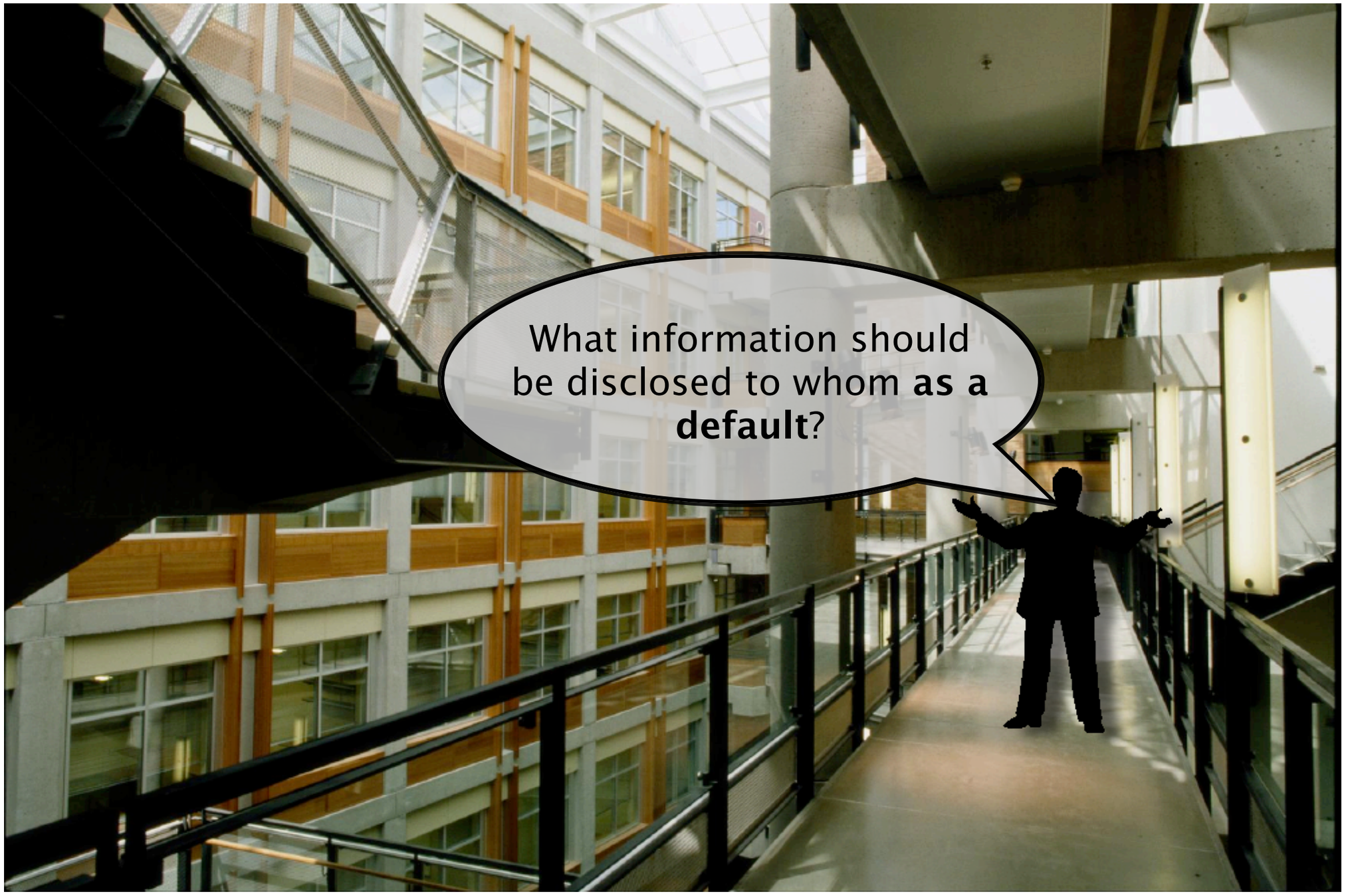
"The state of conscious and permanent visibility [assures] the automatic functioning of power..."

Michel Foucault, *Discipline and Punish*

Prison building at Presidio Modelo, Isla De la Juventud, Cuba
image from Wikipedia

Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu

Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu



Paul Allen Center for Computer Science and Engineering, Seattle, WA
image from cs.washington.edu


Surely there's a
safer, yet
useful default...

Physical Access Control (PAC)

- every user has access to a **personal store of data**
    - stores events that occurred when and where they were **physically present**
    - augments users' memory of places, objects, and people **encountered**
- provides **symmetric visibility**
- *principle:* start from human sensory capacity and extend from there

8

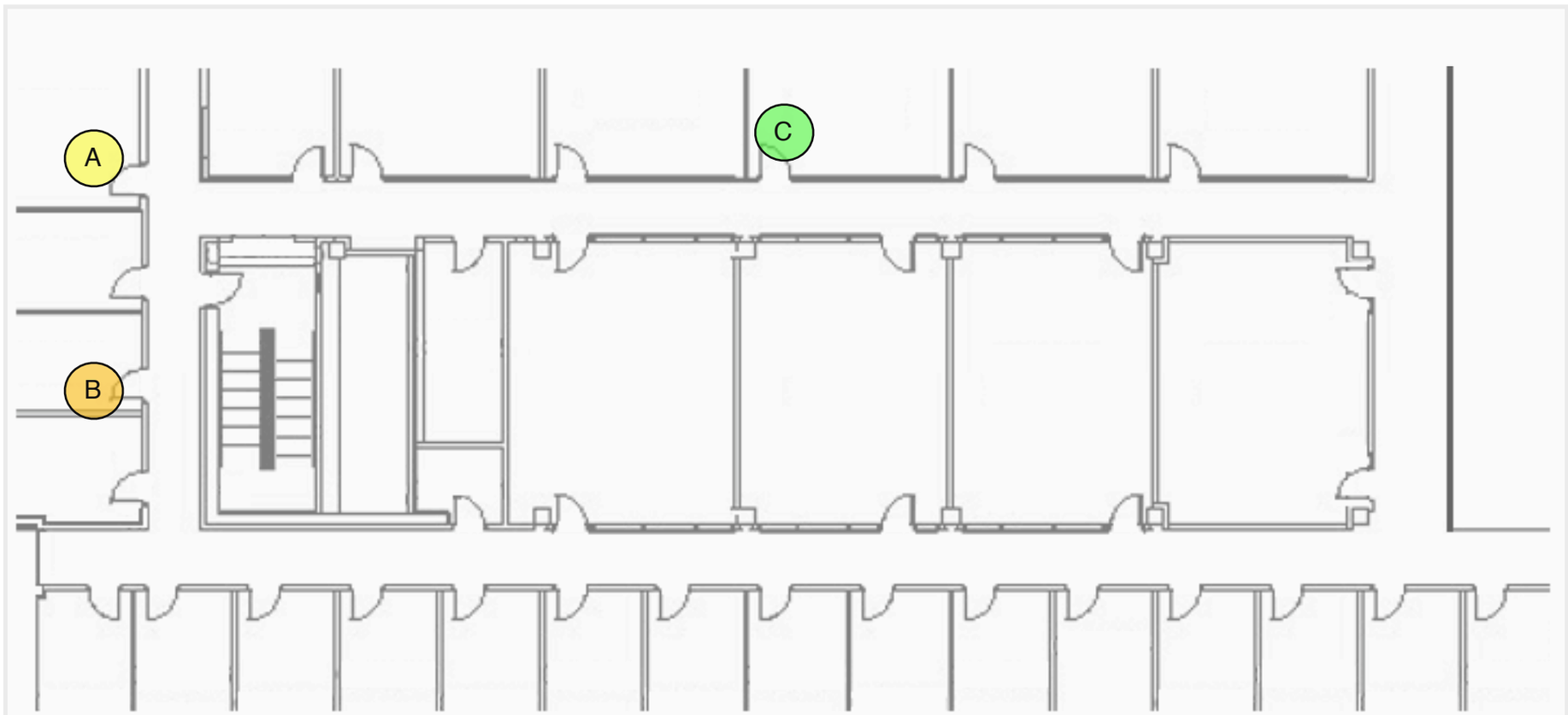
Conceptual Demo

Time: 0

B 's data

A 's data

C 's data

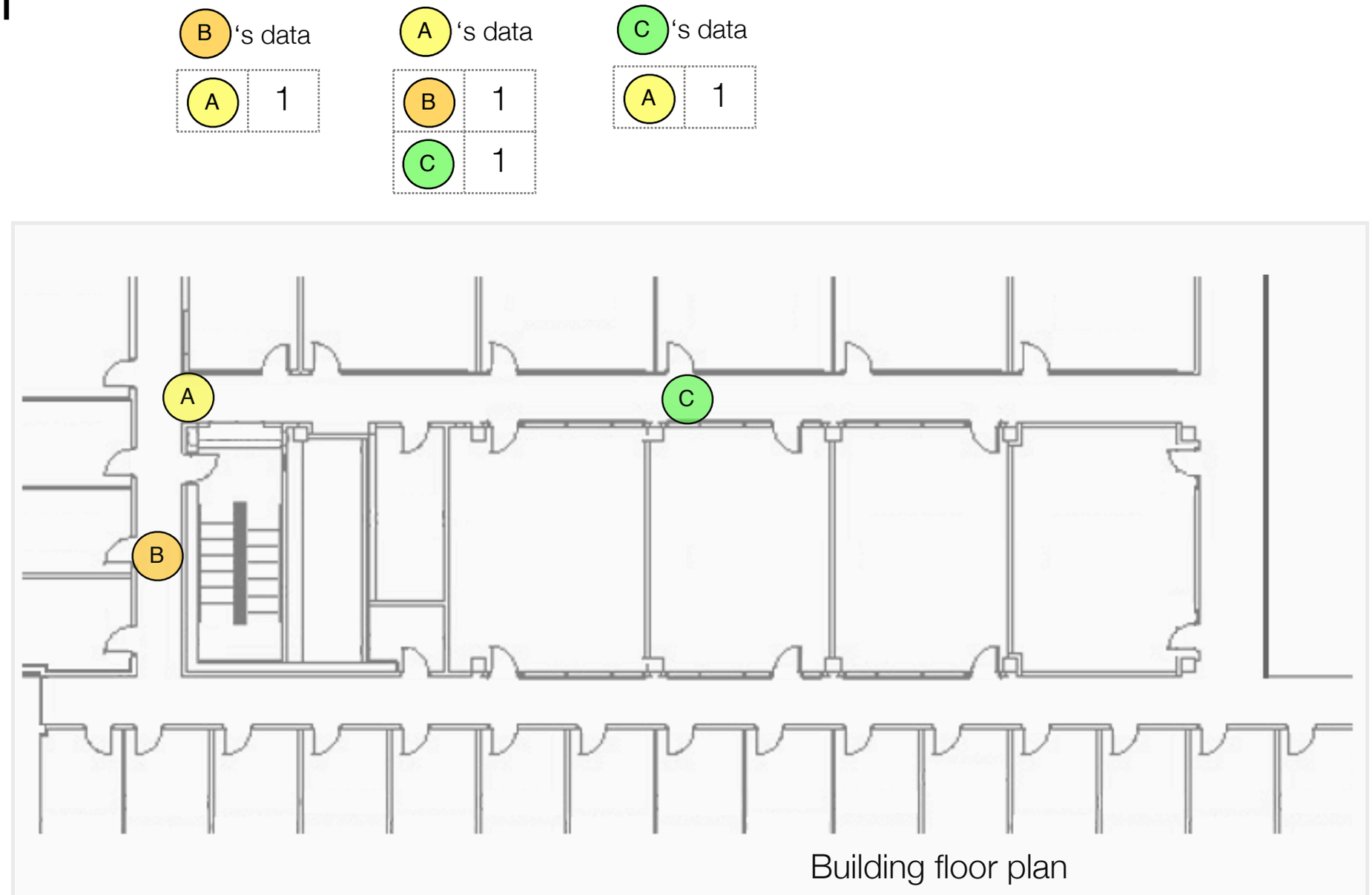


Building floor plan

9

Conceptual Demo

Time: 1



Building floor plan

9

Conceptual Demo

Time: 2

B 's data

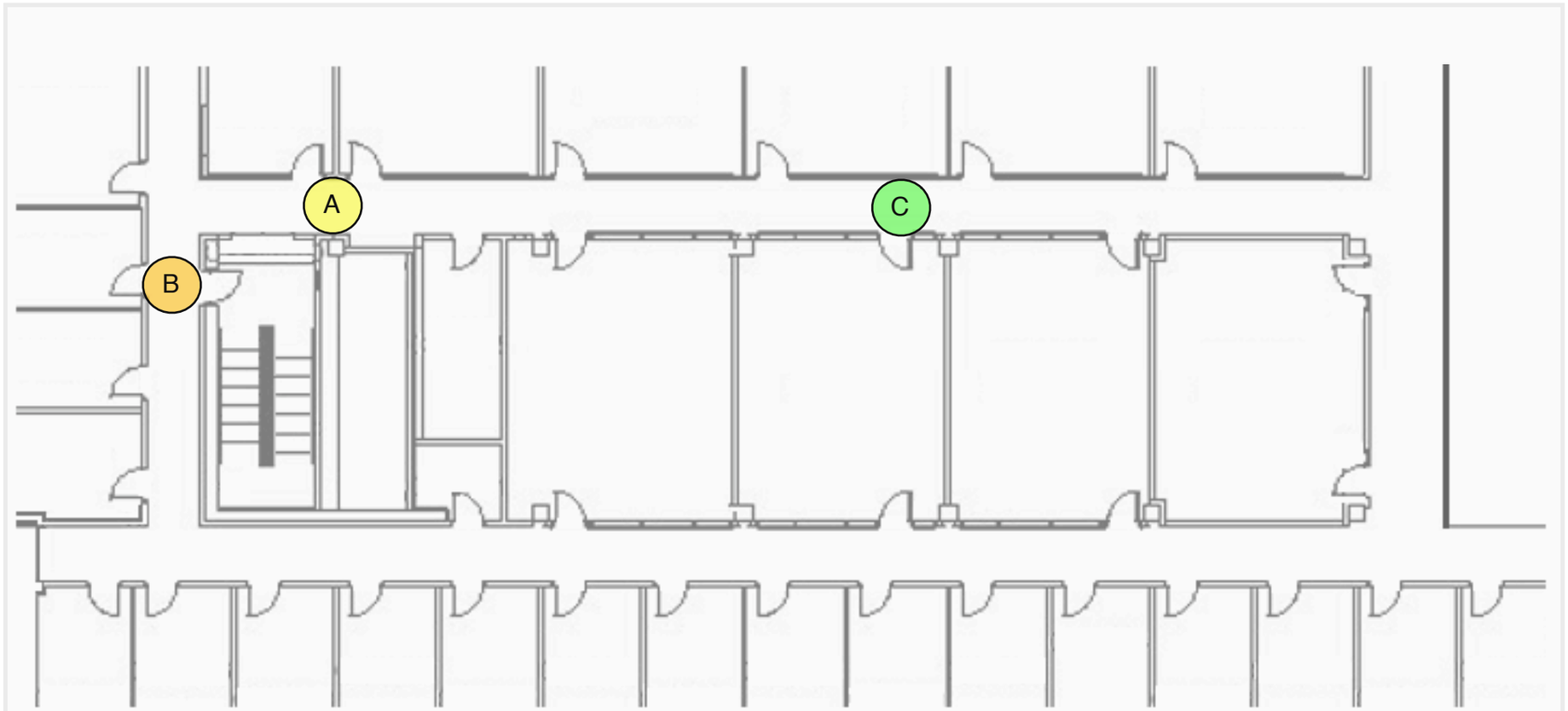
A	1

A 's data

B	1
C	1-2

C 's data

A	1-2



Building floor plan

9

How does PAC *not* model everyday experience?

10

How does PAC *not* model everyday experience?

- 360˚ vision

screen capture from “The Big Lebowski”

10

How does PAC *not* model everyday experience?

- 360˚ vision

screen capture from “The Big Lebowski”

- perfect observations entering a room full of people


from doe.gov

10

How does PAC *not* model everyday experience?

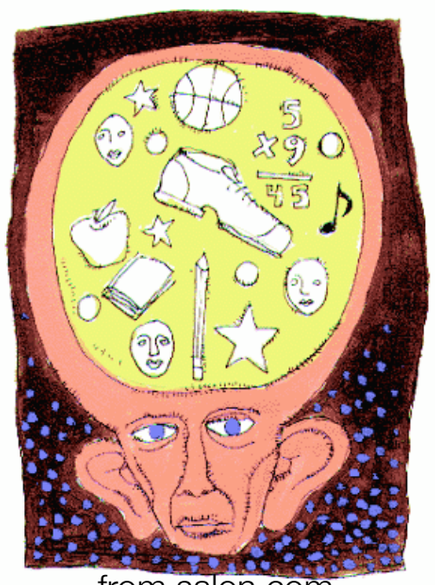
- 360˚ vision

screen capture from “The Big Lebowski”

- perfect observations entering a room full of people


from doe.gov

- memory does not decay



from salon.com

10

How does PAC *not* model everyday experience?

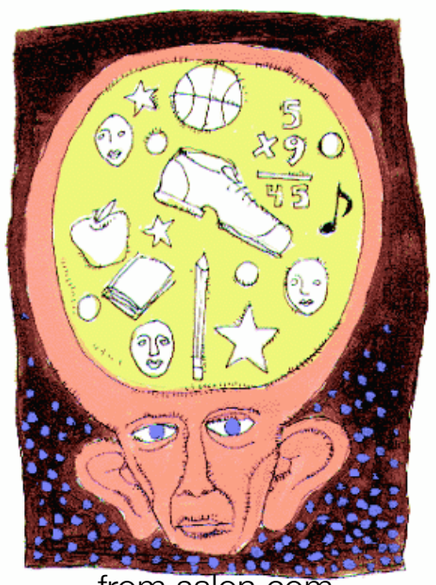
- 360˚ vision

screen capture from “The Big Lebowski”

- perfect observations entering a room full of people


from doe.gov

- memory does not decay

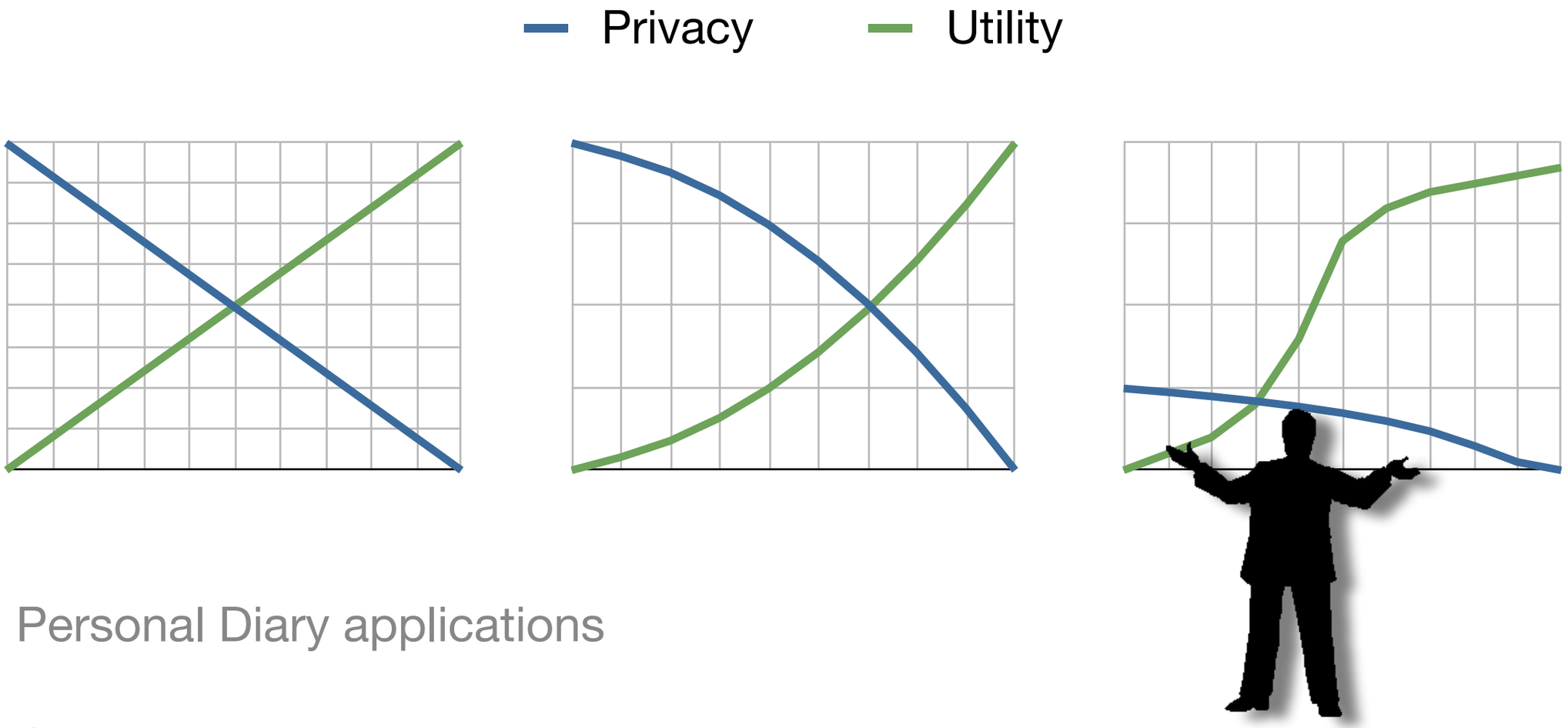


from salon.com

- loss of **plausible deniability**

10

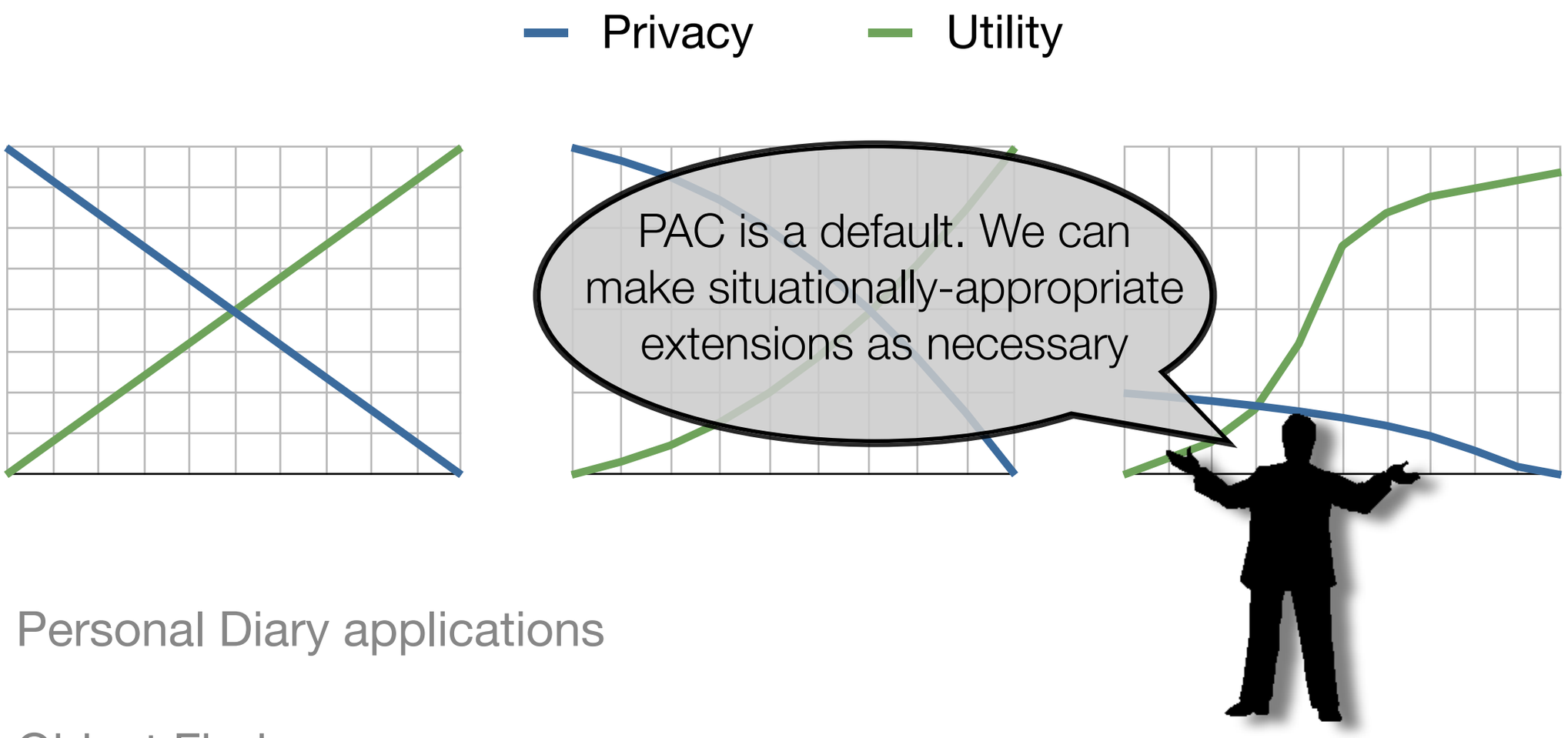
Applications of data collected through PAC



- Personal Diary applications
- Object Finder
- Personal History Analyzer

11

Applications of data collected through PAC



- Personal Diary applications
- Object Finder
- Personal History Analyzer

11

Modes of information disclosure

Malicious

Personal information is compromised by unauthorized parties

Addressed by secure systems engineering

Institutional

Organizations collect, use, and share personal and behavioral data

Addressed by contracts, federal law, corporate practice...

12

Modes of information disclosure

Malicious

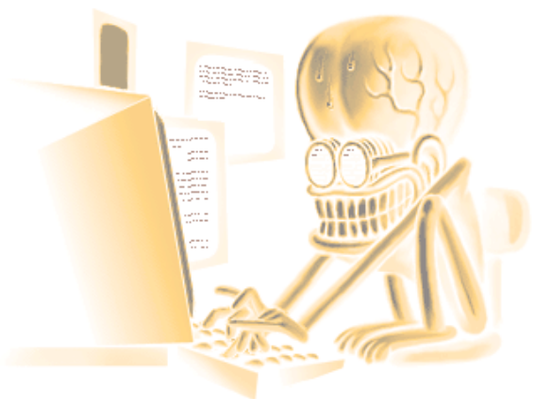
Personal information is compromised by unauthorized parties

Addressed by secure systems engineering

Institutional

Organizations collect, use, and share personal and behavioral data

Addressed by contracts, federal law, corporate practice...



Mediated

Peers and superiors access information through some authorized interface

Mediated by access control policies

12

Implementation of PAC in the RFID Ecosystem

RFID Ecosystem architecture

tag read event (TRE): `{tag identifier; antenna identifier; timestamp }`

14

RFID Ecosystem architecture

tag read event (TRE): `{tag identifier; antenna identifier; timestamp }`

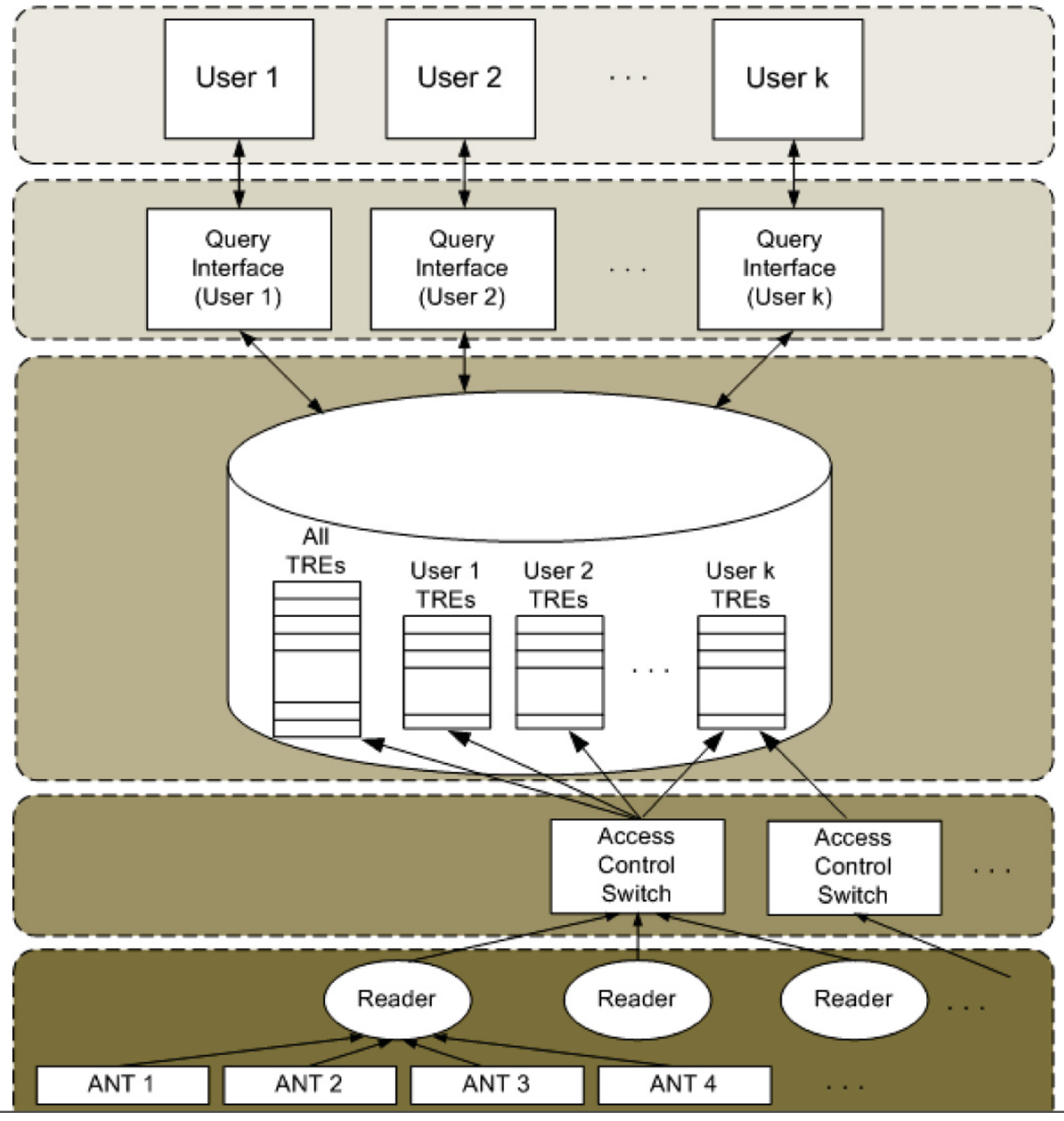
Users

Applications

Centralized database

Access control switch

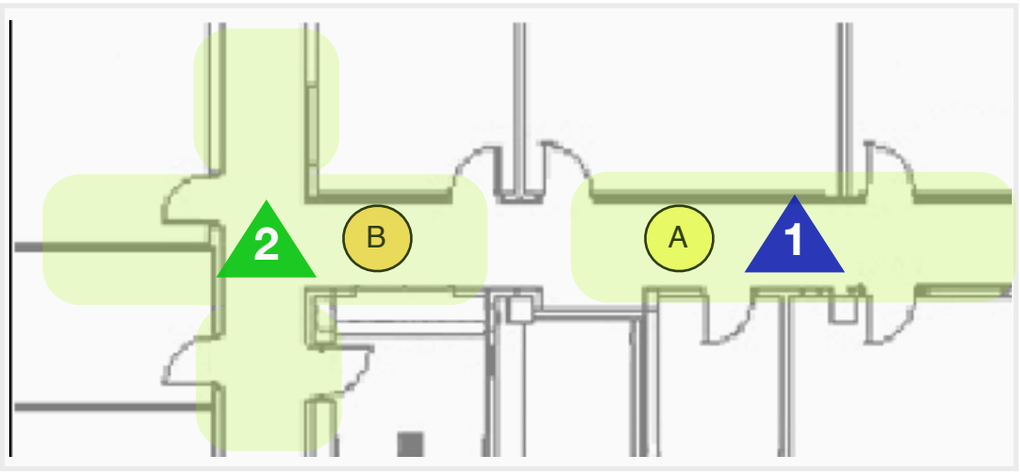
RFID hardware



14

Mutual visibility

determine whether the entities described in two tag reads were **mutually visible** (share an unobstructed line of sight)



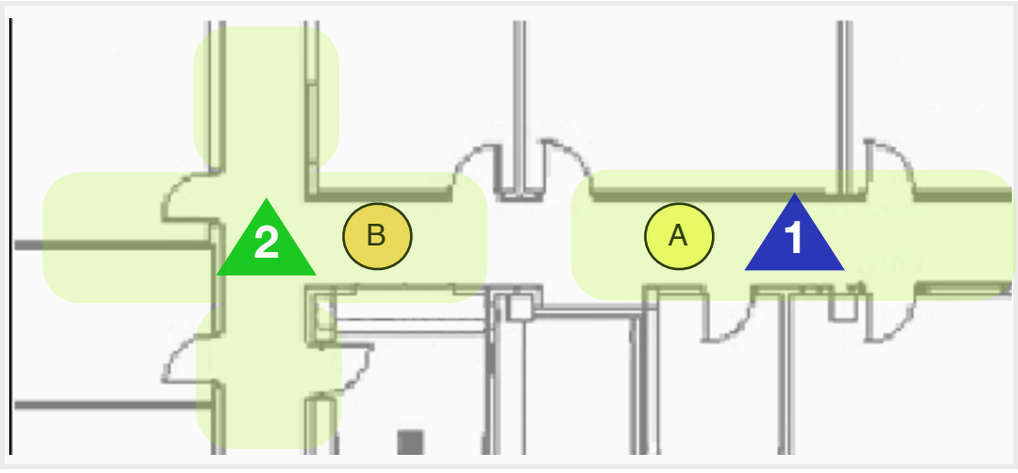
{Alice (A); Antenna 1; 08:02:45 }

{Bob (B); Antenna 2; 08:02:50 }

15

Mutual visibility

determine whether the entities described in two tag reads were **mutually visible** (share an unobstructed line of sight)



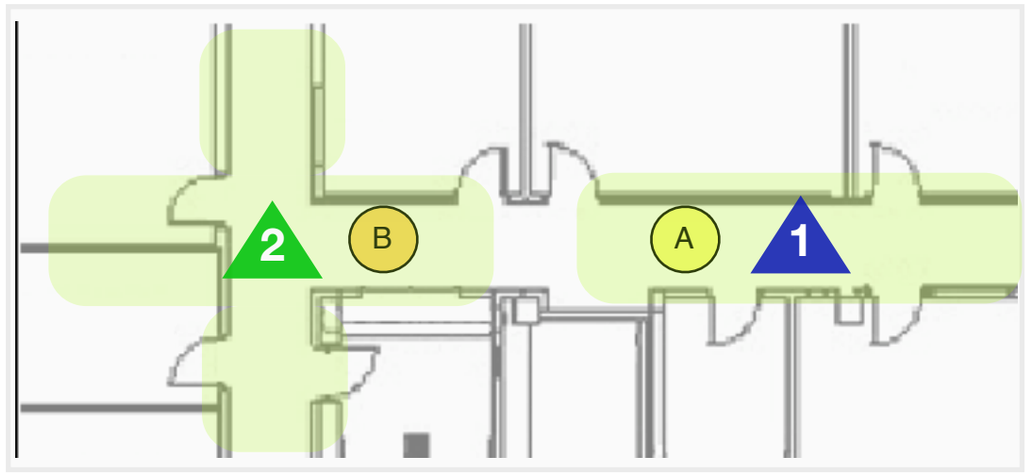
{Alice (A); Antenna 1; 08:02:45 }

Mutually visible?

{Bob (B); Antenna 2; 08:02:50 }

15

Mutual visibility (continued)



{Alice (A) ; Antenna 1 ; 08:02:45 }

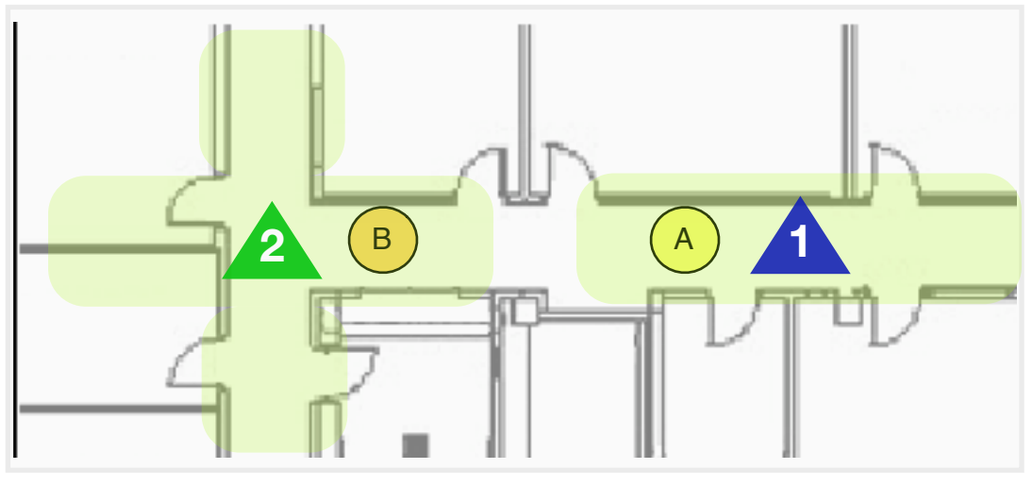
Mutually visible?

{Bob (B) ; Antenna 2 ; 08:02:50 }

16

Mutual visibility (continued)

- need to use antenna location as tag location



{Alice A ; Antenna 1 ; 08:02:45 }

Mutually visible?

{Bob B ; Antenna 2 ; 08:02:50 }

16

Mutual visibility (continued)

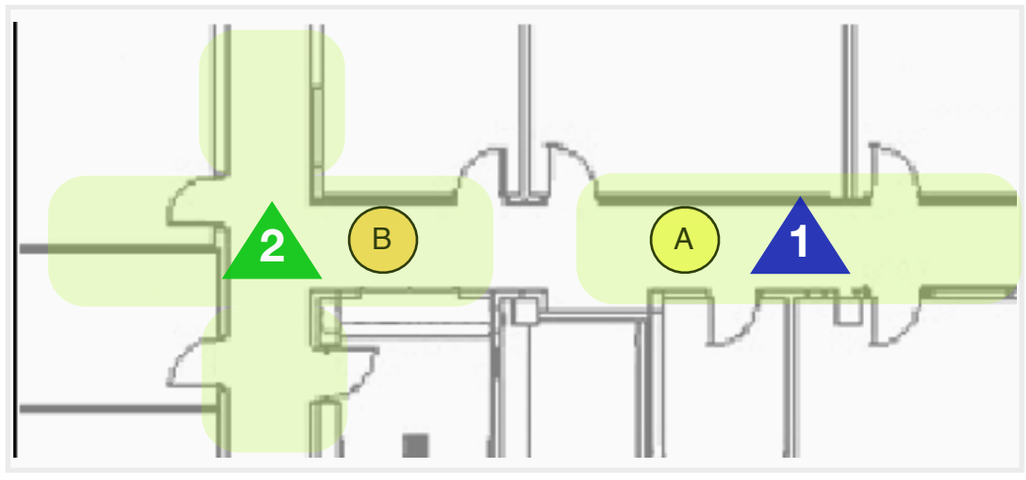
- need to use antenna location as tag location
- two tags read events are said to be mutually visible if they satisfy two constraints:

  1) **temporal constraint:** occur within a time window Δ of each other

  2) **spatial constraint**:

     A) are read by the same antenna or

     B) the involved antennas are considered mutually visible



{Alice (A); Antenna 1; 08:02:45 }

Mutually visible?

{Bob (B); Antenna 2; 08:02:50 }

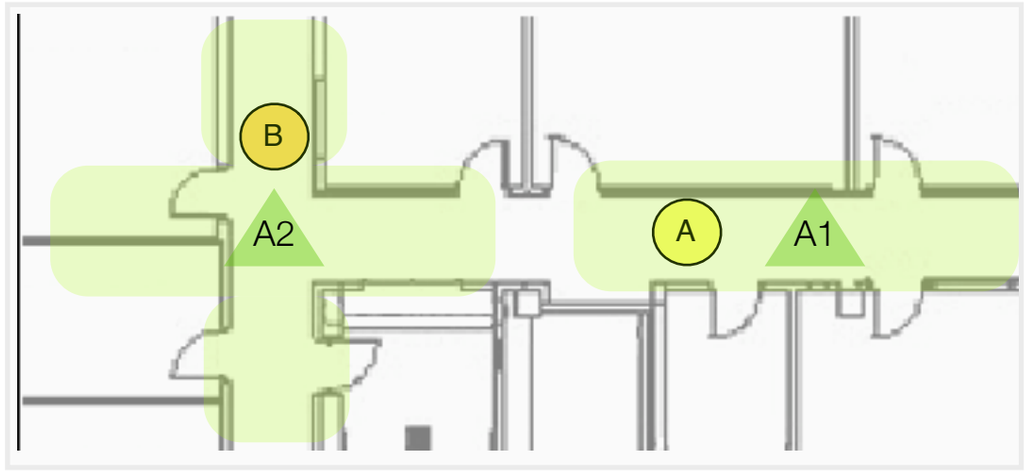
16

Deployment challenges

17

Deployment challenges

- antenna placement

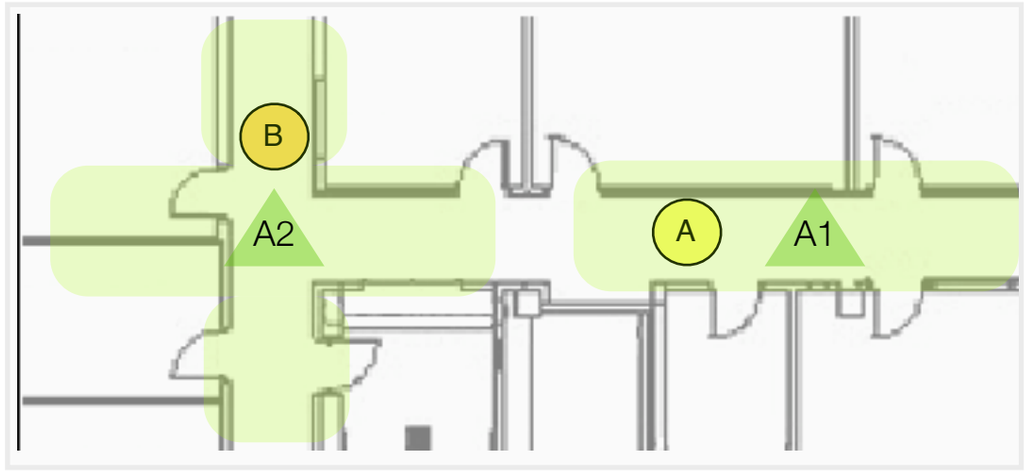



```
{A; A1; 08:02:45 }
{B; A2; 08:02:45 }
```


17

Deployment challenges

- antenna placement



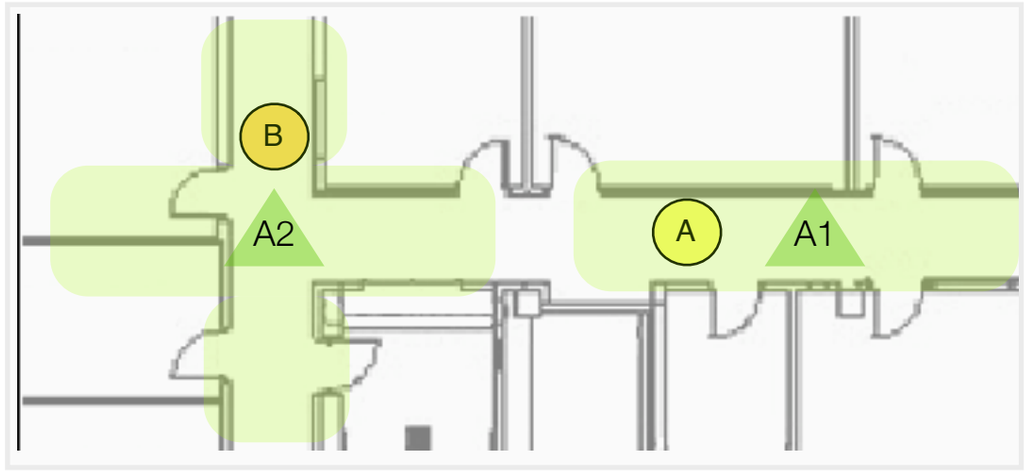

```
{A; A1; 08:02:45 }
{B; A2; 08:02:45 }
```

- distinguishing tagged objects from tagged people

17

Deployment challenges

- antenna placement




```
{A; A1; 08:02:45 }
{B; A2; 08:02:45 }
```

- distinguishing tagged objects from tagged people

- “misplaced” user tags

17

Conclusion

- start from a safe principle of symmetric visibility
- define Physical Access Control
- instantiation within an RFID deployment

18

Collaborators:

Evan Welbourne

Nodira Khoussainova

Vibhor Rastogi

Magda Balazinska

Gaetano Borriello

Yoshi Kohno

Dan Suciu

Physical Access Control for Captured RFID Data

Vol. 6, No. 4
October–December 2007

IEEE pervasive COMPUTING
MOBILE AND UBIQUITOUS SYSTEMS
www.computer.org/pervasive