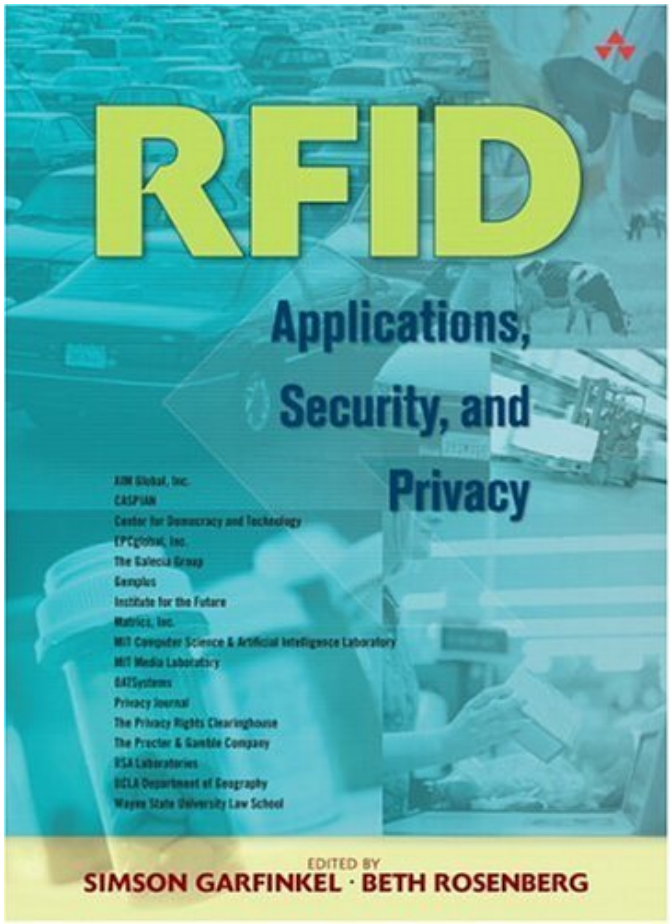
RFID Security and Privacy

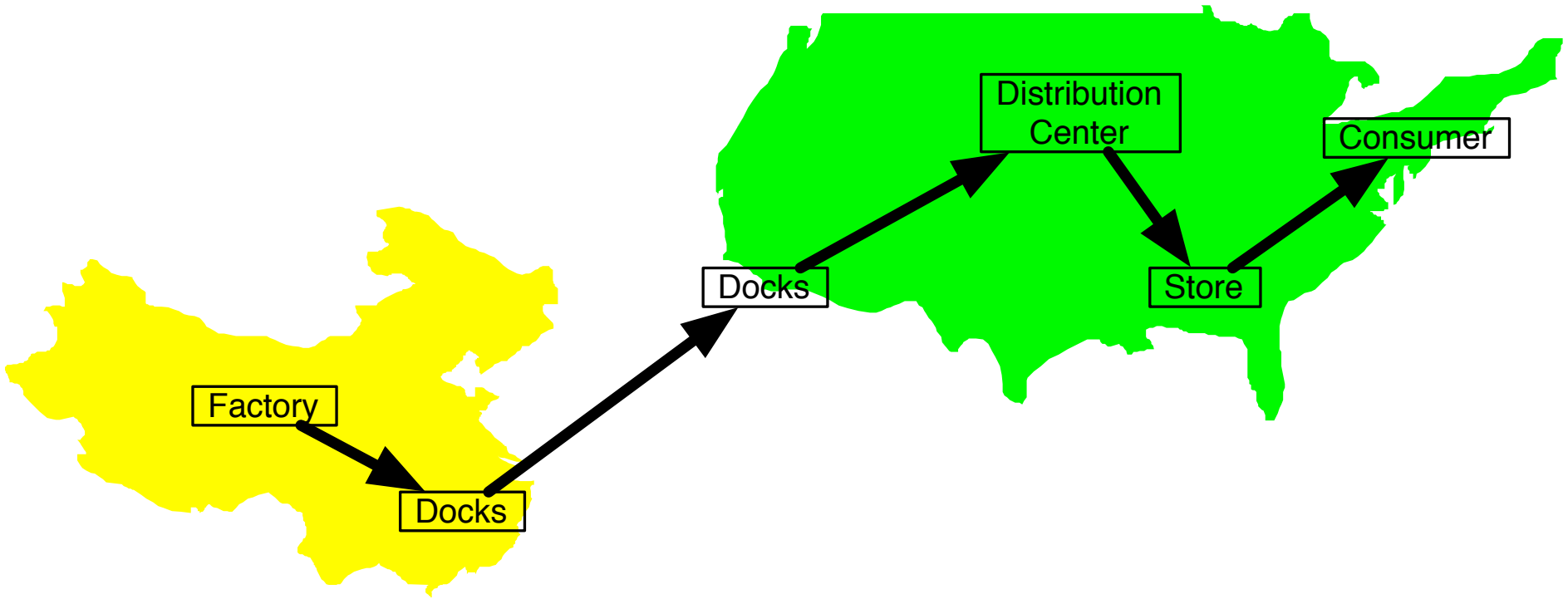
Simson L. Garfinkel, Ph.D.



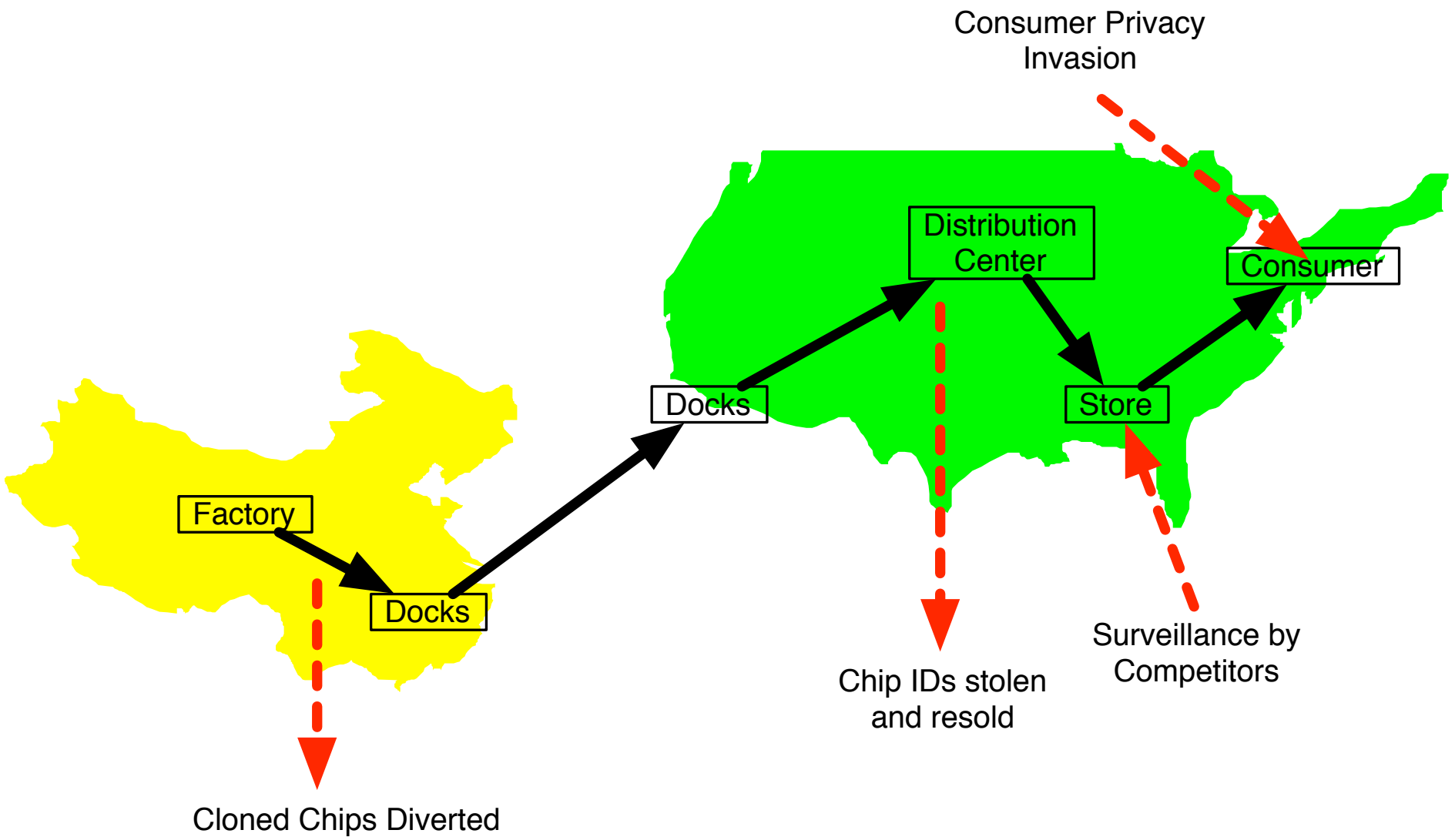
Center for Research on Computation and Society
Harvard University

October 5, 2005

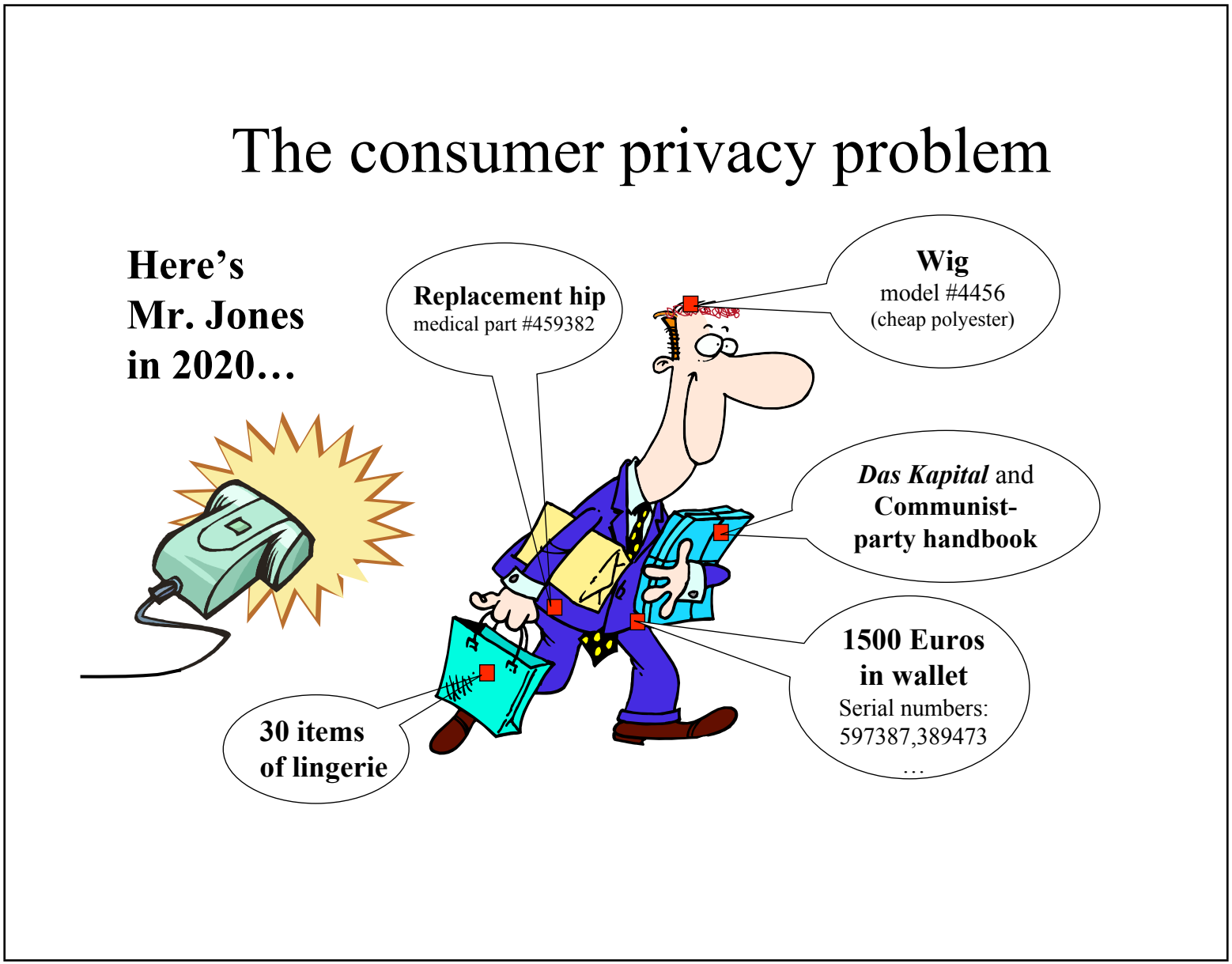
RFID: The Industry's Vision



RFID: Privacy and Security Concerns



One vision of the privacy problem



Source: Ari Juels, RSA Security

Another vision of the privacy problem

Another vision of the privacy problem

Hidden tags transmit to hidden receivers in the house.

The problem is *visibility* and *transparency.*

Barcodes must be visible to work.

Radio waves are invisible and penetrate; RFID tags can be hidden

This is both a privacy *and* security problem.

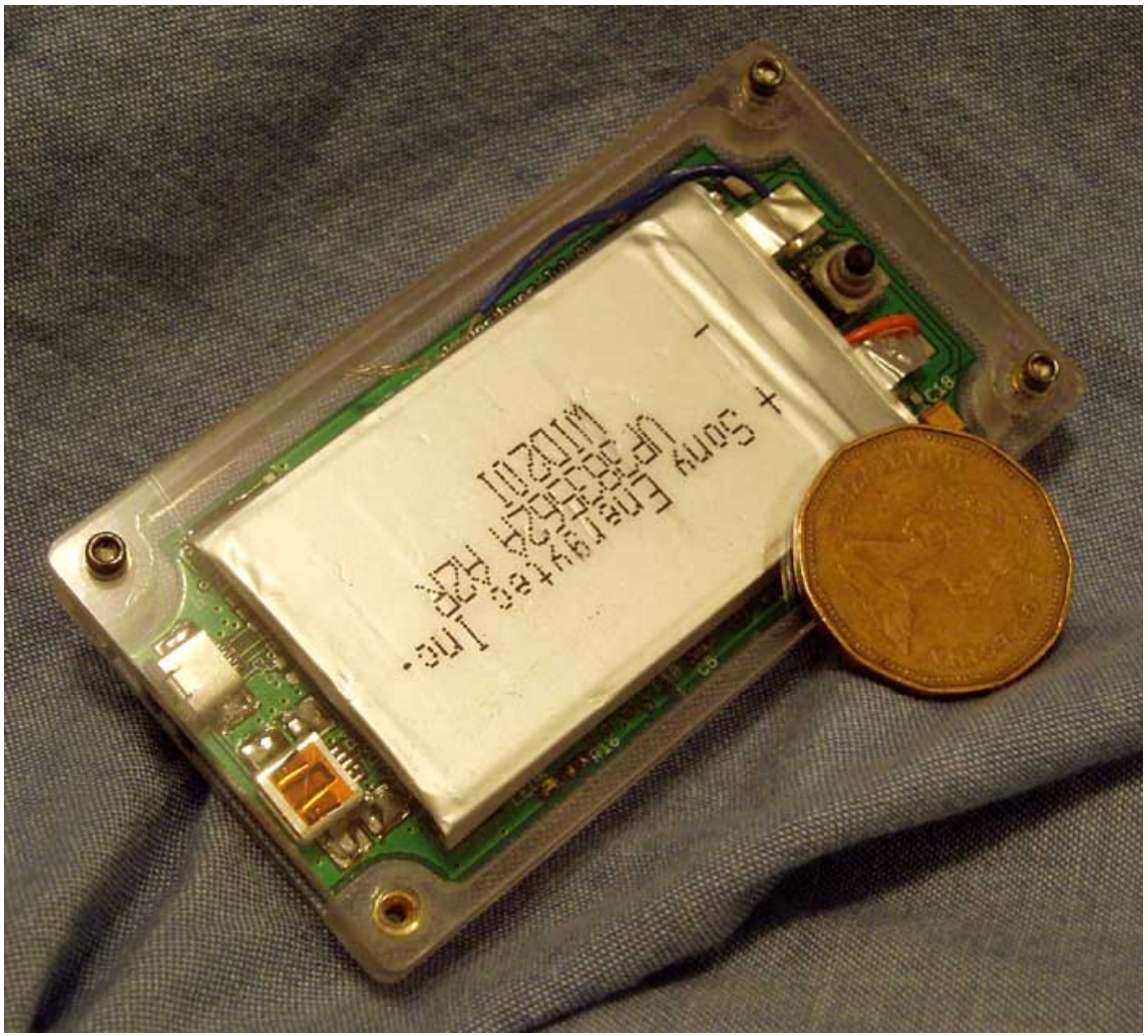
Security Threats

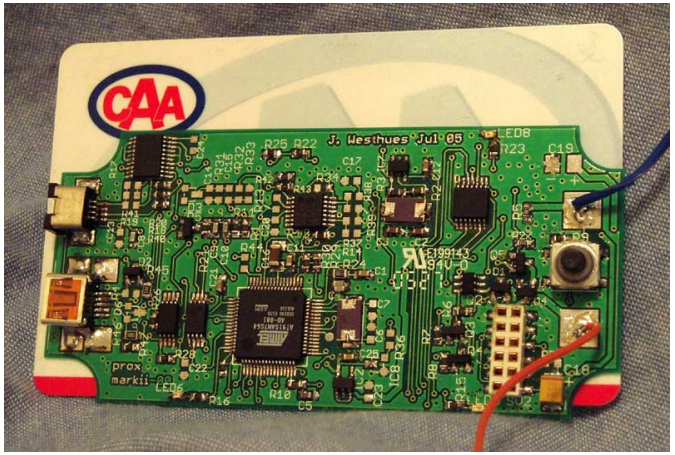
- Jamming
- Replay attacks
- Covert reading

Privacy Threats

- Covert reading
- Tracking over time
- Individual profiling

The threat realized: a prox-card cloner.





Source: Jonathan Westhues

Proposed industry solutions

At the tag:

- Kill
- Encryption

At the ONS:

- EPC Trust Services
- EPC-IS provide “fine-grained access control.”

How does one provide “fine-grained control” with 10 million players?

First problem with the industry solution: Managing the keys.

If all of the keys are different, how are they managed?

First problem with the industry solution: Managing the keys.

If all of the keys are the same, how is it protected?

Kill is a simple solution that works today, but not tomorrow.

Post-consumer use of RFID? (Refridgerators, Closets, Washing Machines)

Recycling?

Returns?

How do you verify a kill?

What about blind people?

Kill unreasonably limits RFID.

There are several proposals from outside the industry:

- Sure Kill
- Foil-lined bags
- The Blocker Tag
- Randomization
- Switches
- RFID Bill of Rights
- Abstinence

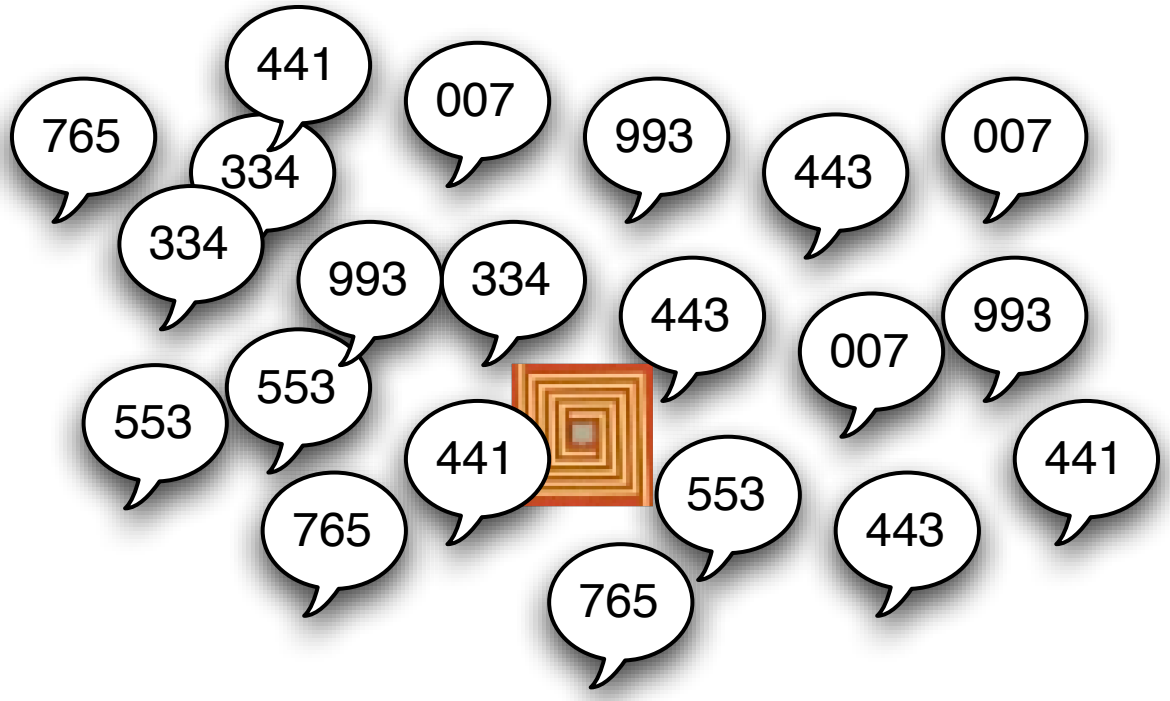
Sure Kill

This is “kill” a Biblical Sense.” — Sanjay Sarma

Foil-lined bags

These are better known as “Booster Bags.” Checkpoint’s MetalPoint detects them.

The “Blocker Tag” is a single that that looks like billions:



Consumers need to get and trust the tag.

Blockers could be made illegal. (Attacks on anti-theft systems.)

Juels proposes “polite blocking” as a compromise.

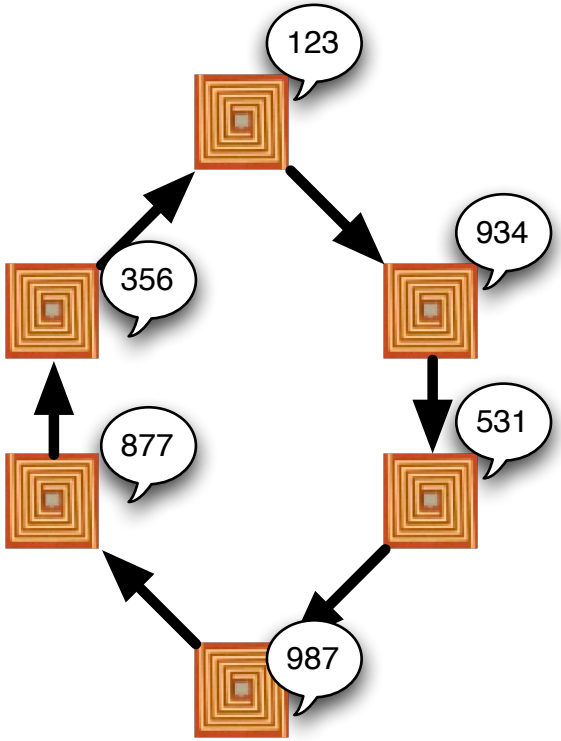
A switch could be used to turn the RFID chip on and off

RFID Inactive

RFID Active

Randomization

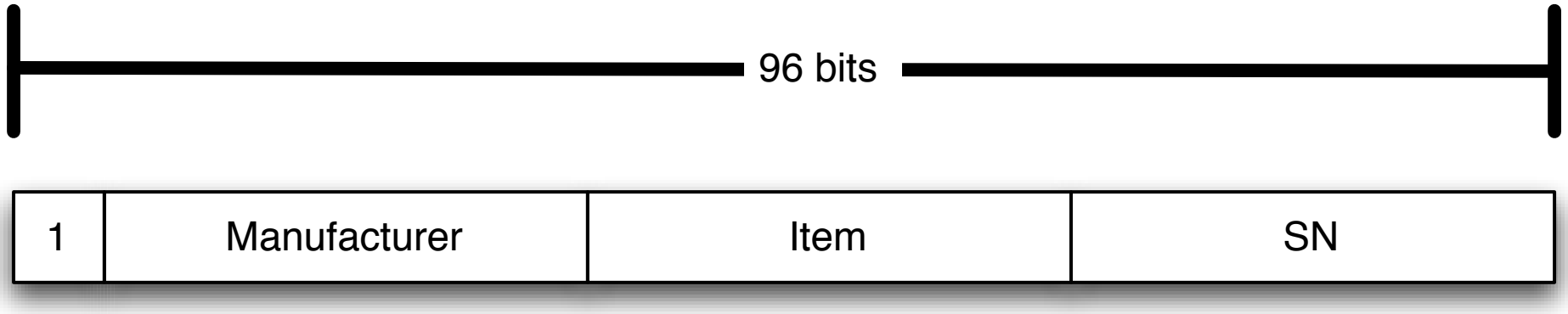
Pseudorandom rotation:



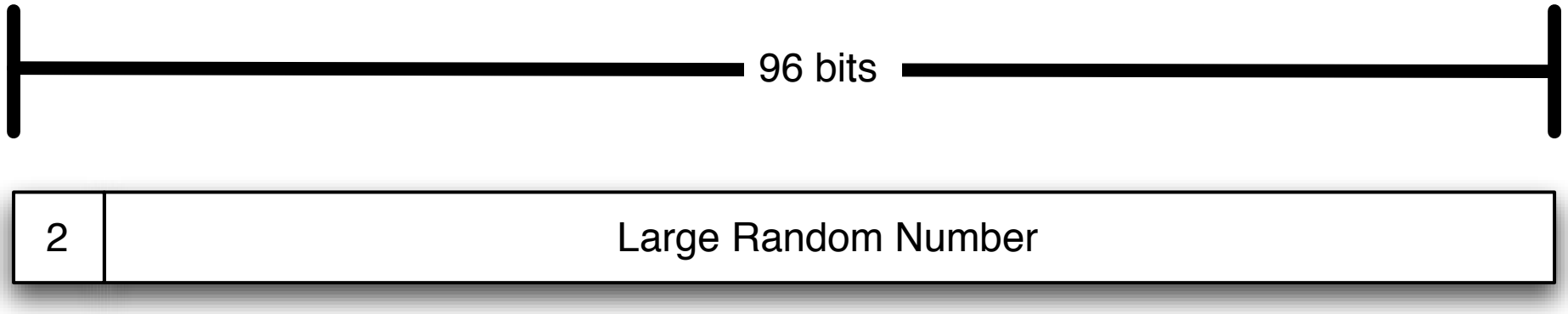
Random Assignment

If the ONS is going to be tightly controlled, randomization poses no additional overhead.

Randomization breaks the traditional ONS model

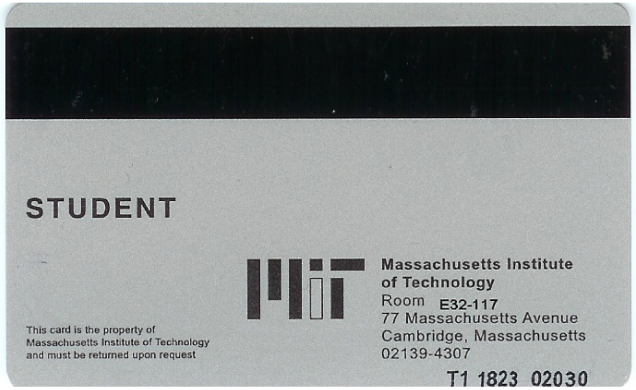


Instead, you get this:



Policy-based Solutions: The RFID Bill of Rights

MIT put an RFID chip in my ID card!



I have many questions about my chip...

Does it have my name on it?

Who has access to the database?

How far can my card be read?

What's the "security?"

What about cash purchases?

Where are the readers?

What's done with all of this data?

The RFID Bill of Rights addresses the most obvious RFID abuses

Users of RFID systems and purchasers of products containing RFID tags have:

1. The right to know if a product contains an RFID tag.

2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.

3. The right to first class RFID alternatives: consumers should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RIFD or exercise an RFID tag's "kill" feature.

4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.

5. The right to know when, where and why an RFID tag is being read.

EPCglobal's Guidelines fall short.

1. Consumer Notice—of tags, not readers.
2. Consumer Choice—consumers are allowed to discard or remove "or in the future disable" the tags.
3. Consumer Education—consumers "will have the opportunity easily to obtain accurate information about EPC and its applications."
4. 'Record Use, Retention and Security—Companies will follow existing privacy legislation for their databases.

These guidelines:

- Assume that no information is stored in the tags.
- No "opt-out."
- Little transparency, no accountability

http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

http://tinyurl.com/b9r2t

Abstinence

If we don’t solve these security and privacy issues, RFID may be rejected by business and consumers.

That would be a pity.

Questions?