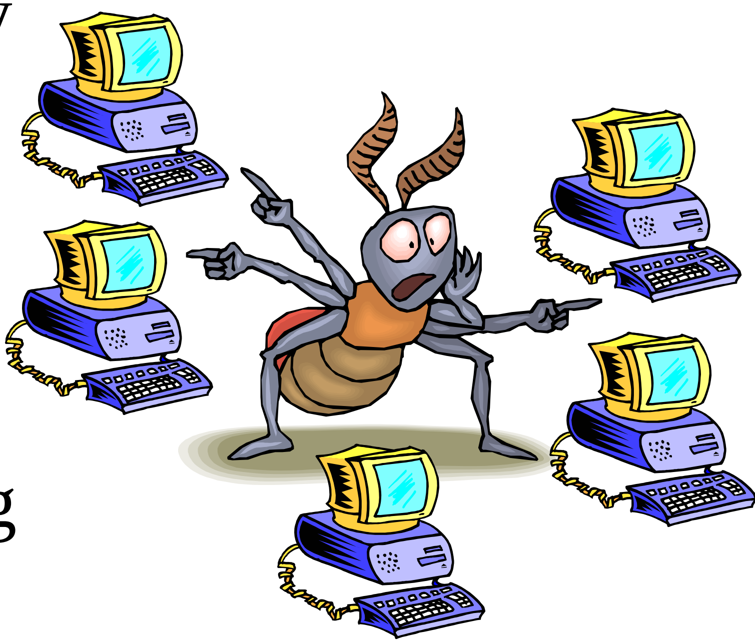
# RFID and Consumer Privacy

**Dr. Ari Juels**
**Principal Research Scientist**
**RSA Laboratories**
**FTC workshop, 21 June 2004**

RSA LABORATORIES

# RFID means: A world with billions of ant-sized, five-cent computers

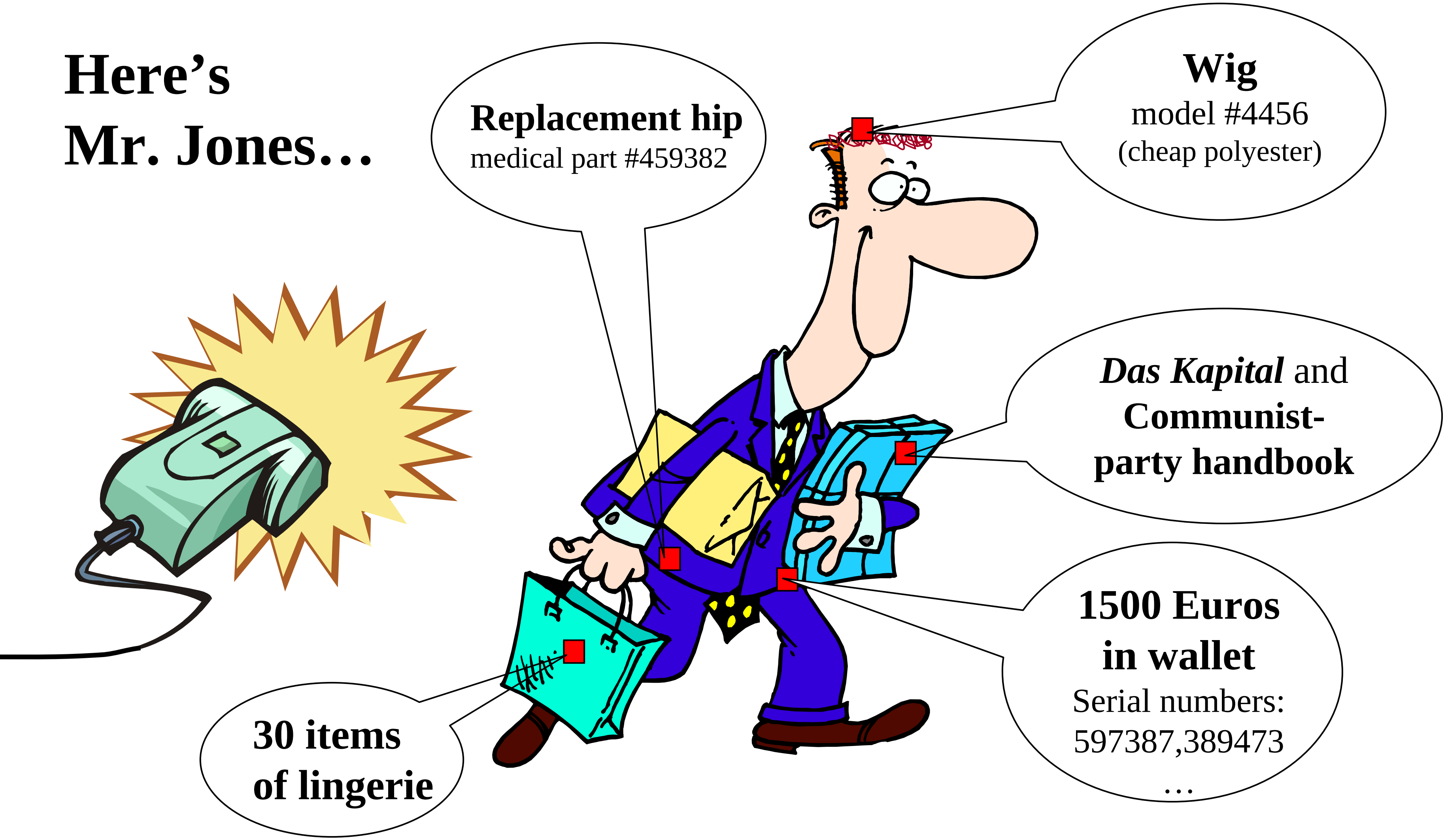
- What does this mean for privacy and security?
- Little computational power
  - Most common RFID tags can’t do “encryption” (and “encryption” wouldn’t solve problems anyway)



- Subject to surreptitious scanning
- Mobile and personal
- Good computer security is hard in general
- With good tools and foresight, we know how to achieve *adequate* computer security

# The consumer privacy problem

**Here's Mr. Jones…**



**Replacement hip**
medical part #459382

**Wig**
model #4456
(cheap polyester)

***Das Kapital*** and **Communist-party handbook**

**1500 Euros in wallet**
Serial numbers:
597387,389473
…

**30 items of lingerie**

+ tracking and profiling

# We’ve heard examples of consumer backlash

- Considerable media coverage, successful boycotts of Gillette, Benetton, Metro AG, etc.
- Utah, California, Massachusetts, etc. working on RFID privacy legislation
- 42% of Google results on “RFID” include word “privacy”

# One solution: “killing” of RFID tags

***“Dead tags tell no tales”***

***Problem: RFID tags are much too useful…***

# Some consumer applications today

- ExxonMobil Speedpass
- Contactless building-access cards
- Library books
  - Video rentals
- House pets

# Consumer applications tomorrow

- “Smart” products
  - Clothing, appliances, CDs, etc. tagged for store returns
- “Smart” appliances
  - Refrigerators that automatically create shopping lists
  - Closets that tell you what clothes you have available, and search the Web for advice on current styles, etc.
- Aids for physically and cognitively impaired
- RFID-enabled mobile phones (e.g., Nokia)
  - Scan movie poster to learn show times
  - Scan consumer product to get price quotes
- Recycling
  - Plastics that sort themselves

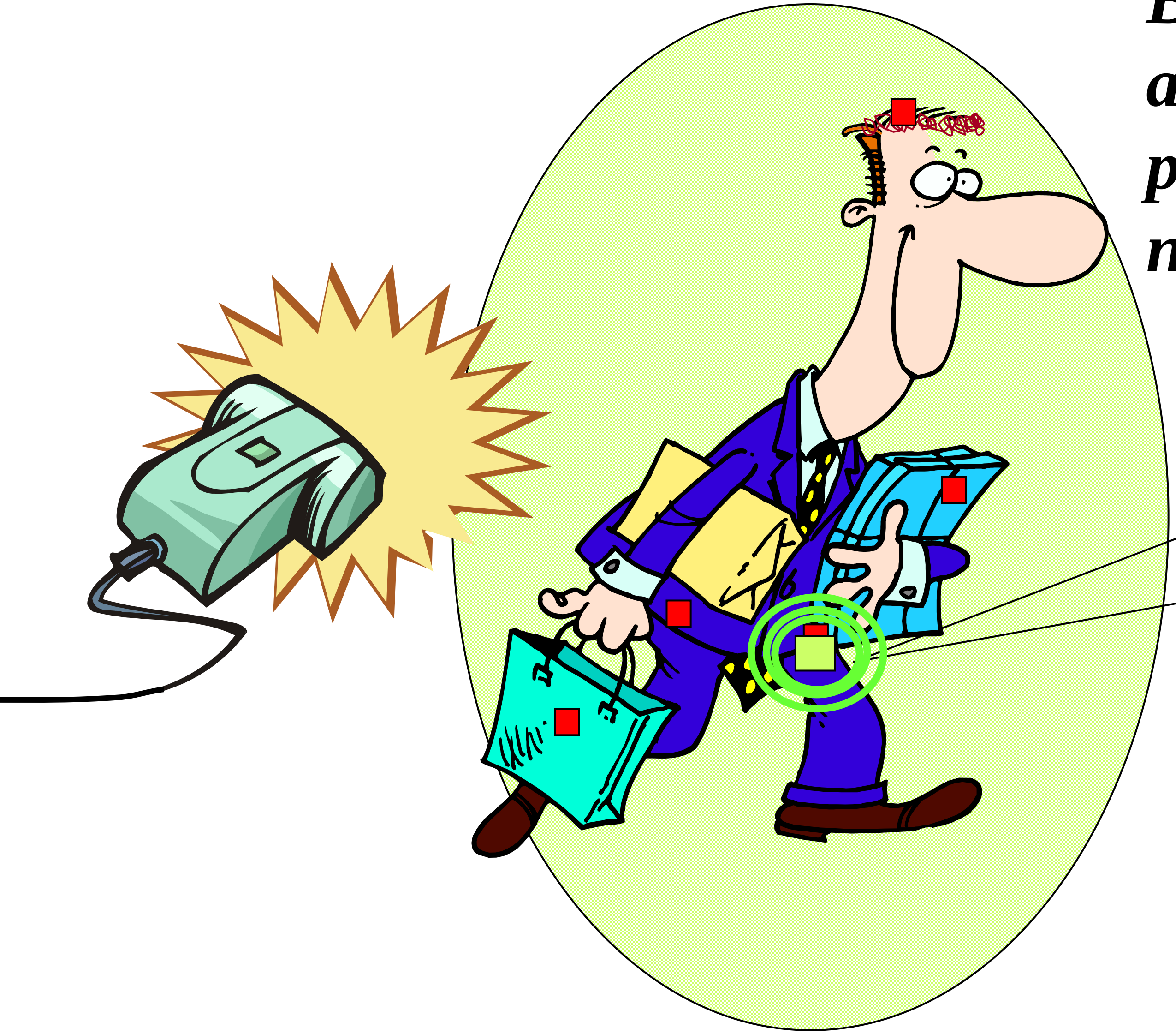
# The Key Message

1. **Embedding of RFID tags in consumer items will happen, and presents a serious danger to privacy if deployed naïvely.**

2. **The danger can be mitigated: It is possible to strike a technical and social balance between privacy and convenience.**

# The “Blocker” Tag

***Blocker simulates all** (billions of) **possible tag serial numbers!!***



**1,2,3, …, 2023 pairs of sneakers and 5068 dishwashers and… (reading fails)…**

Privateway Supermarkets
Two bottles of Merlot #458790

**Blocker tag system should protect privacy only for *purchased* items**

# Consumer privacy + commercial security

- Blocker tag is ***selective***
- Blocker tag works with RFID-tag **privacy bit**
- Example: Supermarket
  - Blocker only blocks all tags with privacy bit ***on***
  - Items in supermarket have privacy bit ***off***
  - On checkout, privacy bit is flipped ***on*** for consumer
    - PIN required, as for “kill” operation

# More about blocker tags

- Blocker tag can be cheap
  - Essentially just another RFID tag
  - Can be embedded in shopping bags, etc.
- Standards integration essential
  - Possible EPCglobal support
- Both opt-in and opt-out approaches and very nuanced privacy policies are possible
- Blocker prototype demo here today
- *A number of other technical approaches to privacy problems are possible*

RSA Labs’ RFID Web Site:

rfid-security.com