A new Approach to RFID Privacy
Zero Knowledge Device Authentication

Enabling the potential value of RFID
through elimination of persistent consumer
and device identifiers in the ambient space

Stephan J. Engberg, CEO
Open Business Innovation

Web: http://www.obivision.com
Email: Stephan.Engberg@obivision.com

Making Privacy Default
… because the alternative is not an option

Agenda

- Privacy and security – two sides of the coin
- RFID security problems
- Zero-knowledge Device Authentication
- Advantages Post-Purchase
- Outlining the RFID privacy challanges

The failure of Privacy paradigms

- Code of Conduct – No trust/massive abuse
  - Case: US Telemarketing do-not-call
    - 55 million people registered through 2003 (57%)
- Informed Consent – Advanced blackmail
  - No privacy or no Service ⇒ fatalism and distrust
    - UK analysis: 70% report – ”cannot avoid registering”
  - EU Data Protection – bureaucratic but not ensuring privacy
- Anonymity – No take-up and fear of fraud
  - Market failure of Privacy Enhancing Technologies

Deploy <u>balanced</u> Privacy Enhancing Technologies
Give End-user Control – Get Trust & User Data

RFID Attackers

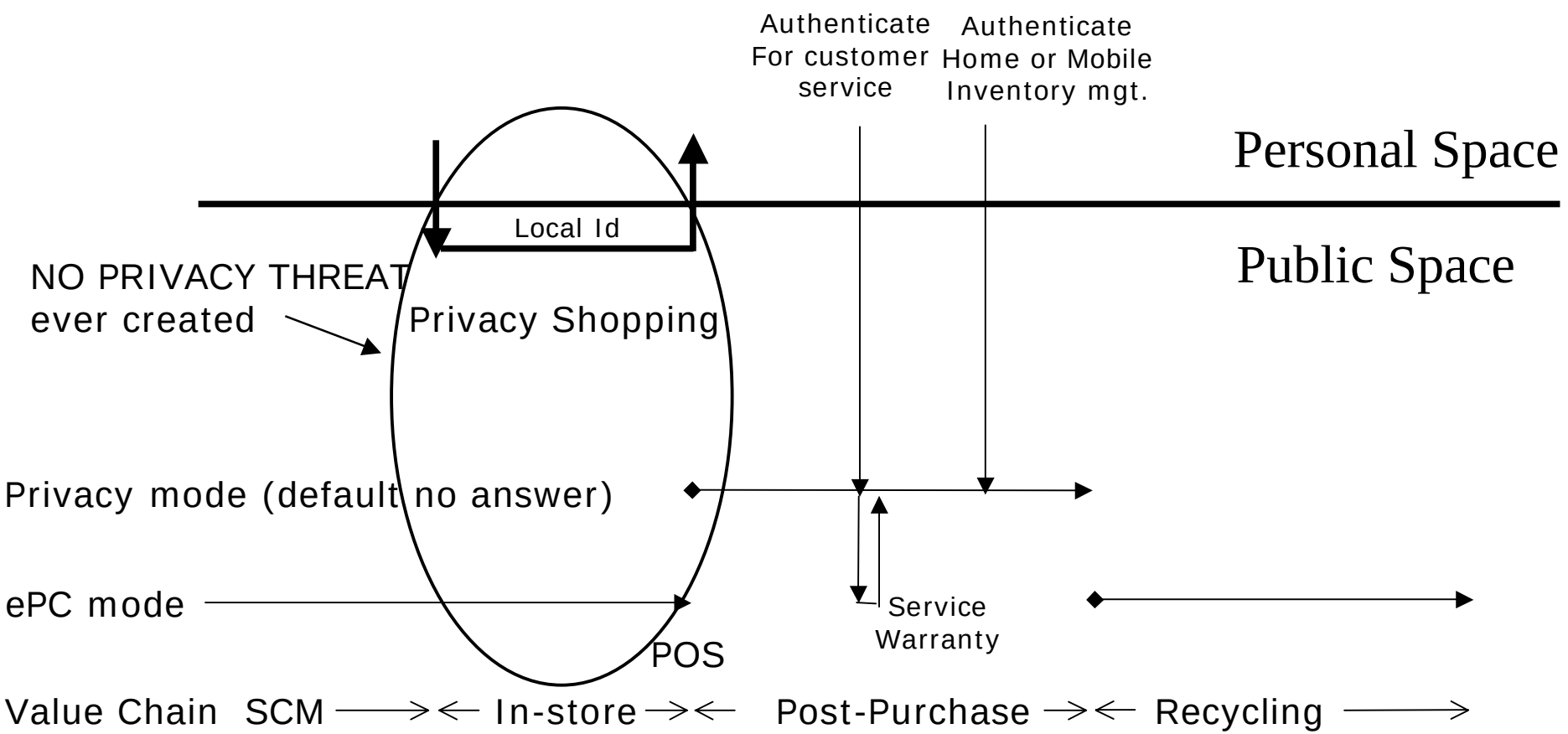
- Terrorists –
- Burglers –
- VIP –
- Workplace –
- Social –
- Retailers –
- Corporate –
- Hackers –
- Government –
- Government –

RFID have many positive uses
but without rethinking also
Security threats
Data Leakage
Tracking
Etc.

Translates into ***Trust destruction***
CLOSE – in the face of the individual

A dramatic escallation of
the Surveillance Society

RFID Privacy overview



RFID Privacy Mode

- At POS, RFID control is transferred to Consumer
  - RFID ”Privacy mode” is activated and RFID go silent
  - RFID remain *killed* unless Consumer activates
- Zero-knowledge Device Authentication
  - Low computational PET scalable to asymmetric keys
  - Single-step so that RFID can remain quiet/killed to strangers
- If RFID active when leaving the store; either
  - Product is being stolen – activate surveillance cameras etc.
  - Shop/supplier violate privacy – document and call police
- The Privacy problem turns into a win-win solution
  - RFID active for update, customer service and recycling
  - Open for Post-Purchase upgrade for intelligent services
  - With in-store Privacy Shopping open for selfservice
  - Open for custumising along the value chain
  - Little trade-of between privacy and CRM/loyalty programs
  - Can in be fully anonymous even with credit payments

Other considerations

- Dual-band solution maintain interoperability
  - Without privacy - mandatory KILL at POS
  - With privacy – consumer option to KILL
- RFID readers interoperability
  - SCM/In-store – no interoperability problems
  - At POS – readers needs additional command
  - Customer Service – more advanced possibilities
- In-store privacy issues is independant of RFID
  - BUT payments, authentication, mobile devices etc. have no security with emerging standards.

Summation

- **From the point of Trust Socio/economics**
  - RFIDs represent huge potential value / security destruction
  - RFID are easily understood threats !
  - Question: Why does Industry ignore privacy and security?
- **To promote RFIDs and reap the huge values**
  - Eliminate the threats – give end-user CONTROL
  - Employ balanced Privacy Enhancing Technologies (PET)
- **Privacy requirements solvable usings PETs**
  - Removing tracking ids post-purchase (Kill/Privacy Mode)
  - Local Identifiers only for consumers in-store (Privacy Shopping)
  - Special requirements for various applications solvable
    - Proximity, authenticity, Theft Control, Shipping, Id Cards etc.

Active Privacy is both possible
and an enabler of RFID take-up