EU Policy on RFID & Privacy

Developments 2007, Outlook 2008

Andreas Krisch <andreas.krisch@vibe.at>

http://www.edri.org/

http://www.unwatched.org/

European Digital Rights (EDRi)

- Umbrella organisation of privacy and civil rights organisations in Europe

- founded in June 2002

- 28 member organisations

- 17 different countries

- bi-weekly newsletter EDRi-gram since 2003

- German translation since 2006 on http://www.unwatched.org/

Contents

- Overview 2007
  - Results of EC Public Online Consultation
  - EC RFID Expert Group
  - EDRi Positions on RFID & Privacy
  - Opinion of the EDPS on EC RFID communication
  - Other Contributions
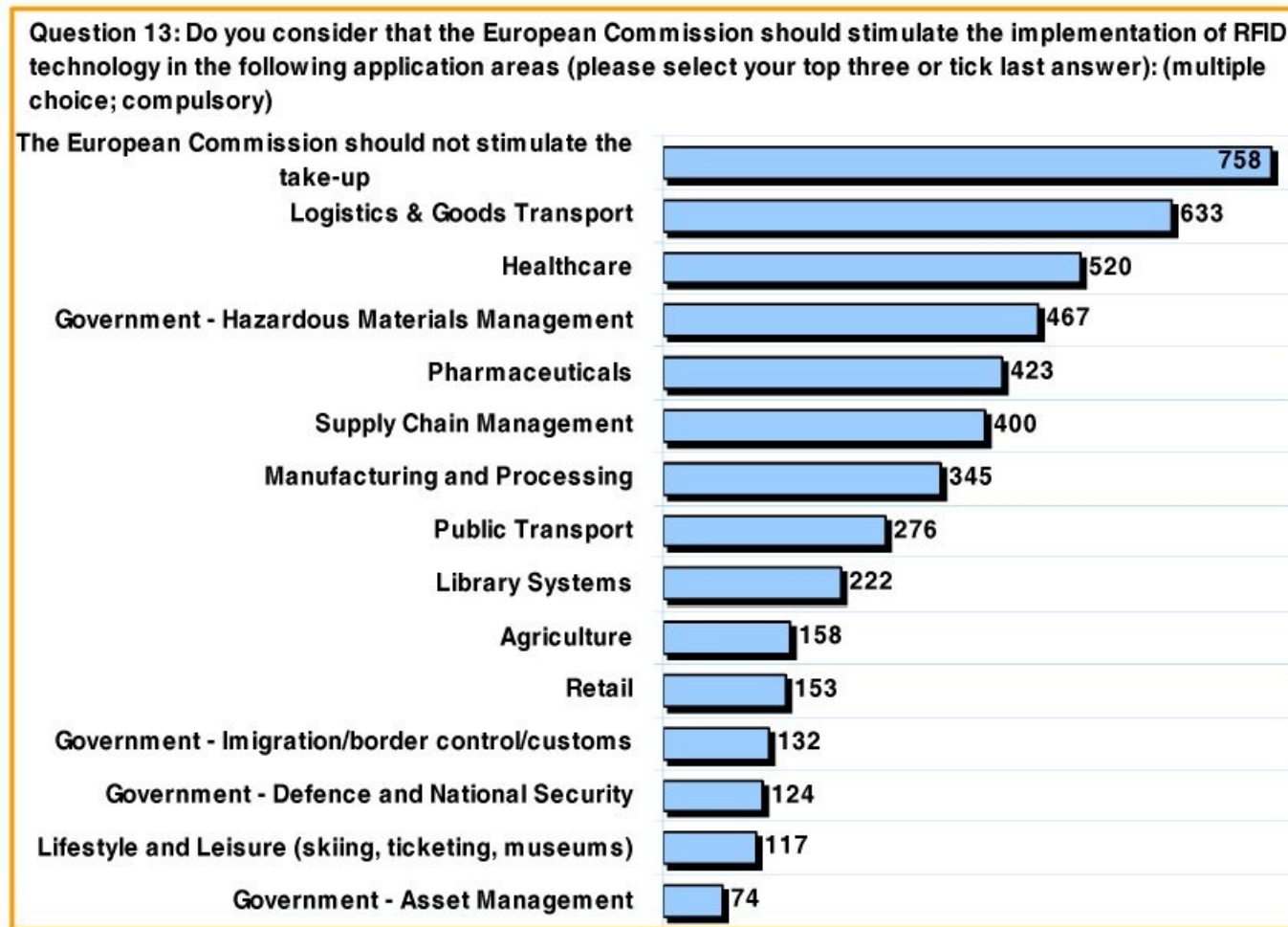- Outlook 2008
- References

EC Online Consultation (1)

- July – September 2006; 2190 respondents
  - 70% „interested citizens", 15% industry (Q5)
  - 43% from Germany, 24% from France (Q7)
  - Belgium, UK, Austria 4-5% each
- Is there great potential offered by RFID? (Q10)
  - 44% no, 41% yes
- 61%: insufficient information available for informed analysis (Q9)
- adequacy of current legislation (Q12)
  - > 50% answers: 2/3 feel legislation is inadequate
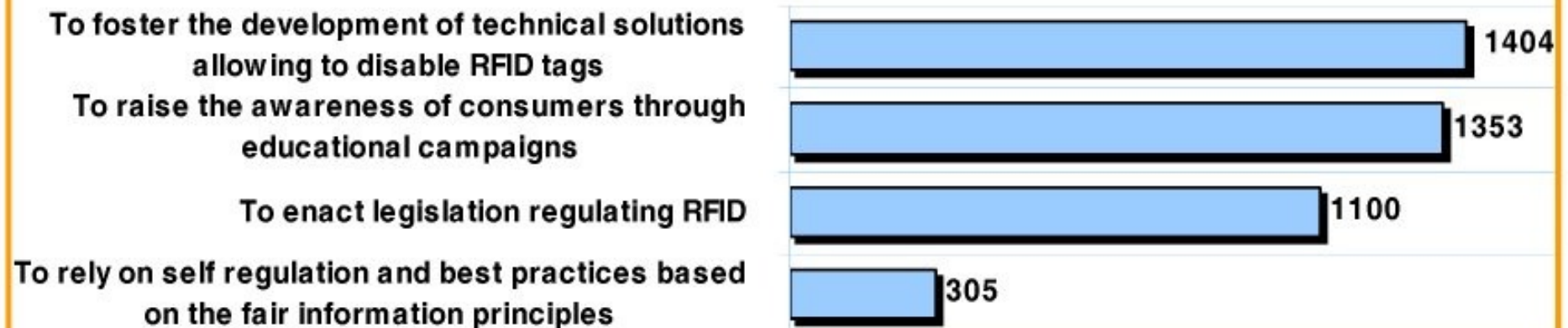
EC Online Consultation (2)

- Should the EC stimulate RFID implementation?

Question 13: Do you consider that the European Commission should stimulate the implementation of RFID technology in the following application areas (please select your top three or tick last answer): (multiple choice; compulsory)

Application Area	Value
The European Commission should not stimulate the take-up	758
Logistics & Goods Transport	633
Healthcare	520
Government - Hazardous Materials Management	467
Pharmaceuticals	423
Supply Chain Management	400
Manufacturing and Processing	345
Public Transport	276
Library Systems	222
Agriculture	158
Retail	153
Government - Imigration/border control/customs	132
Government - Defence and National Security	124
Lifestyle and Leisure (skiing, ticketing, museums)	117
Government - Asset Management	74

EC Online Consultation (3)

- RFID might lead to more surveillance (Q12)
  - clearly and visibly mark RFID Tags
  - introduce "kill" commands
  - self-regulation / industry guidelines are insufficient

Question 18: What in your opinion would be the best solution(s) to eliminate or greatly reduce the security, data protection and privacy concerns that may arise from deploying applications of RFID technology? (you can tick more than one option) (optional)

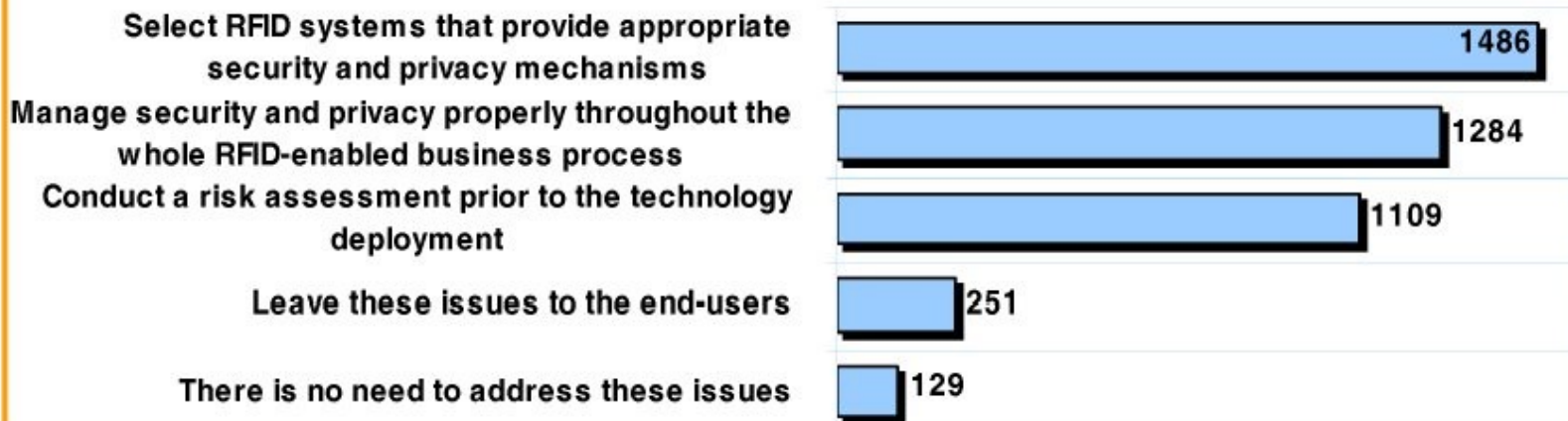| Solution	Value
To foster the development of technical solutions allowing to disable RFID tags	1404
To raise the awareness of consumers through educational campaigns	1353
To enact legislation regulating RFID	1100
To rely on self regulation and best practices based on the fair information principles	305

EC Online Consultation (4)

- ## RFID in Supermarkets
    - 1984 respondents
    - 2/3 say: automatically deactivate at check-out

Question 19: If you are in a supermarket, would you prefer a RFID tag related to a product to be: (you can tick more than one option) (optional)

Automatically de-activated at the point of sale	1339
A removable sticker attached to the product itself	1010
A proximity tag with a very short reading distance of less than 5 cm	881
Part of the product's package box	471

EC Online Consultation (5)

- How to treat privacy & security risks?

Question 21: How in your opinion should the RFID application provider treat security, data protection and privacy issues? (you can tick more than one option) (compulsory)

Select RFID systems that provide appropriate security and privacy mechanisms	1486
Manage security and privacy properly throughout the whole RFID-enabled business process	1284
Conduct a risk assessment prior to the technology deployment	1109
Leave these issues to the end-users	251
There is no need to address these issues	129

Question 23: Do you think that privacy enhancing technologies in RFID applications should: (optional)

be made mandatory (e.g., "privacy by design" rule)	1063
be promoted at European level	681
be left to the market	245

EC Online Consultation (6)

- Research options:
  - clear preference (3/4) for research on PETs (Q34)
- Governance of Internet of Things
  - 83% answered Q36
  - 86% of these agree on a transparent, fair, non discrimatory governance model, free of commercial interests

EC Online Consultation (7)

... the large majority feel that the large-scale deployment of RFID technology will result in "excessive surveillance and massive privacy violation", "collection of data about consumers in order to control their purchasing patterns", and "a big brother society.

(EU online consultation report, page 33)

EC RFID Expert Group (1)

- established for two years (07.2007 – 03.2009)
  - with an option to be renewed
- Tasks
  - provide advice to EC on recommendation to member states
  - develop guidelines on how RFID applications should operate
  - support EC in awareness raising
  - provide objective information and facilitate the exchange of experiences and good practices

EC RFID Expert Group - Members

- End User Representatives
  - ANEC, BEUC, GMB, UNI
- Industrial Associations
  - Informationsforum RFID, RFID Centre UK, The Traceability Centre
- Privacy Organisations
  - EDRi
- Representatives of Application sectors
  - Carrefour, Deutsche Post World Net, CLECAT, COCIR, EFPIA, EGA, Nokia, NXP, SAP

EC RFID Expert Group - Members

- ## Standardisation Bodies
  - CEN, EPCglobal, ETSI, ICT Standards Board

- ## Observers
  - Representatives of the Member States assuming EU Presidency between 07.2007 and 03.2009
  - Article 29 Working Party
  - European Data Protection Supervisor (EDPS)
  - CNIL

EC RFID Expert Group Activites 2007

- 5 meetings in 2007

- Dialogue between stakeholders on RFID Privacy & Security Issues

  – presentations

  – discussions

  – position papers

- Contribution to the preparation of EC recommendation to the member states on RFID and Privacy & Security Issues

EDRi Positions on RFID & Privacy

- Three written Contributions to the RFID Expert Group:
  - RFID Privacy Issues
  - RFID Security Issues
  - RFID and Informed Consent

EDRi RFID Privacy Issues (1)

- Identification vs. Information

  - RFIDs **identify** objects rather than only providing information

  - a global system identifying objects can lead to a global system identifying persons

  - main purpose of RFID is often to **provide information** on objects

  - -> limit identification to an absolute minimum

  - -> **person** using an application should be the **initiator of interactions**, not the other way round

EDRi RFID Privacy Issues (2)

- Data protection
  - strengthen DPAs (financially, organisationally)
  - minimise use of personal data, privacy friendly defaults
  - standardise interfaces for DPAs -> automated control of data protection compliance
  - establish standardised data protection audits (EuroPriSe)
  - considerably sanction unlawful behaviour
- open standards
  - enable diversity, support SMEs, enable FOS

EDRi RFID Privacy Issues (3)

- Empowerment & Awareness raising
  - trust is key for successful RFID deployment

    -> needed: effective tools for privacy protection and sufficient information on systematic context
  - provide standardised user-friendly interfaces & tools that help users control the information processed on them
  - develop adequate identity management mechanisms supporting users manage consent, ... (see the PRIME Project)
  - provide balanced, comprehensible, objective information on RFID

EDRi RFID Privacy Issues (4)

- Classification of RFID Systems
  - usually done by application, sector, reading range, used tags, ...
  - rather consider data protection and user control
- data protection
  - data-unprotected – data-shared – data-protected
- user control
  - user informed – user accessible – user controlled

EDRi RFID & Informed Consent (1)

- Information on RFID
    - general information on the technology, ideally provided by independent body w/o commercial interests in the technology
    - information on RFID usage (tags, readers, purposes, ...)
    - use of Logos could be appropriate for indicating presence of tags **and** readers
    - meaning of Logo should be kept simple (avoid confusion)

EDRi RFID & Informed Consent (2)

- Informed Consent

    - If tag remains active when an individual gains its ownership / possession provide information on

    - which information is stored on the tag

    - by whom this information can possibly be accessed.

    - provide information on RFID applications "behind" the readers (e.g. like energy consumption labels)

    - This info is needed as basis to decide whether to enter "RFID enabled areas" or not.

    - Additionally provide general information on RFID.

Andreas Krisch, European Digital Rights – www.edri.org

EDRi RFID & Informed Consent (3)

- Options for retaining or removing RFID functionality
    - opt-out vs. opt-in
    - removal of tags
    - alteration of data stored on tags
    - modify tag functionality (sleep mode, kill command)
    - leave tag and data unchanged

EDRi RFID & Informed Consent (4)

- Opt-out vs. Opt-in

  - EDRi strongly asks for opt-in because ...

  - ... default protection for everybody without requiring RFID knowledge is provided.

  - ... no sufficient access control mechanisms for data on the tag are available.

  - ... individuals have to decide on a general level (RFID yes/no) instead on an application level.

    - ... individuals always are free to opt-in when significant benefits are provided by certain apps.

  - ... it is unlikely that sufficient information is provided at e.g. supermarket check-outs on rush hours.

Excursus: EPC Network

Source: VeriSign

- Components
  - Electronic Product Code
    - to uniquely identify products (item-level)
  - Object Name Service
    - to discover distributed product-information
  - Physical Markup Language
    - to describe product, distribution channel, owner, environmental influences, ...

Andreas Krisch, European Digital Rights – www.edri.org
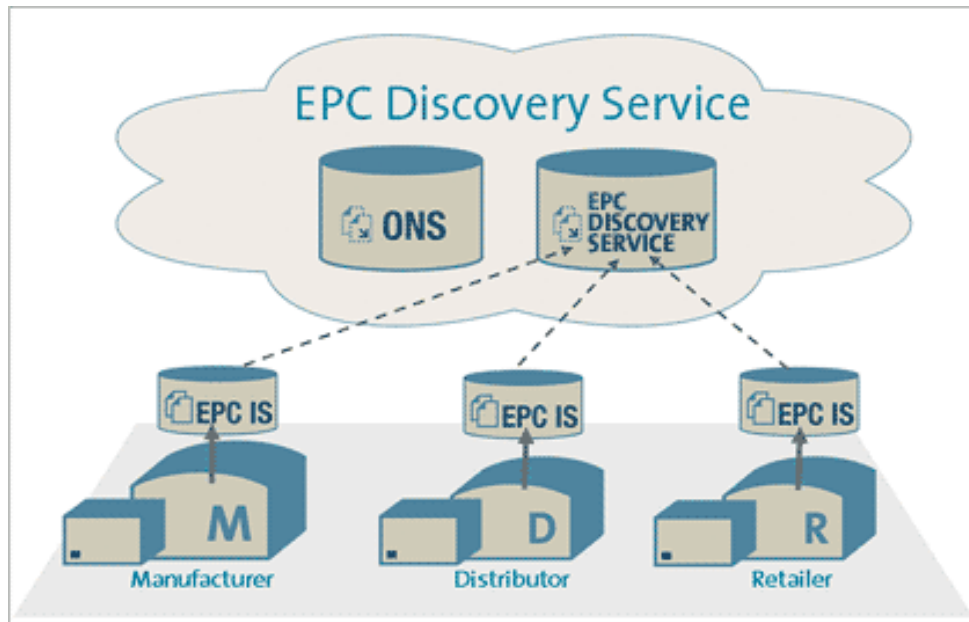
EDRi RFID & Informed Consent (5)

- Modification of RFID functionality
    - deactivation, "kill"
    - tag ceases to transmit any data
    - is said to need 4 x the reading time (-> too slow)
    - is said to be impractical in large quantities
    - option: RFID Zapper, destroying the tag

    - burden of deactivation must not be put on individuals

Andreas Krisch, European Digital Rights – www.edri.org

EDRi RFID & Informed Consent (6)

- Data alteration
  - some call it "disablement"
  - amount or accuracy of data on tag is reduced (e.g. alter unique identifier to product group identifier)
  - some information remains on the tag and is transmitted to readers
  - is said to be very expensive -> no large scale deployment
  - insufficient from a privacy point of view
  - EDRi asks to not support this as means of privacy protection and to avoid the term "disablement"

EDRi RFID & Informed Consent (7)

- Disablement
  - alter RFID functionality to temporarily not working
  - disabled tags transmit no data to readers
  - re-enabled by authorised party

  - is not available as of today, might be developed in future
  - might be a good means of privacy protection
  - might enable opt-in to **applications** rather than RFID in general
  - state-control by **authorised** party is key!

EDRi RFID & Informed Consent (8)

- Removal
  - technically simple
  - intuitive to do
  - 100% effective
  - tags have to be attached in a way that supports removal
  - currently the most practical, cheapest and most reliable option to protect individuals from unwanted RFID functionality.

EDRi RFID & Informed Consent (9)

- Responisibilities for RFID removal
  - opt-in requires distributors to be responsible
  - who introduces technology should be responsible
  - responsibility can be passed to others (e.g. from manufacturer to wholesaler to retailer ...)
  - RFID functionality has to be removed if the next link in the chain is unable / not willing to deal with it.
  - benefit: fits even for very small retailers
  - benefit: consistent with current article surveillance systems
  - benefit: meets common sense responsibility expectations

Opinion of the EDPS (1)

"In order to make the use of the concept of 'privacy by design' compulsory, the EDPS recommends that the Commission uses the mechanism of Article 3 (3) (c) of Directive 99/5/EC, in consultation with the RFID Expert Group."

Article 3 (3) (c) provides *"that the Commission may decide ... that apparatus ... shall be so constructed that they incorporate safeguards to ensure that the personal data and privacy of the user ... are protected."*

(Opinion of the EDPS on the RFID communication, pages 11, 16)

Opinion of the EDPS (2)

"The EDPS recommends considering the adoption of (a proposal for) Community legislation regulating the main issues of RFID-usage in relevant sectors, in case the proper implementation of the existing legal framework would fail."

(Opinion of the EDPS on the RFID communication, page 16)

Opinion of the EDPS (3)

"Measures should in any event:

- *lay down the opt-in principle at the point of sale as a precise and undeniable legal obligation, also for RFID applications that fall outside of the scope of the Data protection Directive.*

- *ensure the mandatory deployment of RFID applications with the appropriate technical features or 'privacy by design'."*

(Opinion of the EDPS on the RFID communication, page 17)

EC Proposal:
ePrivacy Directive amendment

"When such devices [note: e.g. RFIDs] *are connected to publicly available electronic communications networks or make use of electronic communication services as a basic infrastructure the relevant provisions of Directive 2002/58/EC, including those on security, traffic and location data and on confidentiality, should apply."*

(EC Proposal to amend the ePrivacy Directive, recital 28, p. 19)

Other Contributions

- JRC/IPTS: "RFID Technologies: Emerging Issues, Challenges and Policy Options"
  - 250 pages report on challenges and options
- Opinion of the European Economic and Social Committee on Radio Frequency Identification
  - "*The imperative need to preserve privacy and anonymity must be the core of the Recommendation by the Commission to the Member States.*" (page 13)
- Rathenau Institute: What do RFIDs tell about you? - A user perspective on Identity Management

Outlook 2008

- publication of recommendation on RFID
  - public online consultation soon to come
  - final recommendation before summer
- debate on RFID continues
- debate on "Internet of Things"
  - RFID, sensors, Internet, governance, trans-border flow of data, ...
- recommendation on "Internet of Things"
  - end of 2008 / 2009

References (1)

EU Online Consultation Report:
http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf

EU RFID Online Consultation Website: http://www.rfidconsultation.eu

Commission Decision on RFID Expert Group
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_176/l_17620070706en0

Members of the RFID Expert Group
http://ec.europa.eu/information_society/policy/rfid/doc/reg.pdf

Communication from EC "RFID in Europe: steps towards a policy framework"
SEC(2007) 312
http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf

EDRi RFID Privacy Issues (07.2007)
http://www.edri.org/docs/EDRi_RFID_Privacy_Issues_published.pdf

EDRi RFID Security Issues (07.2007)
http://www.edri.org/docs/EDRi_RFID_Security_Issues.pdf

EDRi RFID and Informed Consent
http://www.edri.org/docs/EDRi_RFID_Informed_Consent_published.pdf

References (2)

European Privacy Seal http://www.european-privacy-seal.eu/

Project Privacy and Identity Management in Europe
http://www.prime-project.eu/

Opinion of the EDPS on EC RFID Communication
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documen

Opinion of the European Economic and Social Committee on RFID
http://eescopinions.eesc.europa.eu/EESCopinionDocument.aspx?identifier=c
\ten\ten293\ces992-2007_ac.doc&language=EN

JRC/IPTS RFID Technologies: Emerging Issues, Challenges and Policy
Options http://ftp.jrc.es/eur22770en.pdf

EC Proposal for amendment of ePrivacy Directive
http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/6

Eu-funded research and development projects on RFID
http://ec.europa.eu/information_society/policy/rfid/doc/RFIDprojects.pdf

European Digital Rights

Thanks for your attention!

Andreas Krisch <andreas.krisch@vibe.at>

http://www.edri.org/

http://www.unwatched.org/

Thanks for your donations!

European Digital Rights AISBL

IBAN: BE32 7330 2150 2102

BIC: KREDBEBB