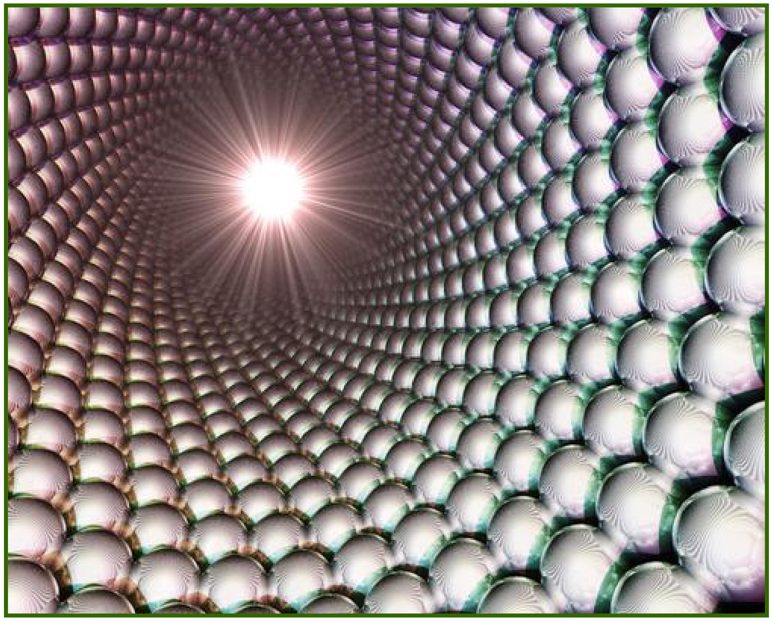


Considerations of privacy and data security in the context of RFID

European Commission Workshop on
“RFID Security, Data Protection and Privacy, Health and Safety Issues”
Brussels, Belgium
16-17 May 2006

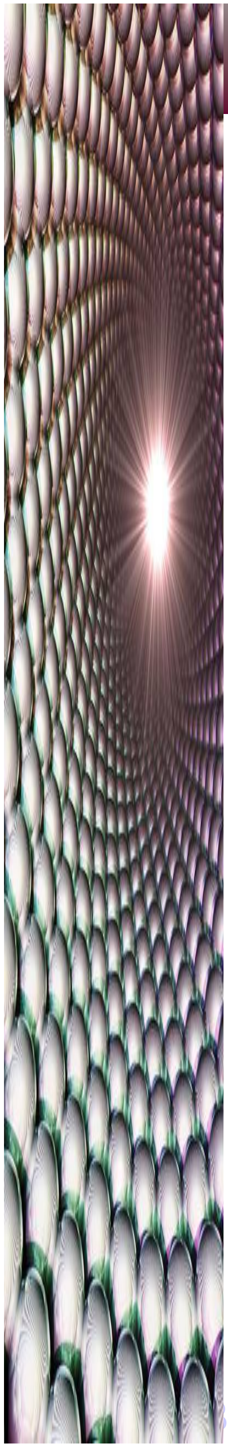
Lara Srivastava,
ITU New Initiatives Programme Director

The views expressed in this presentation are those of the author and do not necessarily reflect the opinions of the ITU or its membership.
Lara Srivastava can be contacted at lara.srivastava@itu.int

© ITU

Trends in today’s information age

- Trends in the ICT market point to the preponderance of radio technologies
- Tremendous growth of mobile cellular and wireless broadband networks
  - e.g. over 2 billion mobiles
- Importance of always-on access/ availability of communications and information anywhere, anytime
- technology is already “somewhat” ubiquitous

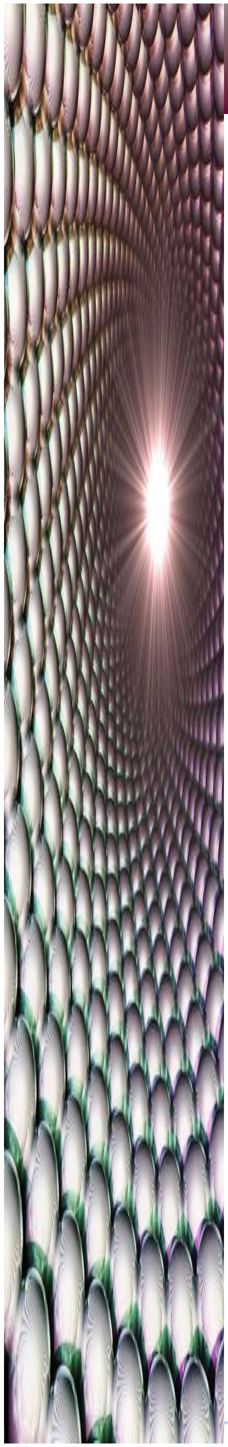


pervasiveness of radio

- terrestrial radio and cellular are the densest radio systems in the world
  - the ratio of radios to humans is nearing 1 to 1

  (e.g. Japan reports 100m radio stations - mobile phones, Wireless LAN, RFID tags…)
- start of a new era?
  - in which this ratio could exceed 1000 to 1
- thus, radios would exist all around us - becoming truly “ubiquitous”
- … they would radically transform the role of technology, making it ‘truly’ ubiquitous

© ITU

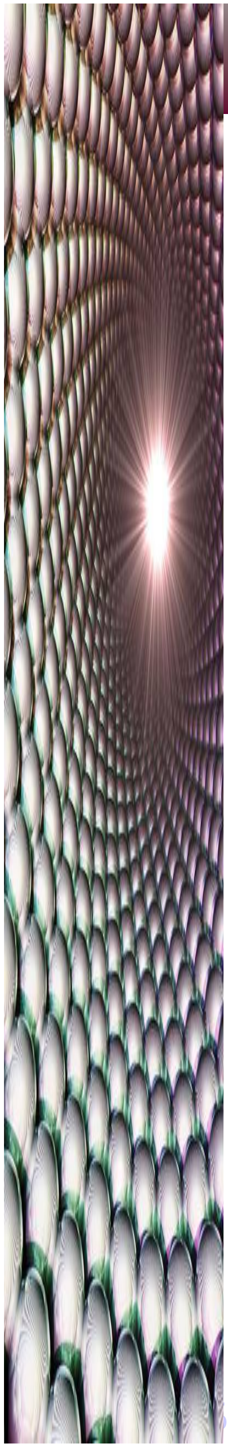


radio-frequency identification and the next internet

International Telecommunication Union
ITU Internet Reports 2005
The Internet of Things

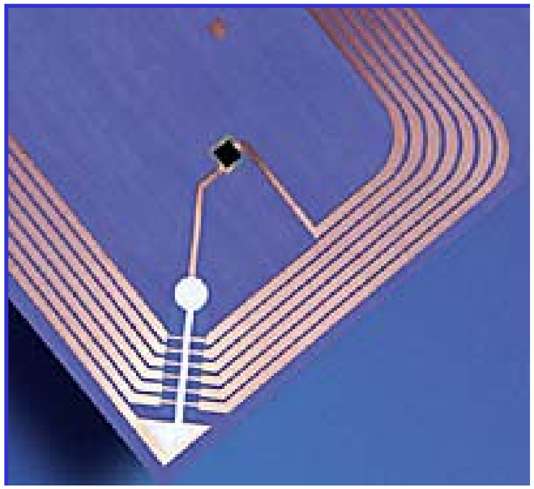
- anytime and anywhere connection by anyone can go further still through radio technology:
  - to include **“anything”…**
- i.e. the internet now connects computers & people to one another, but imagine if it could also connect computers to things
- creation of a “network of things/objects”…
  - giving each thing its own **“identity”** in cyberspace, allowing it too to ‘connect’
  - a whole new dimension: an **internet of things?**

© ITU

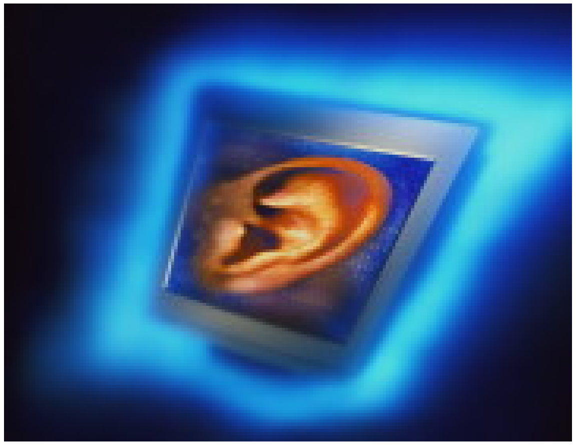


RFID at the core of the next internet - *the ubiquitous internet*

- RFID can wirelessly monitor objects in real-time, without necessarily having line-of-sight
- it can “locate” but also “track” items
- as such, RFID systems provide a sort of “map” of the real world in the virtual world
- in other words, RFID and related technologies are catalysts in the move to ambient networking & intelligence

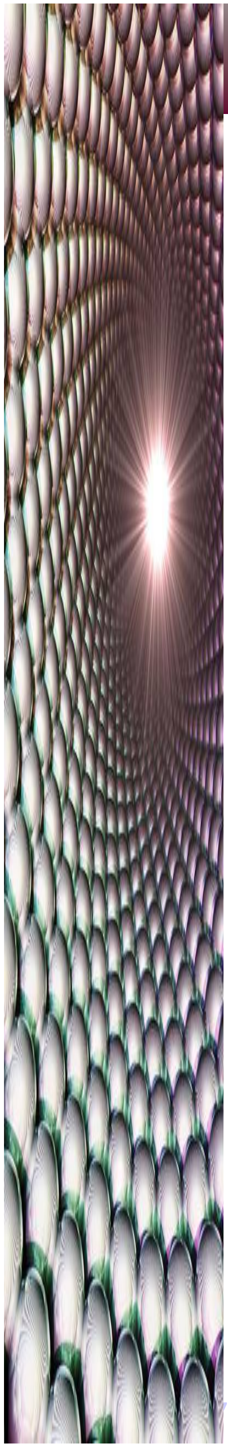


implications of RFID raises some concerns



- Who controls information on the tags?
- Who has access to it, and when?
- RFID deployments have been delayed as a result of such concerns
  - e.g. Benetton
- Public sector has now begun addressing this issue
  - e.g. EU Data Protection WP, Japan's RFID Guidelines

© ITU

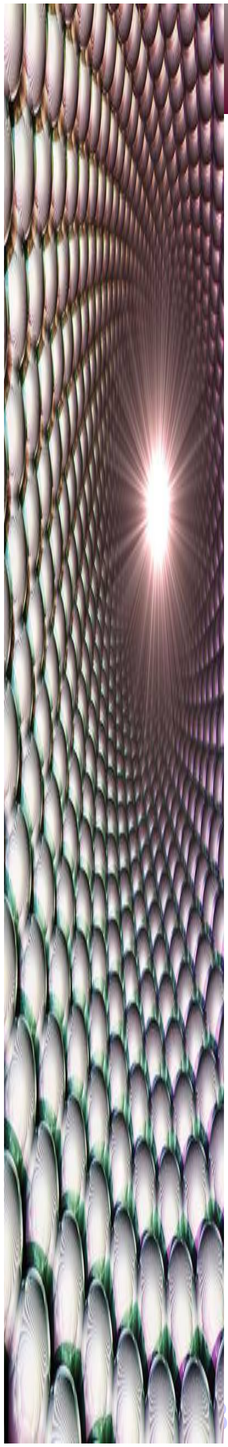


defining privacy in today's context

- privacy is a dynamic concept and is culturally and historically bounded
  - from the ID document, to surveillance cameras, to cookies…
  - Differences e.g. between US, China & EU countries

- privacy revolves around distinction between public & private spheres of human existence
- with new technologies, boundary increasingly blurring
  - internet, mobiles, GPS, digital storage capacity
- today, debate hinges on individual's ability to control the increasing "*permeability*" between private life and public life

© ITU



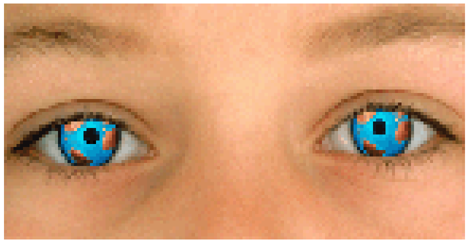
reasons to protect privacy

- despite cultural and historical relativity, the value privacy holds in most modern societies is likely to exist for some time to come
- in some cultures, privacy is seen as a human right and its principles have largely been codified in the industrialized world
- Compelling Reasons important to articulate
  - Privacy as **empowerment** *(to control information)*
  - Privacy as **utility** *(protects people against nuisance)*
  - Privacy as **dignity** *(in reciprocal obligations between parties)*
  - Privacy as **regulating agent** *(check and balance on power of data collectors)*

(Lessig)

privacy: a complex issue

- two facets to the right to privacy:
  - right to protect access to information about oneself
  - right to be free from interference
- user of today’s internet already fill in forms with false information, to preserve their “anonymity”
  - ubiquitous/ambient networking likely to exacerbate this climate of distrust



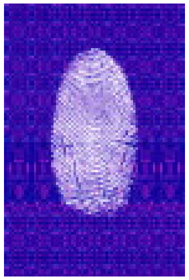
- thus, balance between privacy & convenience needs to be struck early in the design of technology, across several domains:
  - Technical, regulatory, industrial **but also** socio-ethical

© ITU

perceived privacy risks

- Right to **protect information**
  - – provision of personalized services require collection/storage of detailed personal data, preventing users from being anonymous
  - – … and allowing unauthorized 3rd parties to use data, or even facilitating criminal activity (e.g. identity theft via skimming)
  - – cybersecurity threats make data more vulnerable
- Right to **freedom from interference**
  - – spam is already an issue of grave concern
  - – with RFID, unsolicited messaging could be generated not only through mobiles and email, but also through everyday objects

© ITU

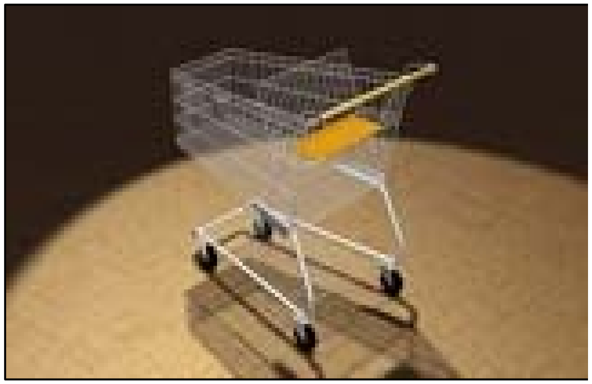


Balancing national security with privacy

- in the current climate of terrorism and national security concerns, pervasive nature of networks/data takes on a new dimension
  - identity documents becoming biometric and RFID records (e.g. Estonia, China, US, UK)
  - discussions under way for embedding radio tags in passports and currency
- care must be taken to strike a balance between national security and citizen privacy, between corporate security and the respect of the employee
- “surveillance” (real or perceived) impedes human creativity and dignity & discourages individuality and decision-making

© ITU

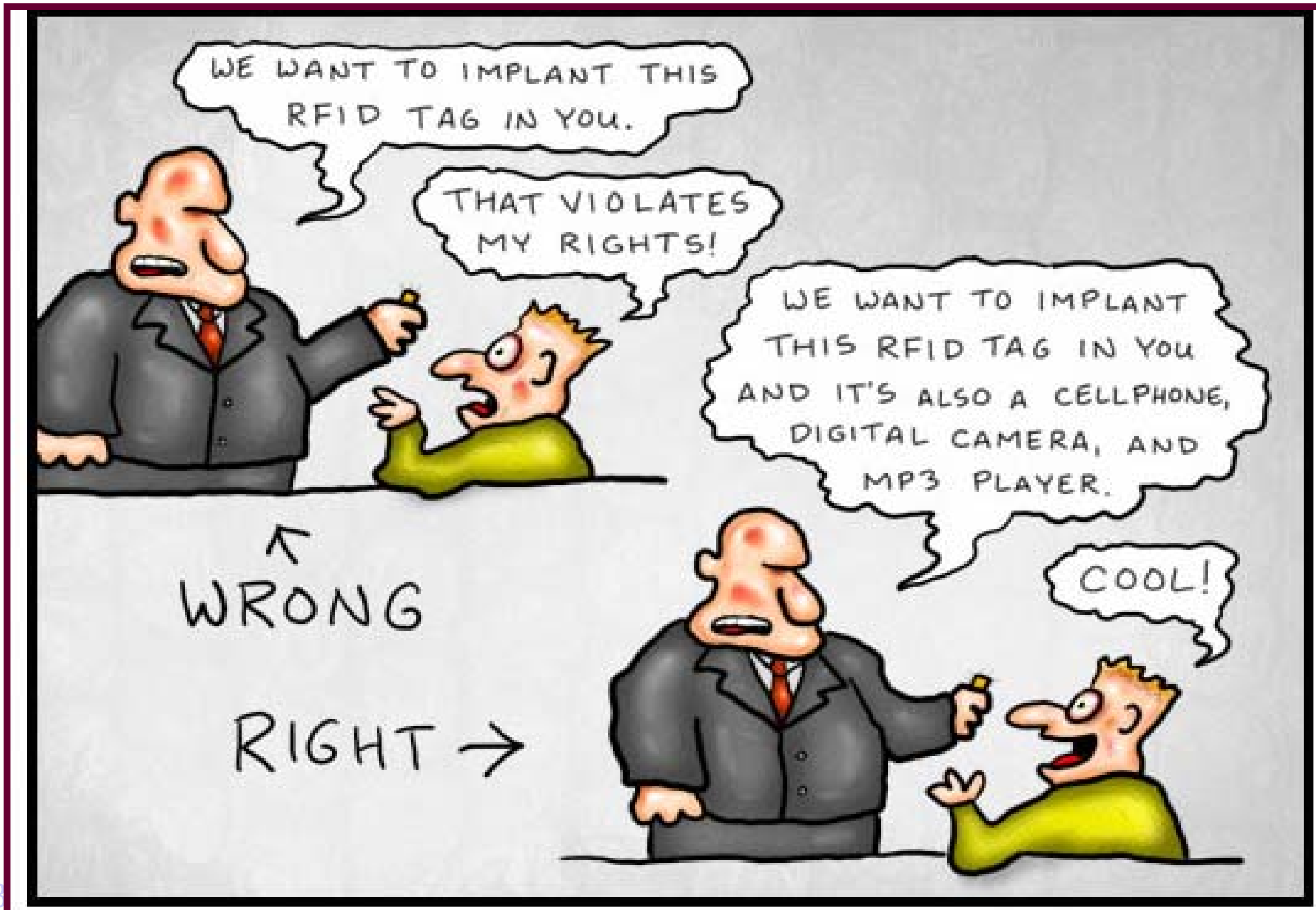
the risk of a privacy divide?



- the case of the supermarket loyalty card
  - if consumers allow stores to keep a record of their shopping habits, they pay less
- some anonymizers on the internet are also available at a premium
- privacy should not become a commodity available only at a financial premium (to those who can afford it)…

© ITU

… or at a premium related to the loss of convenience


WE WANT TO IMPLANT THIS RFID TAG IN YOU.
THAT VIOLATES MY RIGHTS!
WE WANT TO IMPLANT THIS RFID TAG IN YOU AND IT'S ALSO A CELLPHONE, DIGITAL CAMERA, AND MP3 PLAYER.
COOL!
WRONG
RIGHT

Copyright © 2006 David Farley, d-farley@ibiblio.org
http://ibiblio.org/Dave/drfun.html

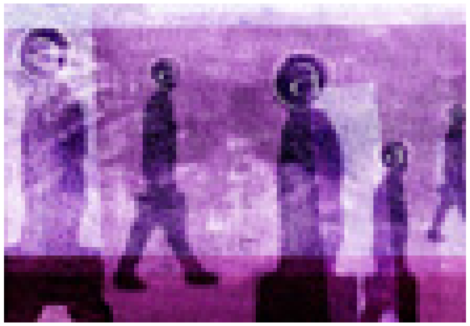
Japan’s RFID Guidelines

- build upon Japan’s “Law for the Protection of Personal Information” (57/2003)
  - they extend definition of personal information to record information on RFID tags, even if specific individual cannot be identified by that information
- currently, companies required to:
  - *inform consumers of purpose of data collection/use*
  - *obtain consumer consent*
  - *prevent leakage, loss and damage to information*
  - *ensure data accuracy and*
  - *appoint information administrator to be responsible for ensuring implementation of these measures & for consumer complaints*
- guidelines acknowledge rapid hi-tech innovation & evolution of privacy, and thus that guidelines will periodically revisited/updated

© ITU

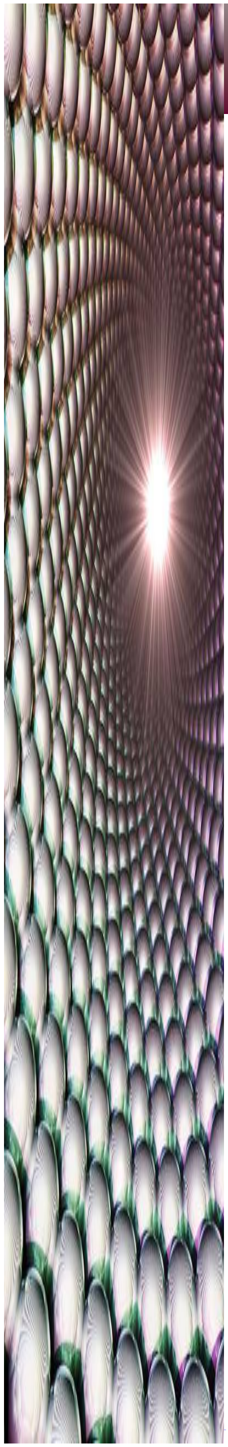
but what needs to be done goes further still …

- global dialogue between key players during deployment BUT ALSO design phase
- better understanding of the technology
  - what are the threats: hype vs. reality
- greater efforts in the design, standardization & implementation of PETs



- global effort towards digital identity management principles and tools
- intensive user education & awareness

© ITU



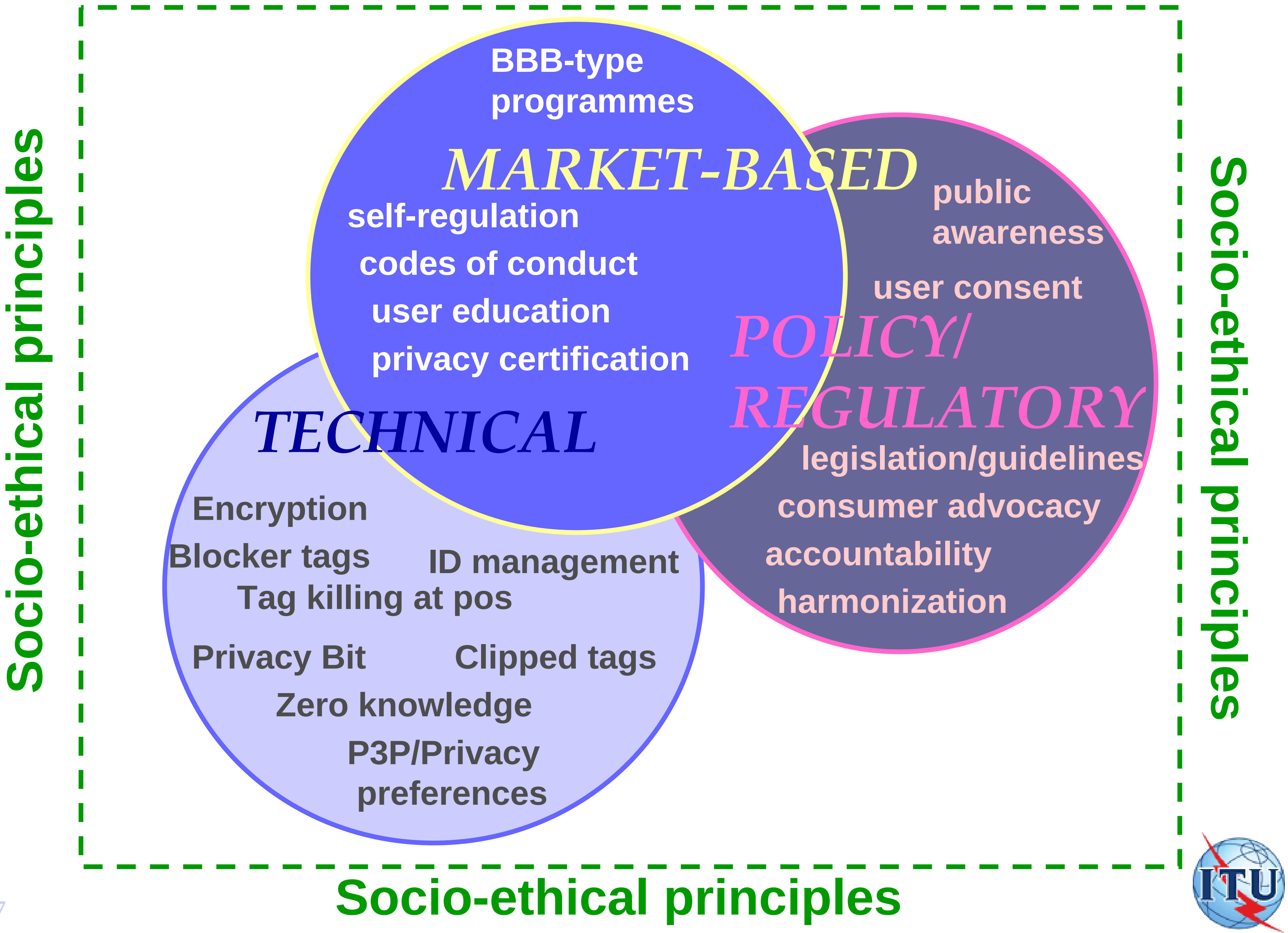
… further still, indeed, as technology lunges forward

- complementary technologies like sensors and wireless sensor networks are beginning to make their mark
- sensors without batteries are being developed, which could make them as ubiquitous as RFID tags
- however, sensors go further than RFID tags in that they can monitor the physical status of objects of people, e.g. temperature, weight, presence of bacteria, humidity, sound etc…
- this could lead to an even more sophisticated level of data collection in the future

ubiquitous network society

© ITU

Technical solutions alone do not suffice



MARKET-BASED

BBB-type programmes

self-regulation

codes of conduct

user education

privacy certification

POLICY/ REGULATORY

public awareness

user consent

legislation/guidelines

consumer advocacy

accountability

harmonization

TECHNICAL

Encryption

Blocker tags

ID management

Tag killing at pos

Privacy Bit

Clipped tags

Zero knowledge

P3P/Privacy preferences

Socio-ethical principles

Socio-ethical principles

Socio-ethical principles

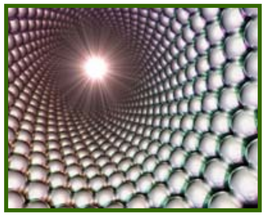
© ITU

coordination and collaboration at the international level is essential

- *dialogue, dialogue, dialogue*
- *development of harmonized approaches*
- *data protection schemes across borders*
- *infrastructure security initiatives*
  - *e.g. standards for RFID system security, cybersecurity*
- *articulation of global digital identity management principles (for people and things)*
- *governance issues*
- *….*

International bodies like the European Commission and the ITU (with its public sector and private sector membership) can play leading roles in these areas

© ITU



thanks!

They say that time changes things… but actually you have to change them yourself

-- Andy Warhol

The ITU New Initiatives Programme

visit us on the web at: **www.itu.int/ni**

lara.srivastava@itu.int

© ITU