# ICT and perspectives of privacy

**Dr. Asher Vaturi**

The Max Stern Yezreel Valley College

# Performance indicators for Indoor and outdoor environment built areas

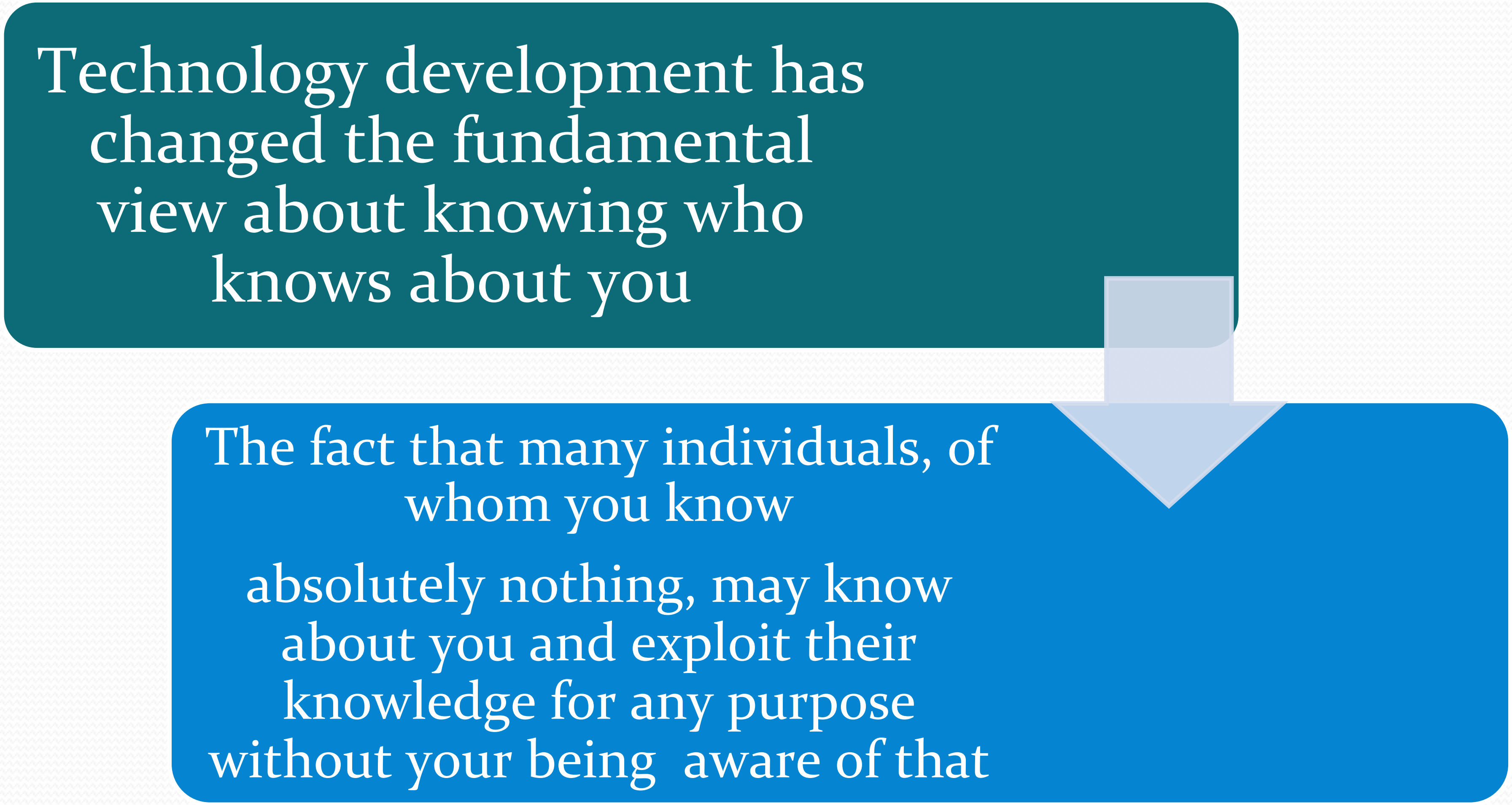
Concern about the overall quality of the indoor environment

We focus on issues such as comfort, health and safety (security), but also accessibility, positive stimulation of people and sustainability

In this sense, privacy relates to safety but also comfort and positive stimulation of people

MANAGING INDOOR ENVIRONMENT QUALITY
Learn how to deliver high quality, productive workplaces.
ORDER YOUR COPY NOW

# Technology and privacy



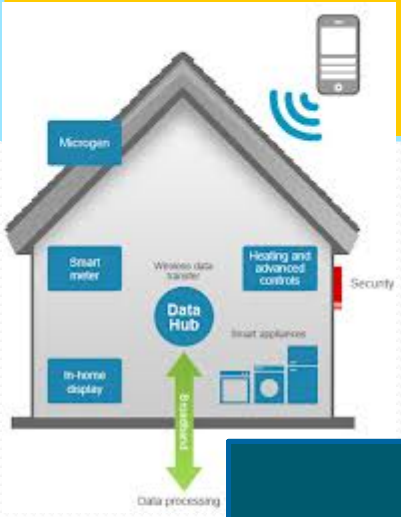
Technology development has changed the fundamental view about knowing who knows about you

The fact that many individuals, of whom you know

absolutely nothing, may know about you and exploit their knowledge for any purpose without your being  aware of that

# The century of “smart”

Smart metering



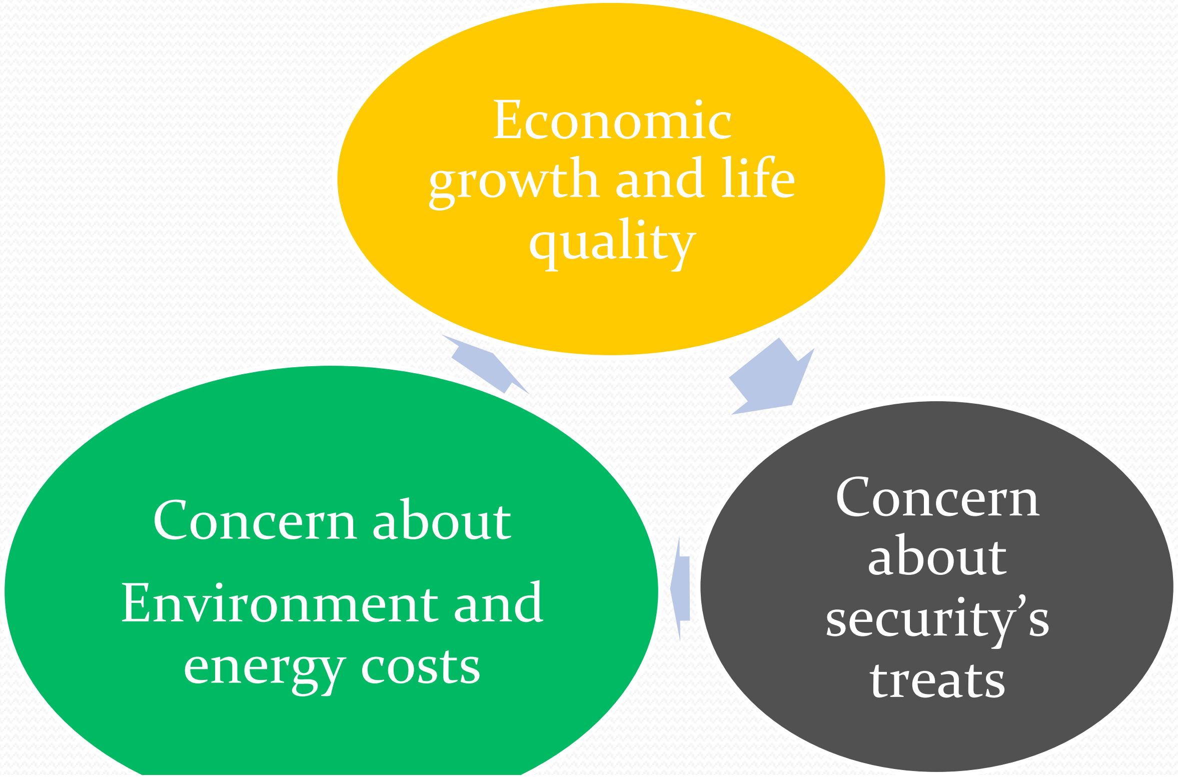
Smart cities

Smart homes

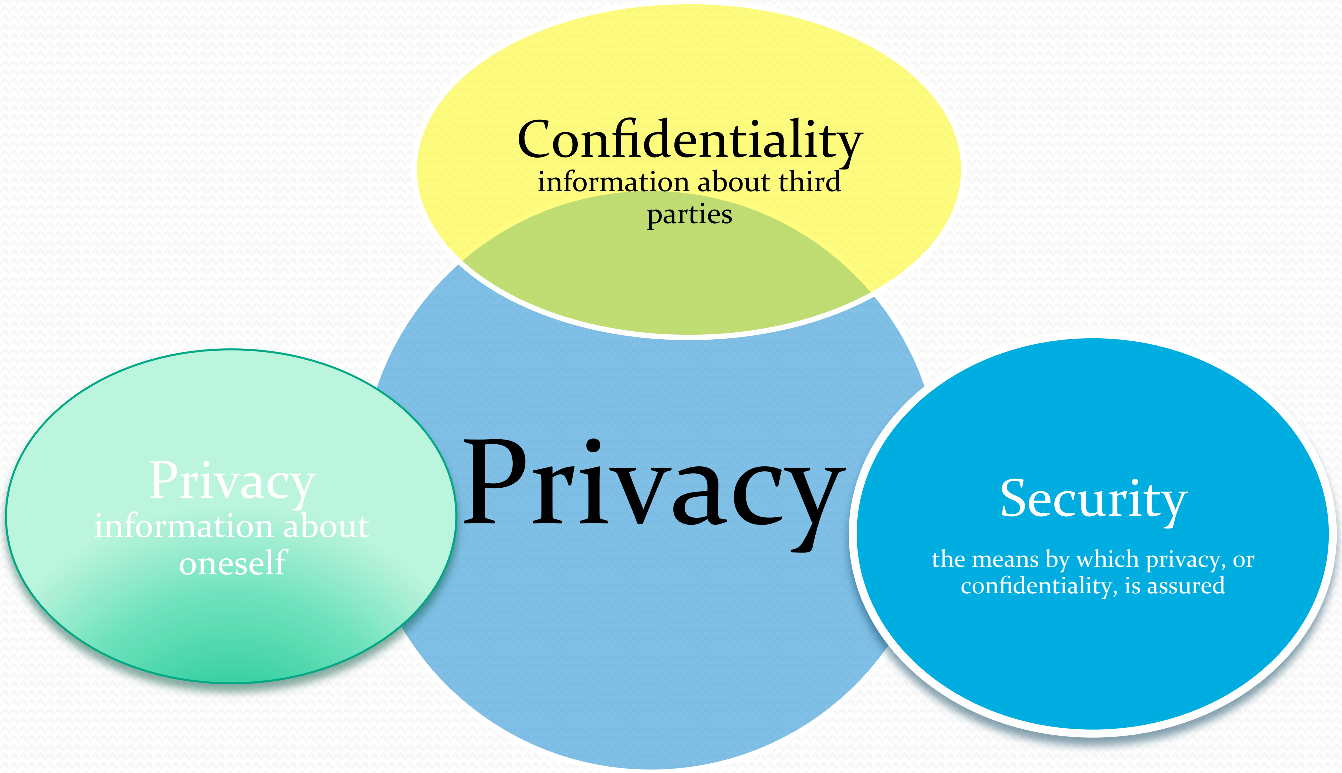
AUTO CURTAIN
HOME ENTERTAINMENT
COMMUNICATION
MOODS
HOME AUTOMATION
GARAGE
AUTO SPRINKLERS
AUTO LIGHTING

# Motivation of tech development in this century

While in the past, military, space, and health technologies have been driving forces, with spin-offs to the consumer market, today:


Economic growth and life quality
Concern about security's treats
Concern about
Environment and energy costs

# Perceptions of privacy



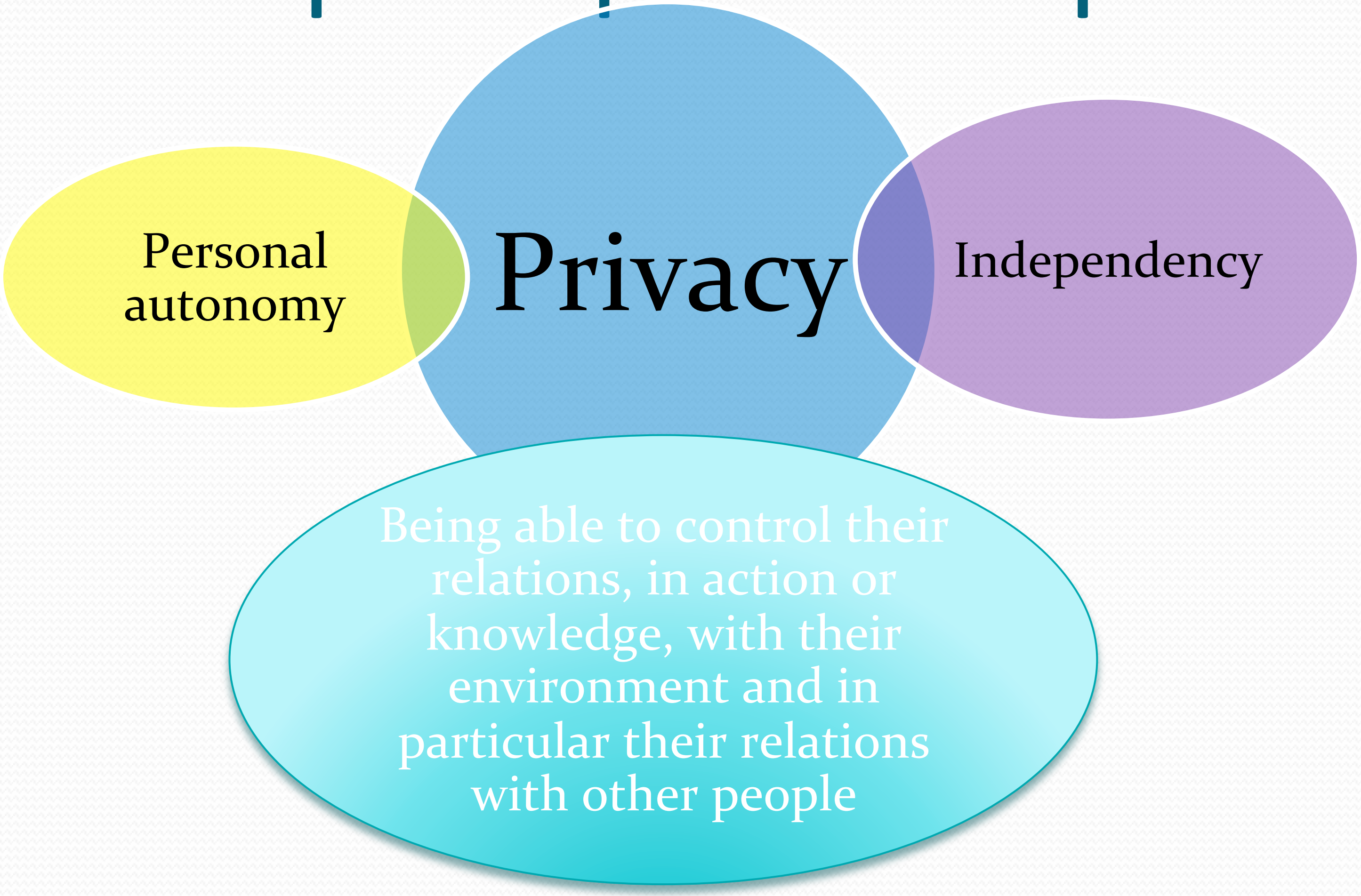
Confidentiality
information about third parties

Privacy
information about oneself

Privacy

Security
the means by which privacy, or confidentiality, is assured

# Other perceptions of privacy



Personal autonomy

Privacy

Independency

Being able to control their relations, in action or knowledge, with their environment and in particular their relations with other people

# The vision of the study

The motivation of the study is the vision of a society that is fully aware of the evolving challenges to privacy posed by emerging technologies and which is equipped to respond to them

# Goals of the study

- To evaluate is about the impact of modern especially emerging technologies, and specifically information technology, on individual privacy
- To suggest means of controlling the potential risks to privacy while getting the maximum benefit from emerging technologies

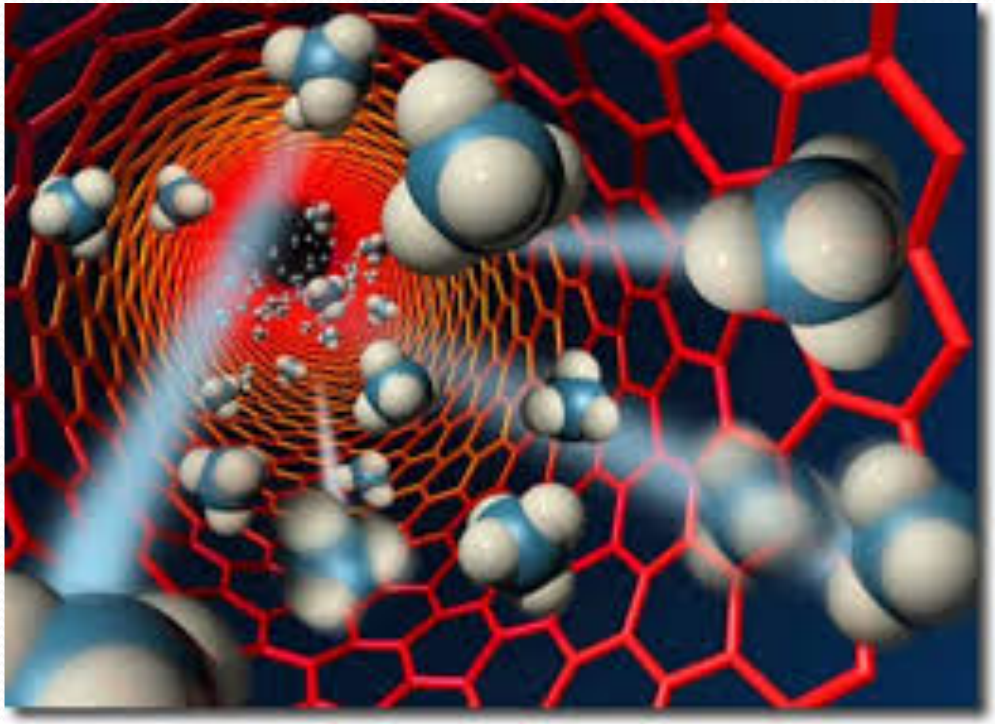
The results are based of EU , FP7 research project PRACTICE

# Expert's survey

- In part A the respondents were asked about personal details
- The possible answers regarding the respondent's "main area of interest" were the five technology areas considered in the survey: Medicine Biology and Biometrics, Nanotechnologies and New Materials, Robotics, Cognition, and Information and Communication Technologies (ICT).
- In part B the respondents were requested to choose a technology from a menu, and then to answer several questions about the specific technology: the foreseen time-frame of its widespread use, its threat to privacy, its influence on changing people's sensitivity about their privacy, and its possible ability also to contribute to privacy enhancement.

# Nanotechnology and New Materials

Nanotechnology has the potential to reduce the size and improve the sensitivity of surveillance equipment, as well as to increase the computing power and storage capacity of electronic devices



# Nanotechnology and New Materials

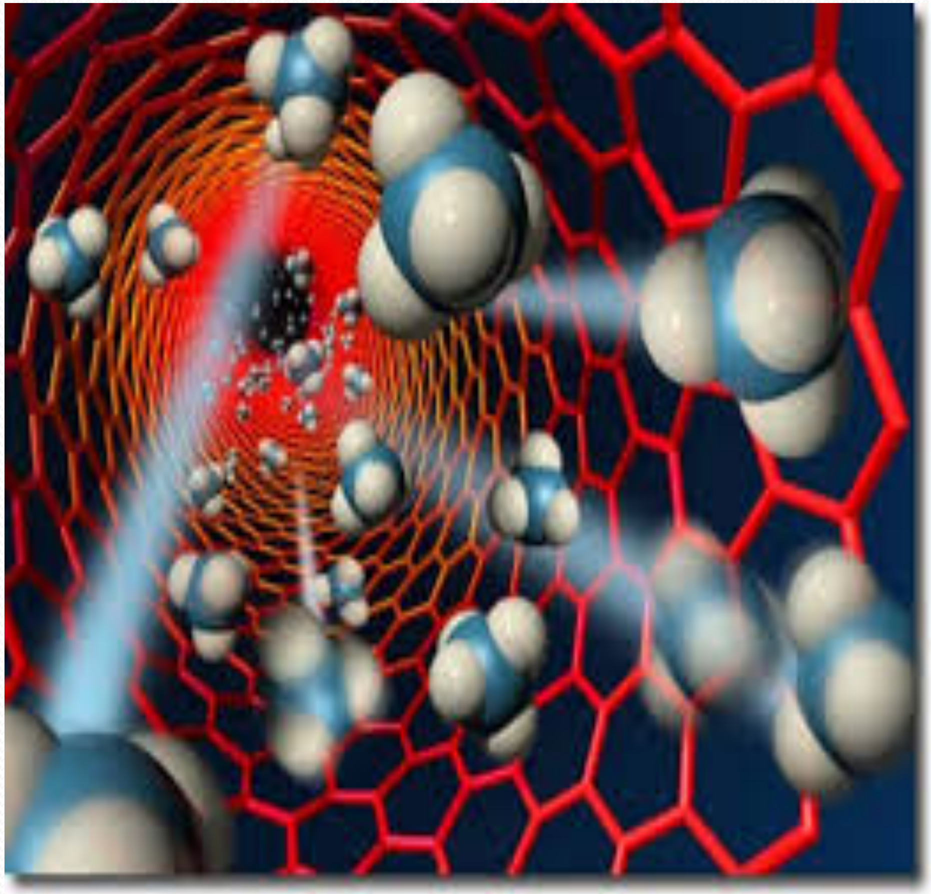
**Threats:**

Nanosensors will be able to spy where a person has visited recently, by sampling environmental clues on clothes – without the person's permission

**Privacy enhancement:**

If nanosensors are much more accurate than any other detector, and produce much fewer false positives

Hence, If properly used by law-enforcement, advanced nanosensors could protect privacy by curbing arbitrary collection of information irrelevant to a legitimate interest.



# Nano-enabled personalised medicine

Nano-enabled instruments and devices (e.g. cantilevers, quantum dots, various sensors) provide better diagnostic information about a person's genetic characteristics.

**Threats:**
Collecting and storing vast amounts of personal medical information in large centralized systems is a threat to privacy. The ability of various nanodevices to provide molecularly-precise genetic information raises concerns about becoming "molecularly naked" in front of insurance companies and other interested parties

# Portable Full Genome Sequencing (FGS)

Current technologies that produce complete DNA sequence of a person are provided by high tech laboratories, at considerable prices, and the data privacy policies are taken in account. Very small amounts of biological material, such as a hair with its follicle, a drop of saliva, or few epithelial cells, are sufficient for FGS.

The misuse of this kind of technology could result in genetic data of people being unwillingly made available to interested bodies such as medical insurance companies, and used by them to the detriment of those people, or for genetic blackmailing.

# Unobtrusive authentication using activity-related and "soft" biometrics

- The technology will provide new capabilities in biometric authentication (developed for security purposes): the extraction of multi-modal biometric signatures (e.g. gesture, gait, body dynamics, sound) based on the response of the user to specific stimuli, while performing specific but natural work-related activities.

# ICT:**Radio-frequency identification (RFID)**

- RFID —tags || , or microchips with antennas, allow the automatic identification and localisation of objects and persons using radio waves. Data collection and their registration become possible.

Treats

- A seamless, global network of electronic scanners will be able to scan radio tags in a variety of public settings, identifying people and their tastes and instantly sending customized ads. RFIDs embedded in the walls and appliances in "smart homes" will be able to inventory possessions, record eating habits, monitor medicine cabinets, and report data to marketers.

# Photonic sensing based on ultra low cost electro-optical components

- This technology will enable detection and authentication of objects by a single cheap sensor.
- **Threats:**
- Cheap surveillance systems used by unauthorised persons. The possibility to deploy large numbers of such systems will be instrumental for "total clandestine surveillance" of public areas, not only by rich, governmental bodies, but also by criminal or terrorist groups.

# Sensors for robots

- Sensors play a major role when the potential impact of robots on privacy is to be determined. Robots can be equipped with every sensor available. **Vision sensors mounted can be used to visually spy a person**

**Threats:**

- The mere presence has the potential to interrupt solitude and create the subjective feeling of being observed and evaluated

  Vision sensors can be used for video surveillance, acoustical sensors for eavesdropping, ultrasonic/laser sensors can be used to map the home of an observed person, radar sensors can be used to control people‘s movement, and gas measuring sensors might be used to observe the presence of a person

# Advanced speech recognition

- This technology converts a speech signal into a text message – ideally disregarding the environment. The capability to extract natural language has already been achieved; the future objective is to extract the emotional state behind speech

**Threats:**

- The threat to privacy imposed by AI systems for speech recognition could be the analysis of the subtext of speech. Whereas until today the spoken word has been what counts and the ‗meaning' is the most intimate, this technological advancement would radically change the notion of public and private and impose a threat to privacy.

# Online behavioural targeted advertising

- Online behavioural targeted advertising is the placement of adverts online based on the user‘s online behaviour. For instance, if an internet user has recently visited a site for male fashion and read some sports sites, it might be assumed that this user is a man, thus enabling advertisers to supply adverts that are targeted at men.
- There are two main kinds of threat. The first is that data is collected about us that we have no control over or knowledge about, and that it is used for purposes that we are equally uninformed about.
- The second, is that behavioral targeted advertising constitutes manipulation of the surfer.

# Overall results

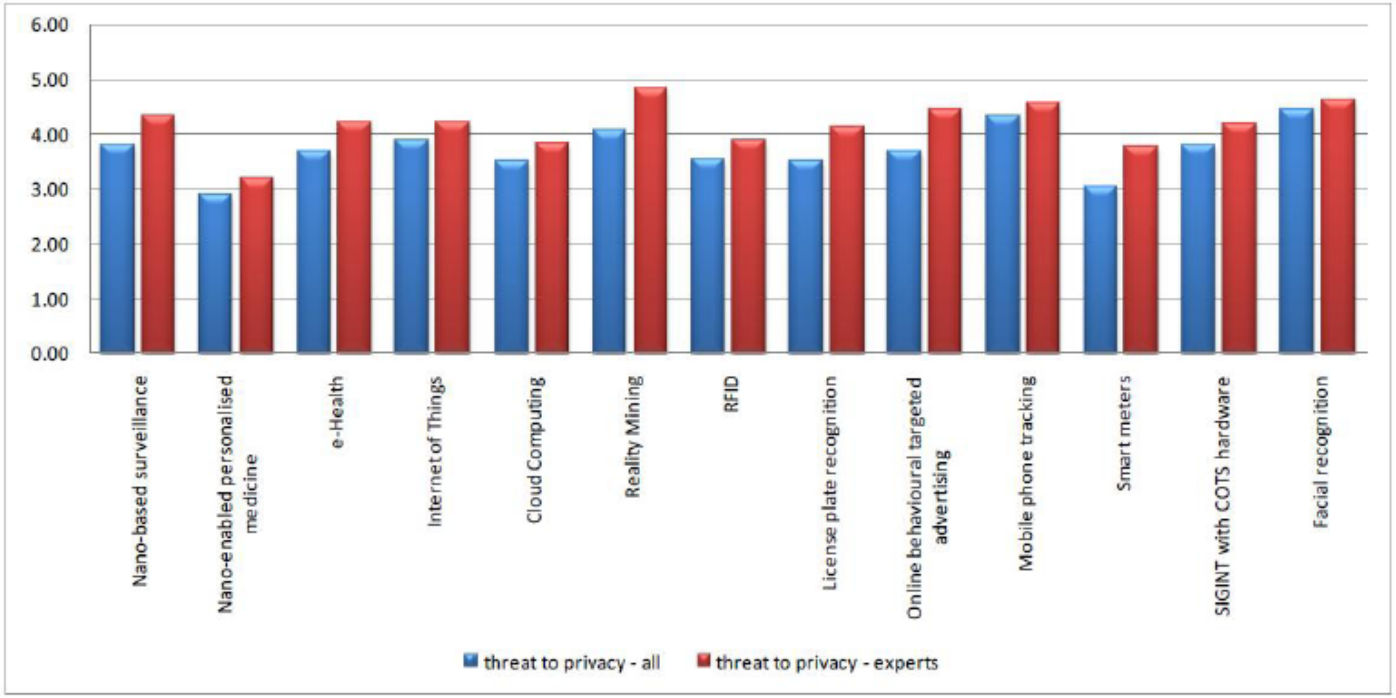


**Fig. 4.8: Threat levels estimated by participants with high expertise in privacy vs. all responses**