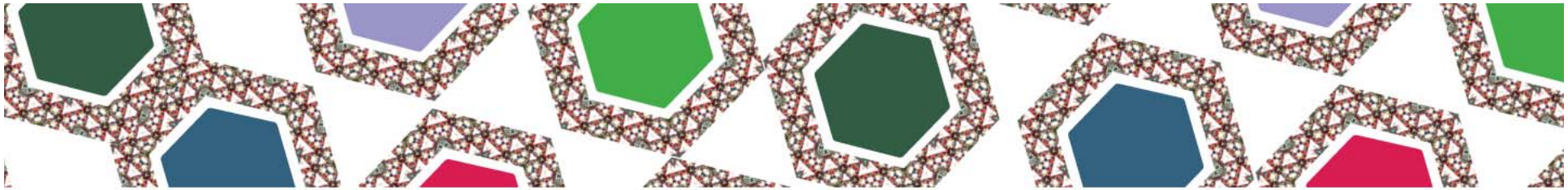


ITU Kaleidoscope 2013

Building Sustainable Communities

Security technologies for the protection of critical infrastructures – ethical risks and solutions offered by standardization

Simone Wurster
Chair of Innovation Economics
Berlin University of Technology, Berlin, Germany
simone.wurster@tu-berlin.de

Critical Infrastructures

‘all physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of the government in a country’ [5]

Pictures: fotolia.com

Security

‘a system of measures, including their embodiments and their interactions, designed to ward off intentionally destructive activity resulting in injury or material damage’ [10]

Two kinds of security

- security of society (public security)
  - security of the citizens
  - security of infrastructures and utilities
  - border security
  - restoring security and safety in case of crisis
- information and communication technology (ICT) security [6]

Security of Society

‘protection against criminal and terrorist attacks, natural disasters, pandemics and major technical accidents’ [6]

Privacy

- ‘The condition of being protected from unwanted access by others – either physical access, personal information, or attention‘ (Bok, 1982)
- Principle privacy-related rights
  - Universal Declaration of Human Rights (UDHR)
  - Regional example Europe: in addition EU Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)

Protection of Critical Infrastructures

Privacy ⟷ Security

- Fulfilling both goals bears specific challenges
- Specific standards may offer solutions

Privacy issues of security technologies [1], [7], [9], [12], [13]

- Many security solutions bear ethical risks [1]:
  - "unseen, uncontrolled or excessive surveillance activities (...) pose risks that go much further than just affecting privacy. They can foster a climate of suspicion and undermine trust”
- There has been no scientific work which investigates standardization related to privacy issues of security technologies so far.

Privacy issues of security technologies [1], [7], [9], [12], [13]

Three kinds of civil security-specific settings can be distinguished [20]:

- private places
- public places
- semi-public places (airports, train stations, ports etc.)

Pictures: fotolia.com

Semi-public areas

- Many semi-public areas represent critical infrastructures and are used by millions of people every day worldwide.
- Security has great importance.
- Specific privacy-related recommendations are missing.

Standards

‘document(s), established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context’

(ISO/IEC Guide 2 "Standardization and related activities - General vocabulary”)

Advantages of Standardization (selection) [2], [3], [4], [11]

- Access to global market for innovative solutions
- Economies of scale, cost savings
- Facilitation of compatibility and interoperability
- Raises acceptance of innovations among customers and public procurers

Survey in the German Security Research Program (2011, 2012)

- Survey in Summer 2011 on standardization needs [8])
- Summer 2012 follow-up study to gain insight into ethical and privacy-related problems of security technologies
- 23 participants:

  from supplier companies of security-related products and services, from research organizations, from universities, from an industry association and people representing the end user

Survey in the German Security Research Program: Results

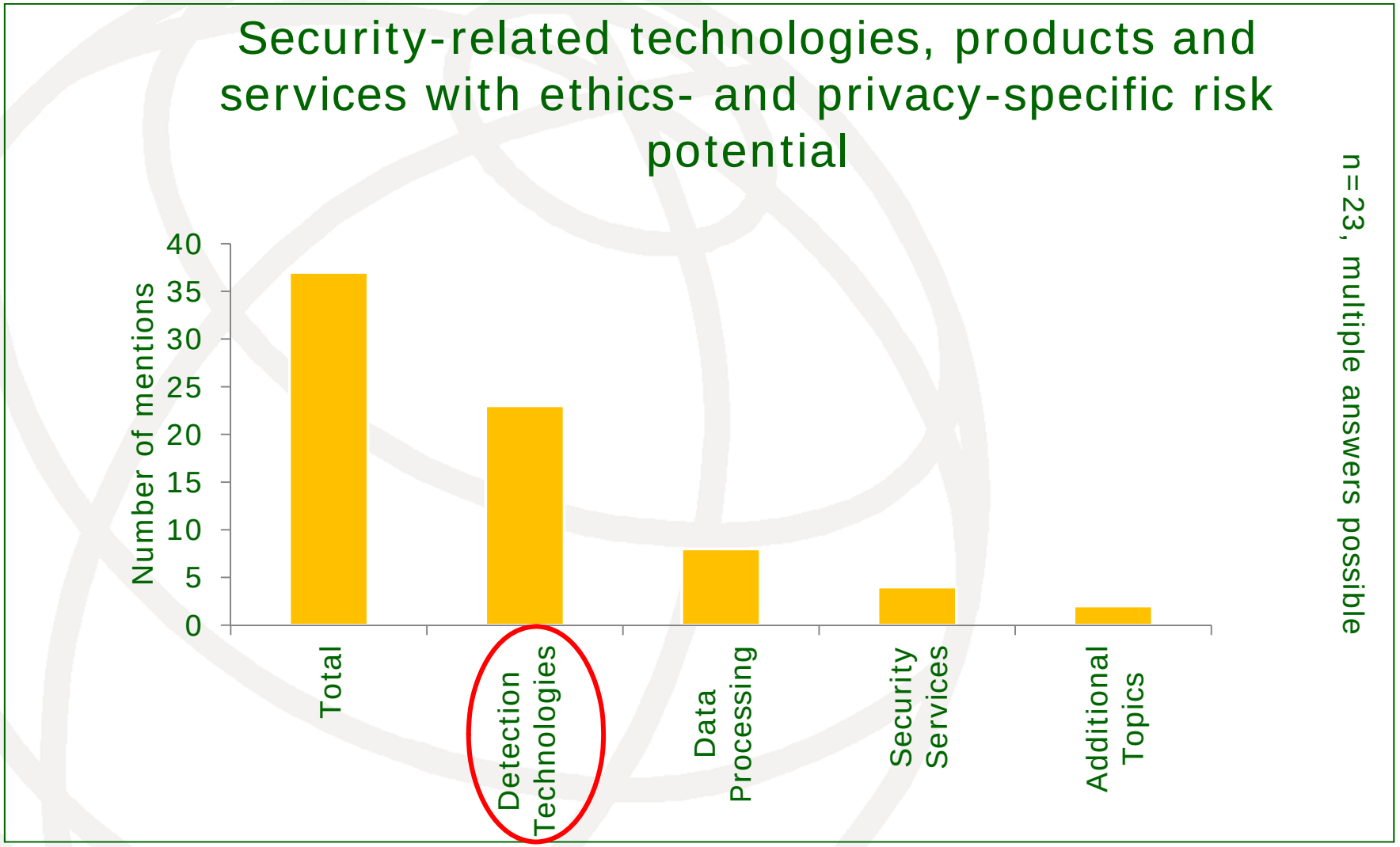
Six of ten questions were related to ethical and privacy-specific risks of security technologies:

1. What security-related technologies, products or services bear special ethical or privacy-specific risks in your opinion?
2. Please use up to five of the described technologies, products or services to rank their risk potential.
3. Please name ethical and privacy risks of the top-ranked technologies, products or services.

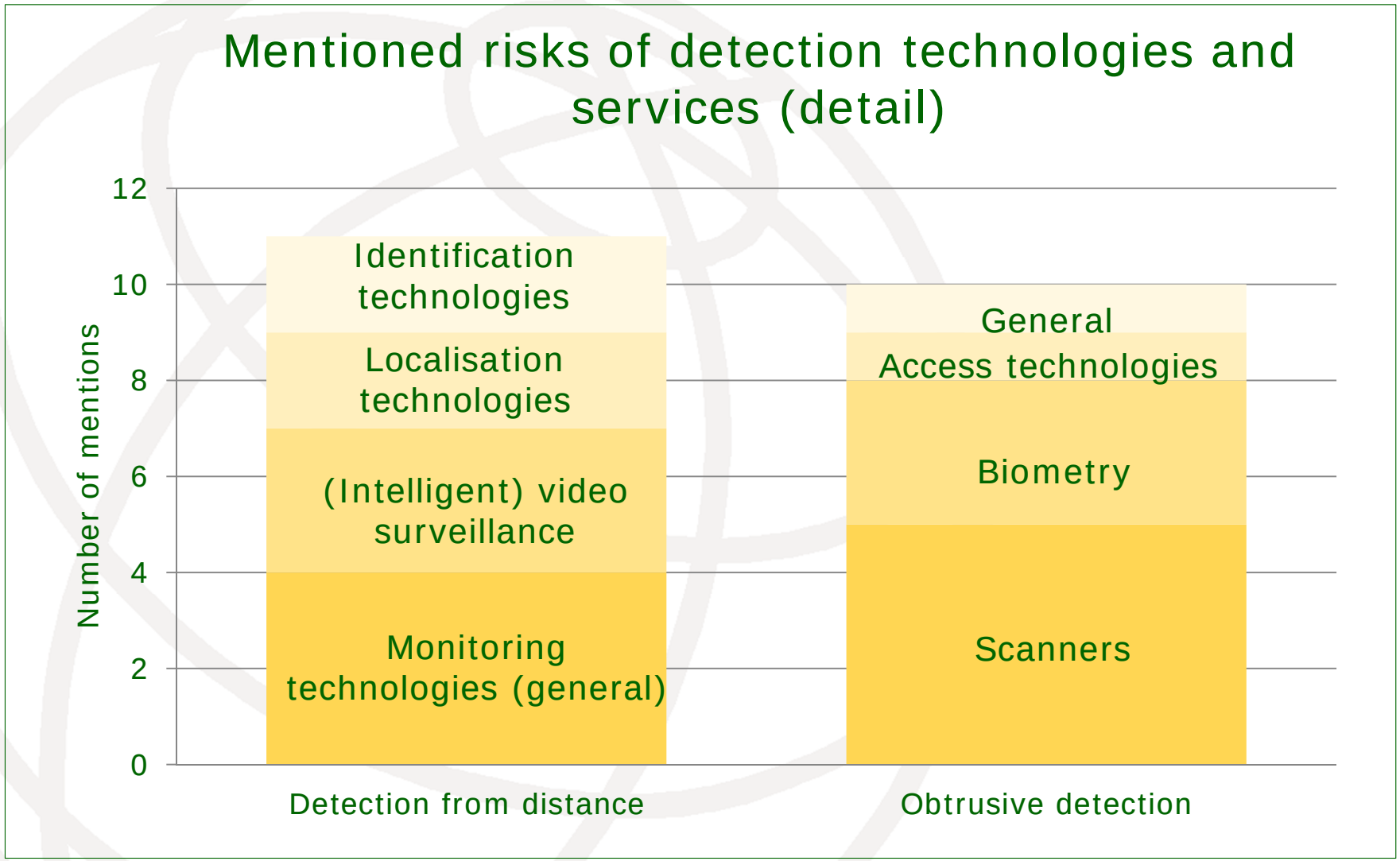
Survey in the German Security Research Program: Results

4. What other ethical and privacy-specific risks are important with regard to other security-related technology, products or services from your point of view?
5. In what way is there a need for standards for better addressing ethical and privacy specific aspects in the development and use of security related products and services from your point of view?
6. Which technologies, products and solutions have specific standardization needs to reduce ethical and privacy risks?

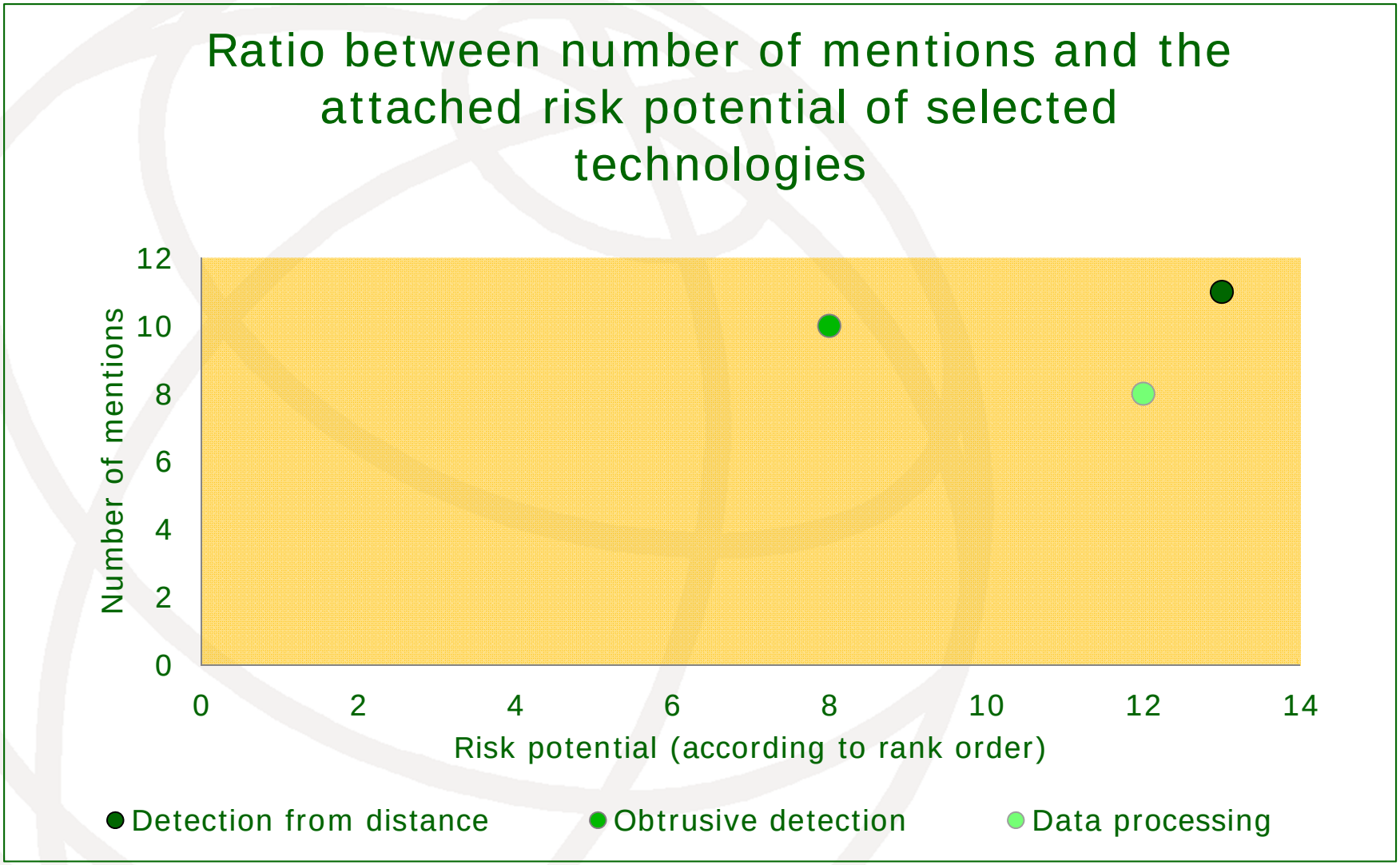
Survey in the German Security Research Program: Results



Survey in the German Security Research Program: Results



Survey in the German Security Research Program: Results



Survey in the German Security Research Program: Results

Overview of potential ethical risks of the first-ranked technologies, products and services

Restricted freedom

- Interference with privacy
- Identification of individuals
- Data mining / ~ analysis, profiling
- People tracking
- Lack of confidentiality
- Lack of legitimacy
- No consent
- Lack of proportionality

Abuse

- Abuse in general
- Voyeurism

Discrimination

- D. in general
- Motion-based profiling
- Data mining / data analysis, profiling

Survey in the German Security Research Program: Results

General recommendations on the need for ethical standards for security technologies:

- Integration of privacy topics into standards in general
- Certifications for ethic-friendly security products
- Better information of the public regarding security measures and the use of detection technologies and formulation of their rights

Survey in the German Security Research Program: Results

Technology fields to reduce ethical risks:

- Data storage
- Video surveillance
- Biometrics
- Access control
- Sensors
- Security services

Pictures: © iStockphoto, biometrie.eu, airportsinternational.com

Standardization to reduce ethical and privacy-specific risks in Europe

Important foundation: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data

- will be displaced -> General Data Protection Regulation (GDPR)
- implementation expected 2015 or later
- current version of the GDPR offers no guidelines for specific technologies

Several CEN Workshop Agreements

- voluntary adoption in Europe
- examples: CWAs 15292, 15499, Part I & II, 16113

Standardization by the international ISO / IEC Committee JTC 1

- Fokus of JTC 1: information technology
- Specific Sub Committee (SC): SC 27, Work Group (WG) 5 Identity Management and Privacy Technologies
- Several privacy standards, e.g. ISO/IEC 29100
- Several standardization projects related to p. impact assessment, p. information management systems & p. architectures

Privacy principles of ISO/IEC 29100, developed by ISO/IEC JTC 1 SC 27

1. Consent and choice
2. Purpose legitimacy & specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclose limitation
6. Accuracy and Quality

1. Openness, transparency and notice
2. Individual participation and access
3. Accountability
4. Information security
5. Privacy compliance

The permanent protection of semi-public areas is not covered!

European and international documents regarding public security and privacy

- European Example: CWA 16113 Personal Data Protection Good Practices
- International Example: ISO/IEC 15944-8 Information technology -- Business Operational View -- Part 8:
  - *Identification of privacy protection requirements as external constraints on business transactions* pay specific attention to privacy in the context of public security

Specific documents for data storage and sensors

- Data storage
  - e.g. EN 15713, ISO/TR 15801, ISO/TS 21547
  - no recommendations for specific storage periods
- Sensors
  - ethical aspects are not represented appropriately in current sensor-specific standards
  - specific privacy topics: sensor tunnels, wireless sensor networks, sensor data fusion

Specific documents for video surveillance

CWA 16113

- a few principles

ISO 22311

- monitoring access to the data
- a mandatory storage time and an appropriate deletion of data after a relevant period
- training of staff in dealing with sensitive data
- 'It is recommended to implement as for as possible privacy specifications published by ISO/IEC JTC 1/SC 27.'

Pictures: www.airportsinternational.com
www.boschsecurity.com

Specific documents for video surveillance

- Risks regarding intelligent video surveillance:
  - Technical principle: combination of video elements, application of data analysis methods and data storage.
  - Compared to traditional forms of CCTV, intelligent video surveillance systems only document detected events that deviate from the "act normal.“
  - Risks of abuse, discrimination risks and possible intimidation effects ([12]).
  - Risks are not covered by current standards.

Specific documents for biometrics

- ISO/IEC 19784-2
- ISO/IEC 19785-1
- ISO/IEC 19792
- ISO/IEC 24745
- ISO/IEC TR 24714-1
  - 14 state-of-the art privacy guidelines
  - no specific applications for the protection of critical infrastructures, public and semi-public areas and the specific use of data in these contexts

Pictures: www.biometrie.eu

Specific documents for access control and security services

- Recommendations regarding privacy issues of **access control** need to be investigated in more detail.
- Private **security services** are no specific topic of the development of security technologies.
- Fundamental ethical issues regarding airport security services are for example in Europe covered by the standard *EN 16082*.

Privacy-related certificates

- Their development is not impossible.
- Example: EuroPriSe
  - certifies that an IT product or IT-based service is compliant with European regulations on privacy and data protection.
- Similar projects, particularly in the fields of CCTV, physical privacy and obtrusive detection are desirable.

Six new working items for new standards

1. A privacy standard for the protection of (semi-public) critical infrastructure, particularly airports and ports

Pictures: fotolia.com

2. General definition of the kind of data stored for security reasons and of specific storage periods when there is no specific suspicion
3. Matching of data

Six new working items for new standards

4. Use of biometric data in the context of public security
5. Ethical standards for sensors
6. General requirements for the processing of video data, the storage period and the deletion when there is no specific suspicion

Pictures: © iStockphoto, airportsinternational.com, biometrie.eu

Future work

- Volunteers are needed in the different countries to start new standardization projects.
- BUT standardization alone does not guarantee the realization of specific privacy-related requirements.
- Appropriate certification schemes and procedures are necessary to ensure the implementation of the desired levels of privacy.

References

[1] Article 29 Data Protection Working Party (2007). Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law. Enforcement, Customs and other Security Authorities http://www.dataprotection.ro/servlet/ViewDocument?id=227.

[2] Blind, K. (2004). The Economics of Standards: Theory, Evidence, Policy. Cheltenham 2004.

[3] Blind, K. (2008). Standardization and Standards in Security Research and Emerging Security Markets. Fraunhofer Symposium 'Future Security', 3rd Security Research Conference Karlsruhe, 2008, 63-72.

[4] CEN/CENELEC WG STAIR (2011). An Integrated Approach for Standardization, Innovation and Research. ftp://ftp.cencenelec.eu/PUB/ /Brochures/STAIR.pdf.

[5] European Commission (2004). Critical Infrastructure Protection in the fight against terrorism (COM/2004/0702). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:HTML.

[6] European Commission (2011). Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards. ftp://ftp.cencenelec.eu/CENELEC/EuropeanMandates/M_487.pdf.

[7] Hempel, L., Toepfer, E. (2004). CCTV in Europe. Final Report. Urbaneye Working Paper No. 13 (August 2004).

References

[8] InfraNorm (2011). Bedeutung von Sicherheitsnormen, -standards und -spezifikationen. http://www.inno.tu-berlin.de/fileadmin/a38335100/PDF_Dateien/Publikationen/Infranorm_Studie_Sec_Normen.pdf.

[9] PRISE (2008). Legal Evaluation Report. http://prise.oeaw.ac.at/docs/PRISE_D3.2_Legal_Evaluation_Report.pdf.

[10] Sinay, J. (2011). Security Research and Safety Aspects in Slovaika. In: Thoma, K. [ed.] (2010). European Perspectives on Security Research. Berlin Heidelberg 2011, 81-90.

[11] Swann, P. (2010). The economics of standardization: an update. Report for the UK Department of Business, Innovation and Skills (BIS). Complete Draft. Version 2.2, 27 May 2010.

[12] Wuerttemberger, T. (2012). Rechtswissenschaftliche Begleitforschung zur intelligenten Videoueberwachung. BMBF-Innovationsforum „Zivile Sicherheit“. http://www.bmbf.de/pubRD/B1-I_Wuerttemberger_Redemanuskript.pdf.

[13] Wright, D., de Hert, P. [eds.] (2011). Privacy Impact Assessment. Law, Governance and Technology Series, Vol. 6. Dordrecht 2011.