INSTITUTE OF TECHNOLOGY ASSESSMENT

Dual-use by design? How ungoverned digital identification practices affect individual agency

4th European Technology Assessment Conference: Value-driven Technologies: Methods, Limits, and Prospects for Governing Innovations. Bratislava, 4.-6. November 2019

ÖAW AUSTRIAN ACADEMY OF SCIENCES

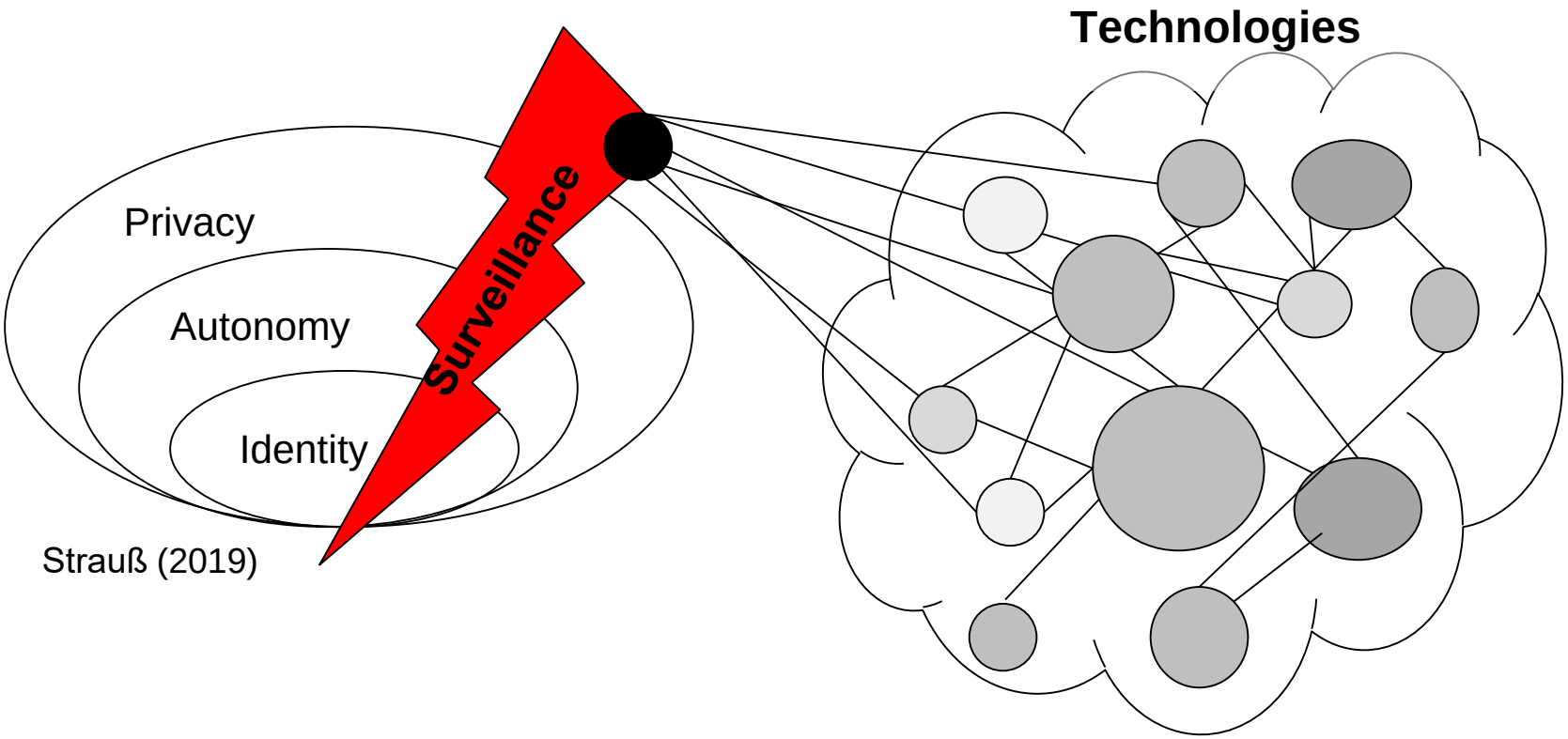
Stefan Strauß

Governing dual-use of surveillance technology – a contradiction in terms?

- Wassenaar Arrangement (1996): primary focus on arms and export control of dual-use technology to strengthen peace and security
- 2009+: Extended policy on **avoiding violation of human rights** of dual-use technology and increasing focus on **'cyber-surveillance technology**':
  - "items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system" (EUC 2016)
- In parallel: „**EU funding for Dual Use** – a practical guide to accessing EU funds for European regional Authorities and SMEs" (EUC 2014)

- **→ contradictory policies between market regulation and stimulation**

(Cyber-) Surveillance and impact on human rights

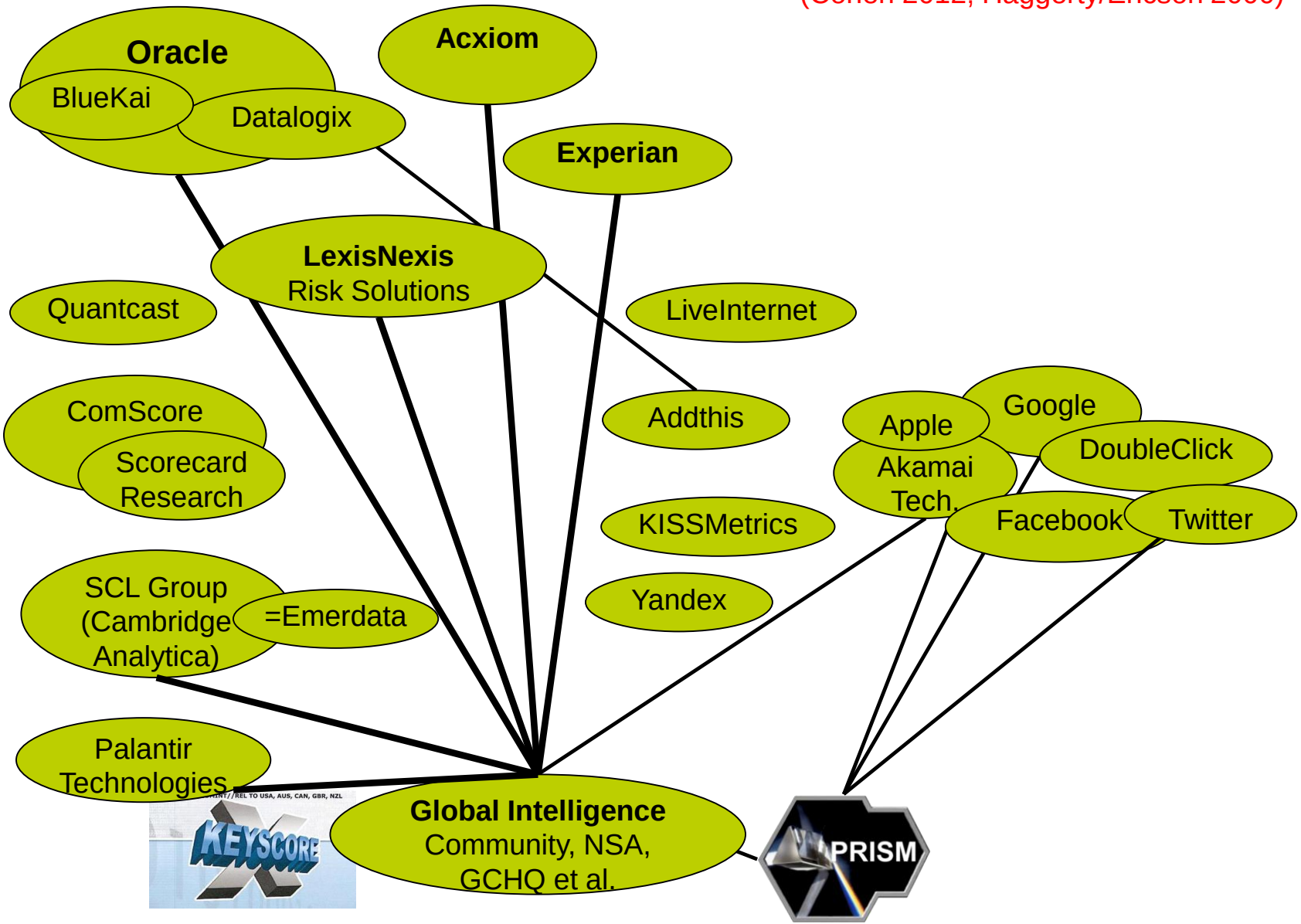


- **→Multidimensional/networked technologies (ICT/cyber…) and dichotomic framings hamper effective governance**
- **→ More promising to govern substantial sociotechnical practices that affect human rights like privacy?**

Data brokers: a “surveillant assemblage”

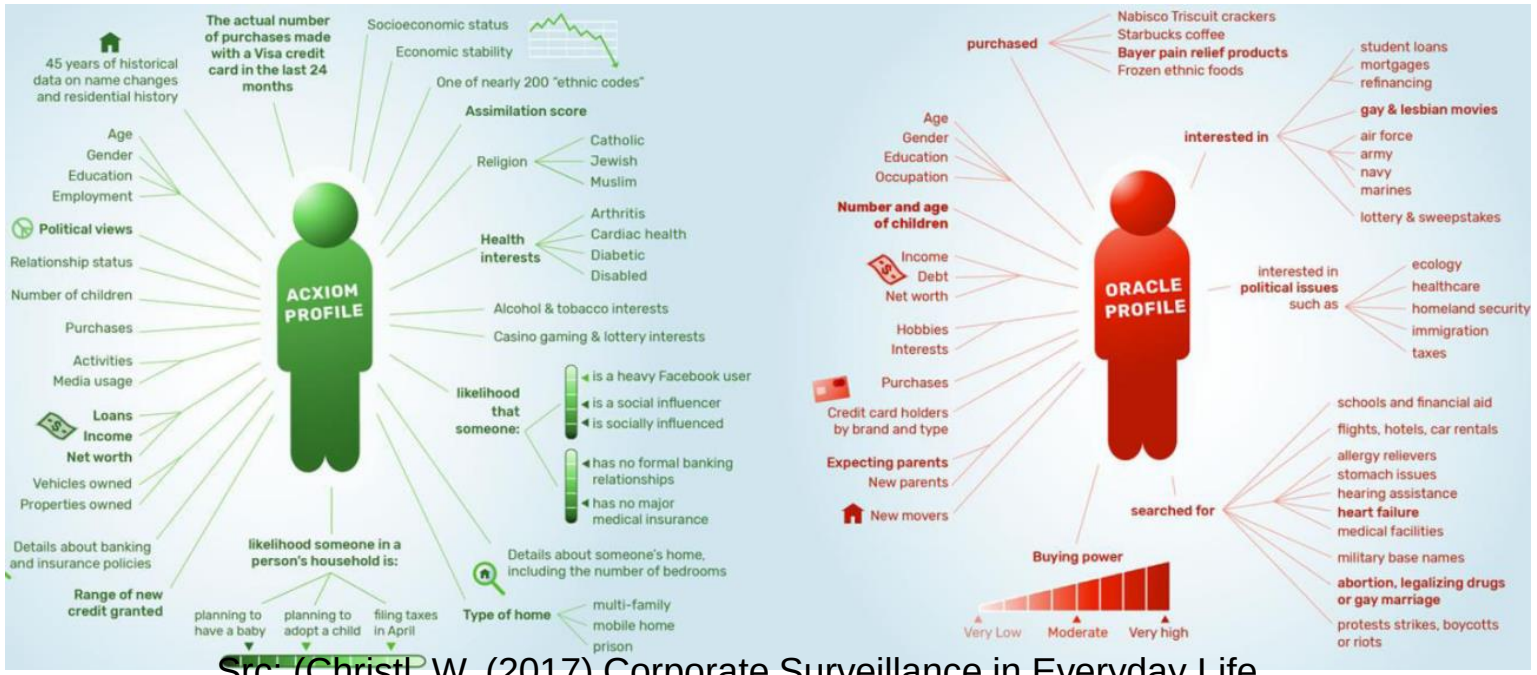
“a heterogenous, loosely coupled set of institutions that seek to harness the raw power of information by fixing flows of information cognitively and spatially“

(Cohen 2012; Haggerty/Ericson 2000)



Network is power: the algorithmic mapping of identity

- Identity graph=database of all known identifiers related to a person (e.g. customer/user profiles, social media activities, network id's, location data etc.)
- → user tracking "**across all devices, screens and channels**" to create **comprehensive identity profiles** / "cross-channel identity" (Oracle)
- E.g.: Axciom provides up to **3,000** attributes and scores on **700 million** people
- Oracle provides more than **30,000** attributes on **2 billion** consumer profiles (Spiekermann et al 2015/Christl 2017)



Src: (Christl, W. (2017) Corporate Surveillance in Everyday Life

What an identity graph reveals

- **Who a person substantially is**
  (biometrics, characteristics, personality etc.)
- **Where a person is and was**
  (e.g. past, present and future locations)
- **To whom and what a person is related to**
  (contacts, relationships etc. in past, presence and future)
- **What a person does, did and is interested in**
  (lifestyle, interests, beliefs, behavior, activities etc.)

Scores=likelihood of future interests, behavior, actions …

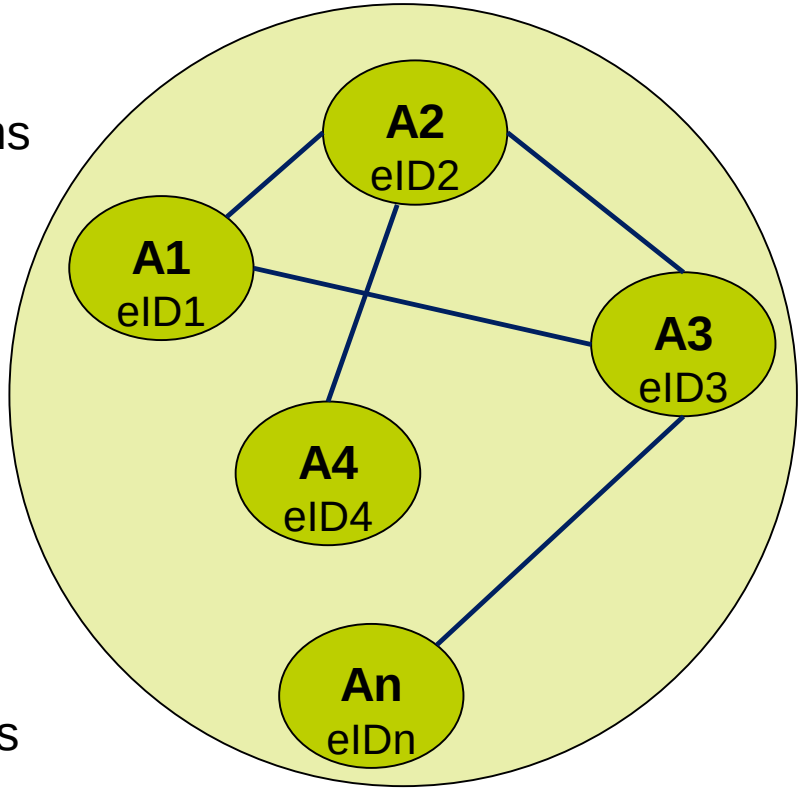
Src: (Christl, W. (2017) Corporate Surveillance in Everyday Life

The digital transformation of identification

Before Web 2.0: mostly distinct application systems (A1-An) with separated user profiles (eID1-eIDn)

Today:

- Significant growth in personalized services + amount of identity information
- Increase in interaction and networking between sub-systems (e.g. Social media, social plugins, standardized user profiles, IDM)
- Increasing integration of (sub-)systems + trends towards meta-profiling and networked IDs



Identifiability-by-Default instead of Privacy-By-Design

Increasing sociotechnical identifiability

Securitization and economization of (digital) identification reinforces dual-use of surveillance technology

- **Global increase in ID practices**
  (e.g. social media, IDM, biometrics, scoring etc.)
- **Increasing surveillance of consumers + citizens**
  - Surveillance capitalism (Zuboff 2019)
  - Comprehensive consumer profiles *„including what people say, what they do and what they buy*“ (Oracle 2015)
  - Surveillance of social media for law enforcement (e.g. US homeland security)
  - Use of “*IoT for identification, surveillance and access to networks or user credentials*” (Clapper, former DNI)
  - “Satellites threaten privacy” (TR 2019)
  - Dystopian scoring e.g. “social credit” system
  - …

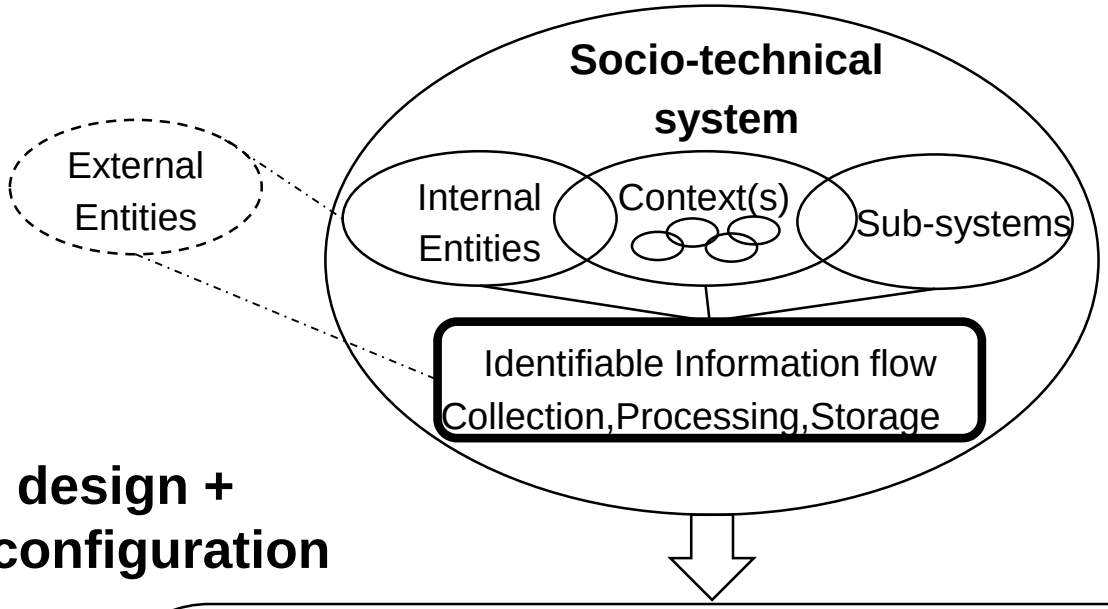
Unregulated algorithmic power through identification practices
by various public + private “surveillant assemblages”

Increasing information asymmetries + agency problems

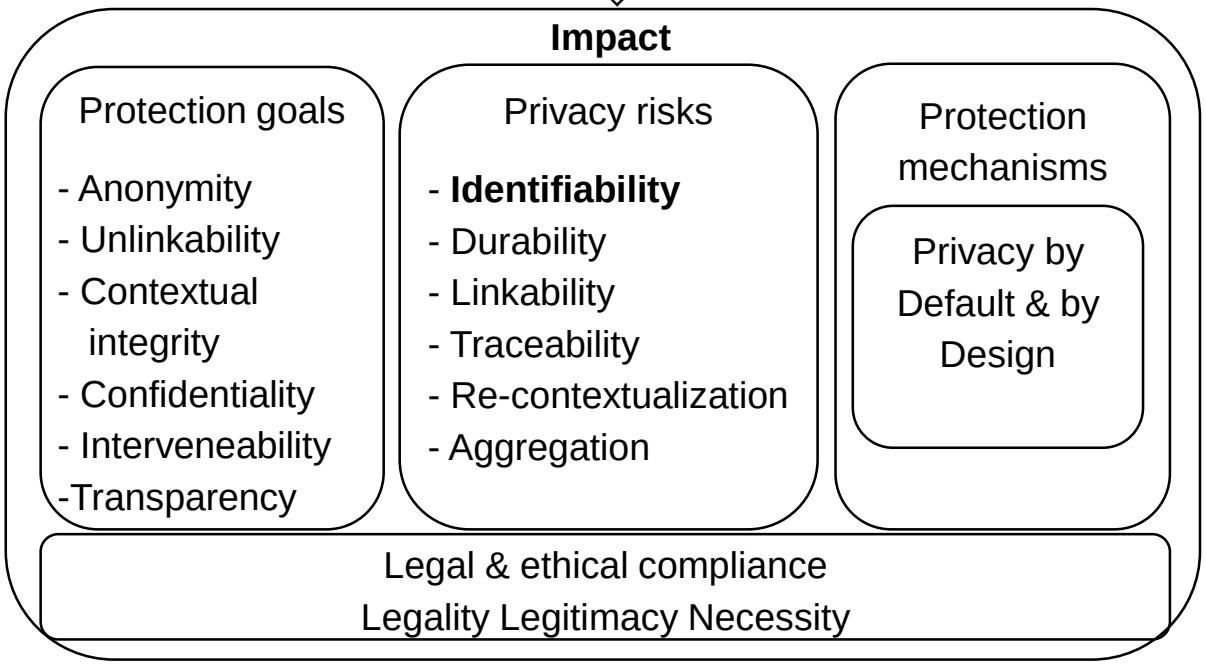
Privacy impact assessment as option to improve governance of dual-use surveillance technology?

- **Need to reinforce institutional accountability and responsibility of technology design and use**
- Increasing challenge of dual-use governance to consider quickly evolving technologies and related risks for human rights (cf.Wagner/Bronowika 2015)
- PIA could …
  - support the (technical and organisational) implementation of privacy by design in technologies and practices
  - build the basis for further risk assessments of dual-use (cyber-) surveillance technology concerning human rights
  - reduce economic incentives to set up business models based on surveillance and thus ease regulation of dual-use markets

Identifiability-based PIA framework



Impact = system design + socio-technical configuration



(Strauß 2019: 233)

Concluding remarks

- Sociotechnical identifiability as core problem of privacy
- → hampers protection and reinforces dual-use surveillance
- Need for: privacy impact assessment + effective privacy-by-design
  - reduce identifiability-by-default at root and thus risks for human rights
    - PIA framework as approach to achieve higher protection standards with
    - more systematic view on privacy risks and identifiable information
- PIA as governance instrument to better regulate dual-use surveillance
- Need for broader debate + better regulation of dual-use “shadow” markets
  - data brokerage and identification practices (e.g. CRM, tracking, microtargeting …)

Thank you for your interest!

Dr. Stefan Strauß
Institute of Technology Assessment (ITA)
Austrian Academy of Sciences
A-1030 Vienna, Apostelgasse 23
Tel: +43 (1) 51581 6599
Fax: +43 (1) 7109883
Email: sstrauss@oeaw.ac.at
Web: www.oeaw.ac.at/ita/en/strauss

Further reading:

Strauß, S. (2019): Privacy and Identity in a Networked Society. London/New York:Routledge.
www.taylorfrancis.com/books/9780429451355