mobile business

Lecture 8

Mobile Surveillance, Data Protection, and Identity Management

Mobile Business II (SS 2021)

Prof. Dr. Kai Rannenberg

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt a. M.

Overview

- Governmental agencies more and more enforce surveillance of communication (“Me too”-Approach).
- Privacy and Security of communication is essential to protect citizens from unlawful surveillance.
- Identity Management Systems help to protect the user from possible threats.

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Why “Surveillance”?

- Fight organised crime:
  - Investigation
  - Prevention

- Socio-political goals:
  - Protect democracy from extremists (e.g. surveillance of the NPD, Al-Qaida, etc.),
  - Keep up preparedness of the military services,
  - Protection from foreign intelligence services.

Bundeskriminalamt

Bundesnetzagentur

Types of Telecommunication Surveillance

- Eavesdropping
- Storage and analysis of connection data
- Automated content analysis (BND)
- Identification of mobile phone users and eavesdropping (IMSI Catcher)
- Data retention
- Determination of the location of callers

We do not cover “bugging” or the manipulation of information technology for surveillance. These issues are regulated in Article 13 GG and § 100 StPO.

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Who is executing Surveillance?

- Surveillance is performed by some specific public agencies (in German called “Bedarfsträger”), e.g.:
  - Police
  - Intelligence services (e.g. Federal Intelligence Service (Bundesnachrichtendienst – BND))
  - Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz – BfV)
  - Foreign (police) authorities requested as administrative assistance via international federation organisations such as Europol
- External supervision of these agencies
  - needed and has been implemented to some degree
  - not trivial due to the secret nature of the agencies’ tasks

Control of the Public Agencies

- Public agencies (“Bedarfsträger”) are under the control of a ministry.
- The parliamentary control commission („Geheimdienstausschuss“) reviews the actions of the intelligence services.
- The Federal Commissioner for Data Protection represents the citizens' interests.
- When investigating according to the code of criminal procedure (StPO – Strafprozess-Ordnung) § 100:
  - The obligation to inform the surveyed person by the public agencies is regulated in § 101 StPO.
    - Notification within 6 months – exceptions may apply.

Control of the Federal Office for the Protection of the Constitution

- The Federal Office for the Protection of the Constitution is controlled by:
  - The minister of the interior responsible towards the parliament
  - The parliament itself
  - The Federal Commissioner for Data Protection or the Commissioner for Data Protection of the states (“Länder”)

- This control is not executed in public!
  - **Problem**: Lack of transparency
  - **Example**: Incidents with regard to the surveillance of the NPD (e.g. “V-Mann Affäre”)

Source: **[StPO]**

Initiation of Surveillance

Distinction between two types:

- Investigation
  - Federal prosecutor and judge approve requests
  - Federal Network Agency ("*Bundesnetzagentur"*) acquires connection data

- "Danger ahead" principle (special urgency)
  - In cases of special urgency, the investigator can refer to the "danger ahead" ("*periculum in mora*") principle
  - The officer-in-charge (security administrator) at the company (provider) decides, cooperates, and notifies authorities

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies ("Bedarfsträger") and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Legal Foundations for the Surveillance of Communications |1

- **Article 10** *Constitution* **("Grundgesetz")**
  - Privacy of correspondence, posts and telecommunications
- **§ 100 of the** *Code of Criminal Procedure* [StPO] defines in which cases communication surveillance is allowed and how it has to be conducted.
  - Comprehensive framework with rules and regulations
  - Measures have to be approved by the prosecutor and the judge, otherwise they cannot be used in court
  - The *Telecommunications Traffic Surveillance Ordinance* (TKÜV) regulates the general process

Legal Foundations for the Surveillance of Communications |2

- **Telecommunications Traffic Surveillance Ordinance (TKÜV)**
  - Reference to § 110 and § 111 TKG
  - Affects telecommunication providers that offer network access to the public (TKG § 110 (6))
  - Affected:
    - Every Internet provider (also including universities and other public bodies offering network access)
    - Hotels/hospitals that offer phone services to their guests/patients

Source: **[BfDI04, BNDG07]**

Legal Foundations for the Surveillance of Communications |3

- **Federal Intelligence Service Law (BND-Gesetz – BNDG)**
  - The Federal Intelligence Service (BND) collects and analyses information of foreign countries, which are of interest with regard to foreign and national security affairs.
  - The BND is authorised to use the means of the Federal Office for the Protection of the Constitution (BfV), if these are necessary to fulfil their duties.
    - This includes, for example, the methodical interception of foreign phone calls.
  - The BND has to follow the statutes of the Federal Data Protection Act (BDSG).

Source: **[BfDI04, BNDG07]**

Legal Foundations for the Surveillance of Communications |4

- **Foreign Trade and Payments Law (AWG) – Control of Exports**
  - For the control of the violation of export controls and for their penalisation: § 39 AWG restricts the secrecy of telecommunications
  - Public agency: *Customs Criminological Office*
  - Controlled by the public attorney's office

- **International Treaties**
  - Treaties such as the "European Mutual Assistance" for Europol extends the public agencies ("Bedarfsträger") by administrative assistance to European agencies
  - Data protection and surveillance become an international topic

Legal Foundations for the Surveillance of Communications |5

- **Most recent Telecommunications Act (TKG) modification (approved by Bundestag/Bundesrat in 2021)**
  - With a wider scope (from Internet and telephone providers to "number-independent interpersonal telecommunication services" like WhatsApp)
  - Mobile network operators must
    - Ensure that IMSI-catchers can also be used in future networks (like 5G) and that their usage cannot be detected;
    - Provide passwords in cases of very serious criminal acts;
    - Enable an unencrypted copy of customer communications in the EU (to be enabled by EU roaming contracts).
  - Data retention reintroduced (Will this apply, before the European Court of Justice (ECJ) will have made its final decision regarding the previous German regulations on data retention?)

Source: **[Heis21]**

mobile business

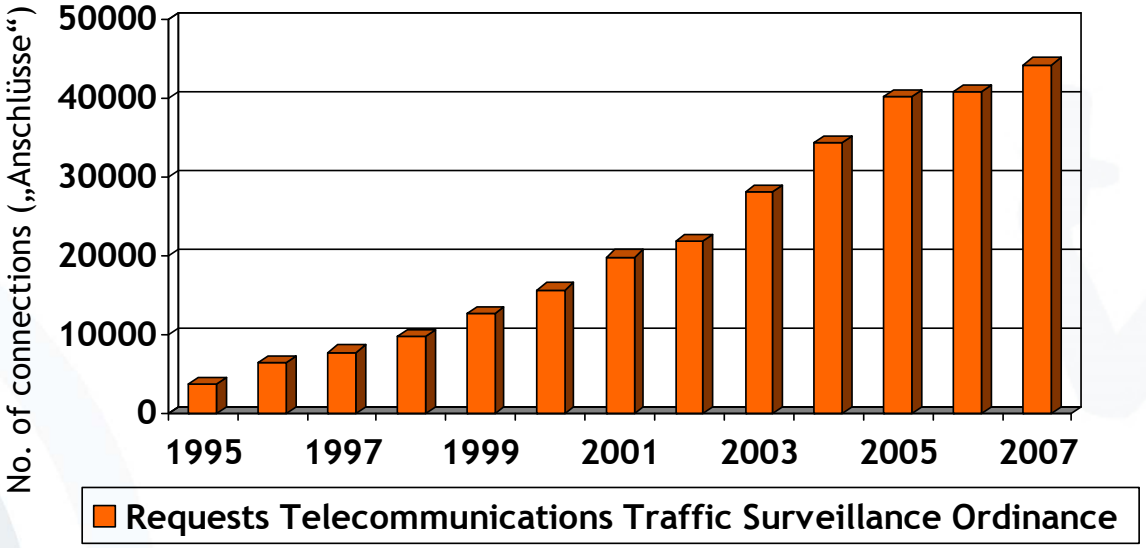
Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies ("Bedarfsträger") and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Queried Telephone Connections (1995 - 2007)

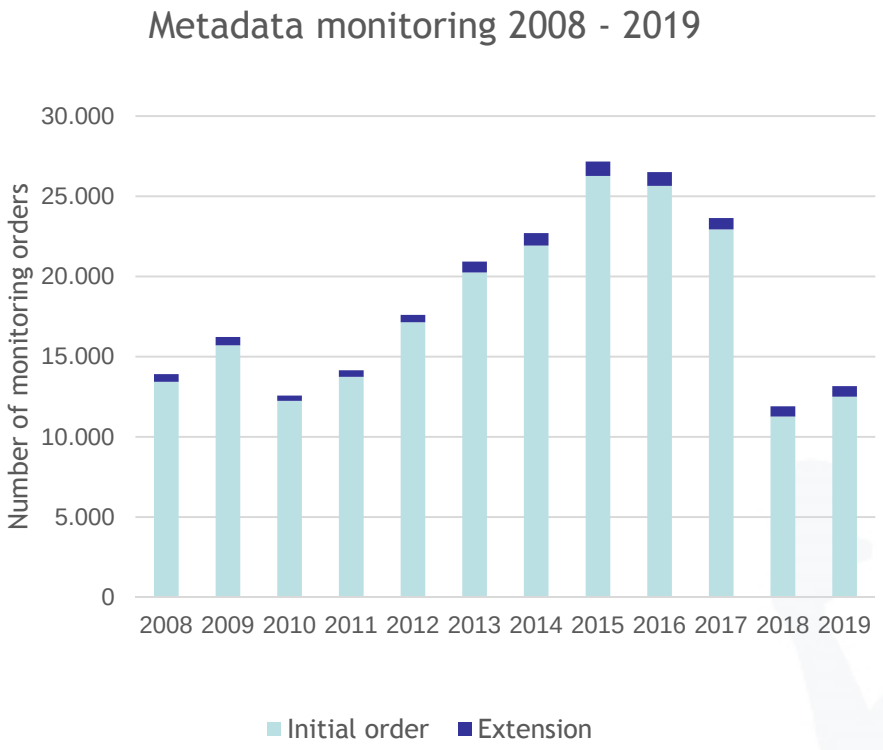
- Compared to 1995, the requests have increased by nearly 1000%, for 2007 a 10% increase compared to the previous year could be observed
- The increase due (partly) to the increase of mobile phone connections
- No evidence for an increased success-rate of investigations
- Since 2008 Bundesamt für Justiz is responsible for and counts surveillance requests instead of connections

Bundesnetzagentur



Source: **[AIDK03, CCCB07, BNA09]**

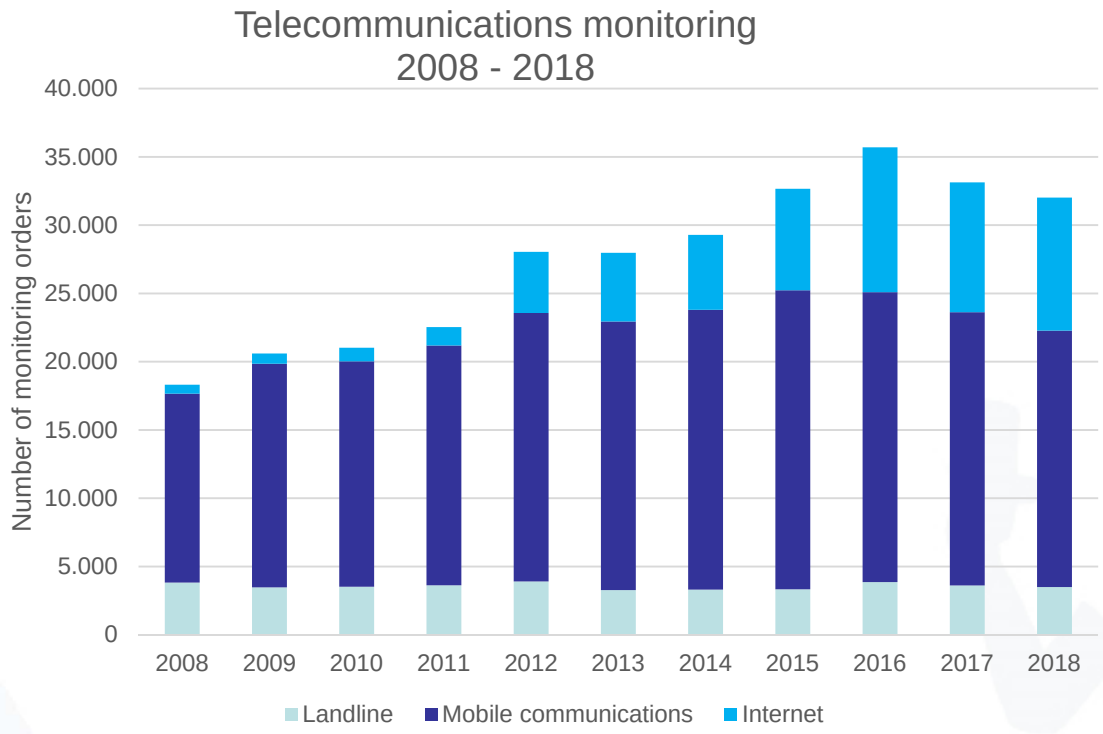
Metadata monitoring (2008 till 2019)



Source: **[BfJ2021]**

Surveillance per communication channel (2008 till 2018)

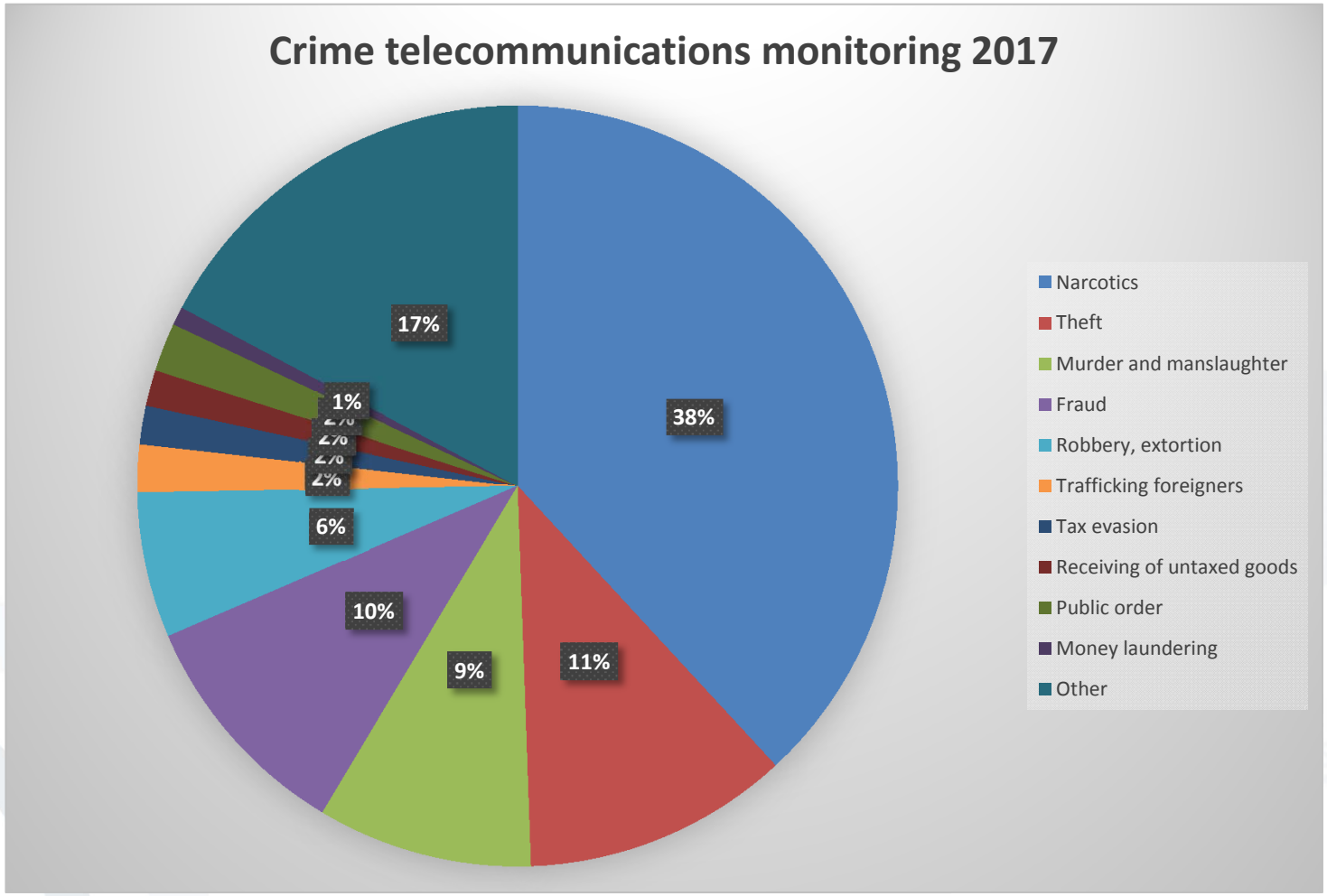
Bundesamt für Justiz



Source: **[BfJ2021]**

Types of investigations reported as reason for surveillance queries

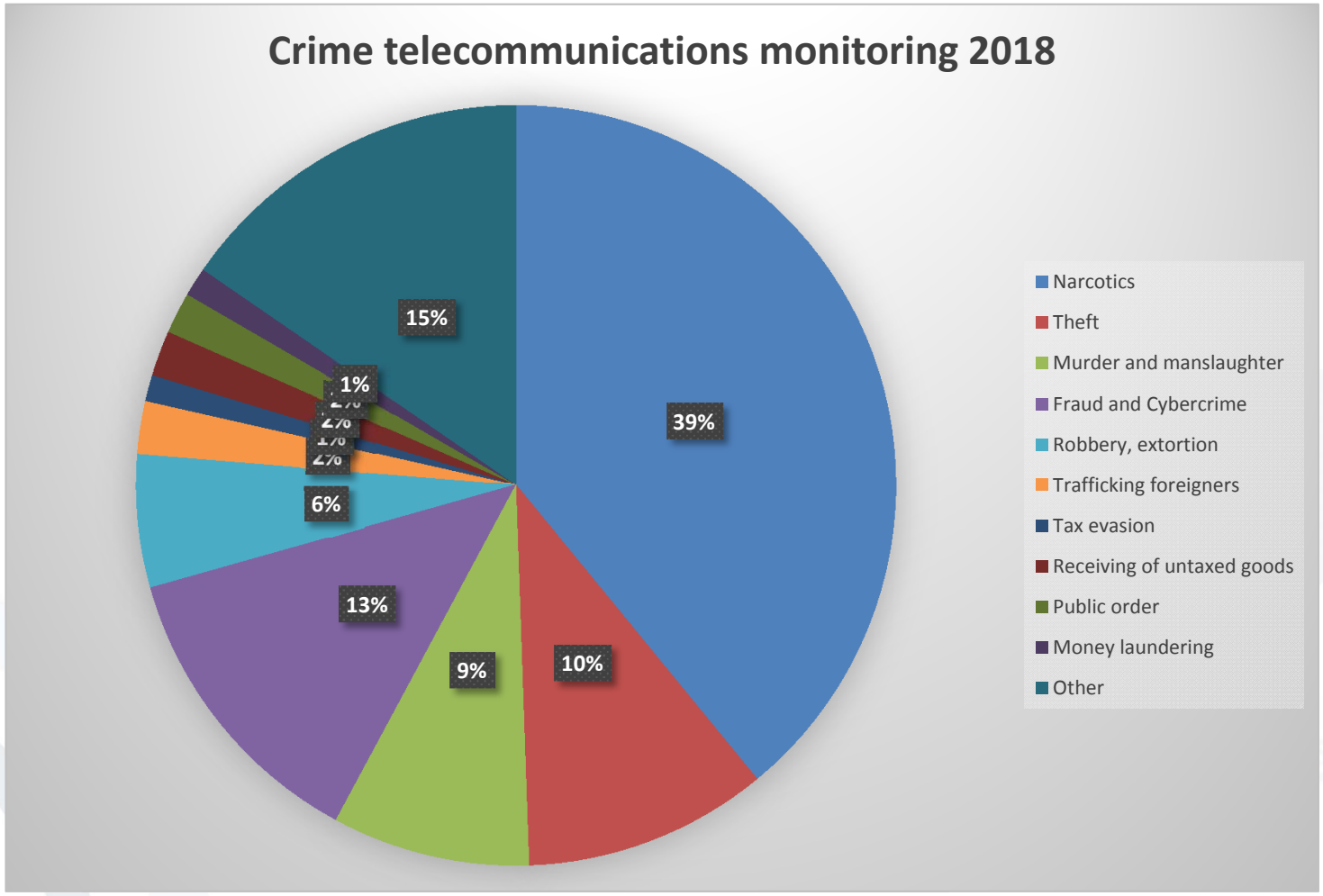
Bundesamt für Justiz



Source: **[BfJ2021]**

Types of investigations reported as reason for surveillance queries

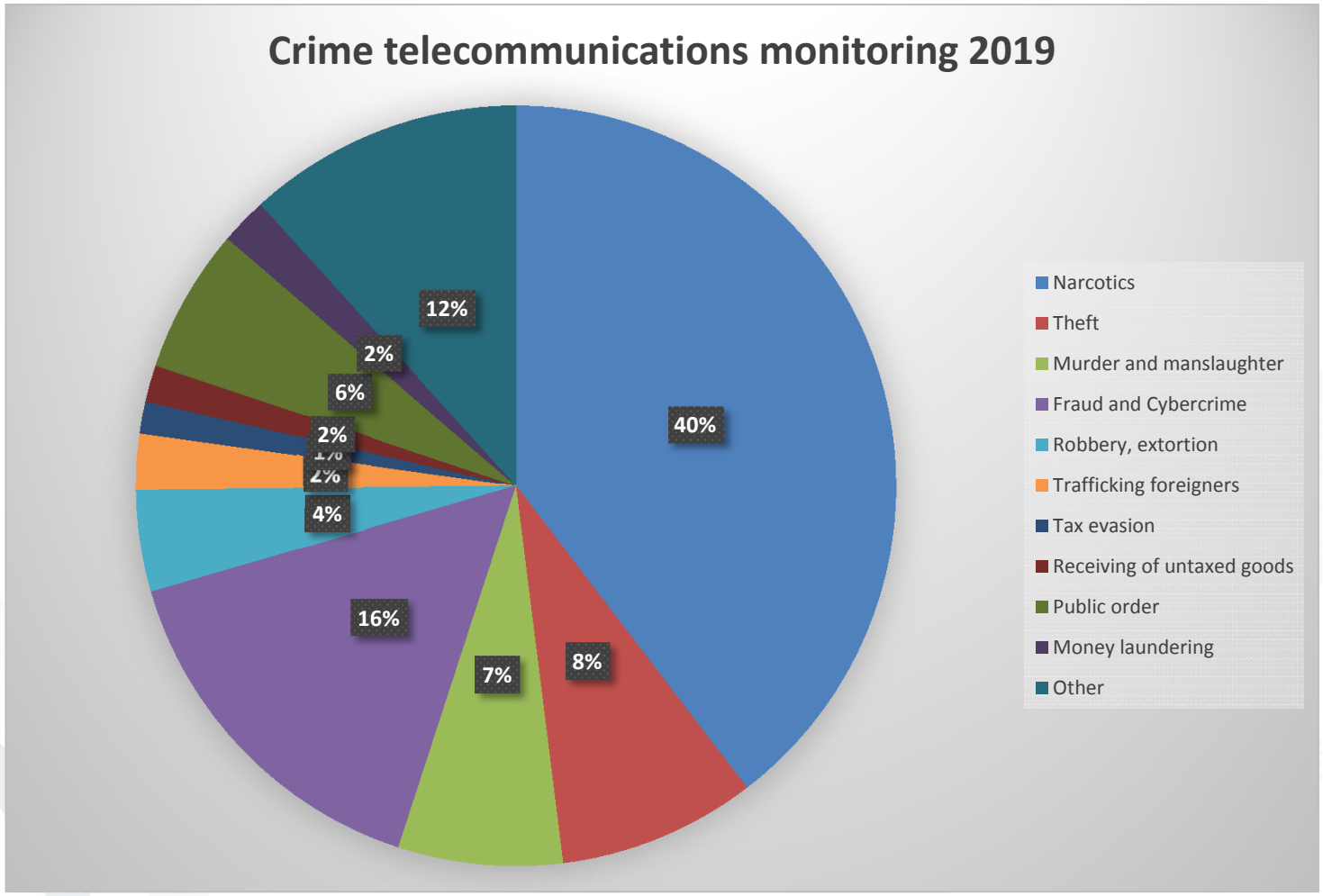
Bundesamt für Justiz



Source: **[BfJ2021]**

Types of investigations reported as reason for surveillance queries

Bundesamt für Justiz



Source: **[BfJ2021]**

Surveillance of Mobile Phones and IMSI-Catcher |1

Due to the diffusion of mobile phones, investigators have new problems:

- Phone number is not linkable to a person's location
- Relation between a person and a mobile phone is not fixed
- Therefore public agencies try to get quick access to the circumstances and content of the communication

Solution: "IMSI-Catcher" by Rohde & Schwarz

Source: **[BInBDI2002, Fox02]**

Surveillance of Mobile Phones and IMSI-Catcher |2

"IMSI-Catcher" by Rohde & Schwarz simulates a strong base station, causing all mobile phones in the network of the respective operator to connect to this simulated base station.

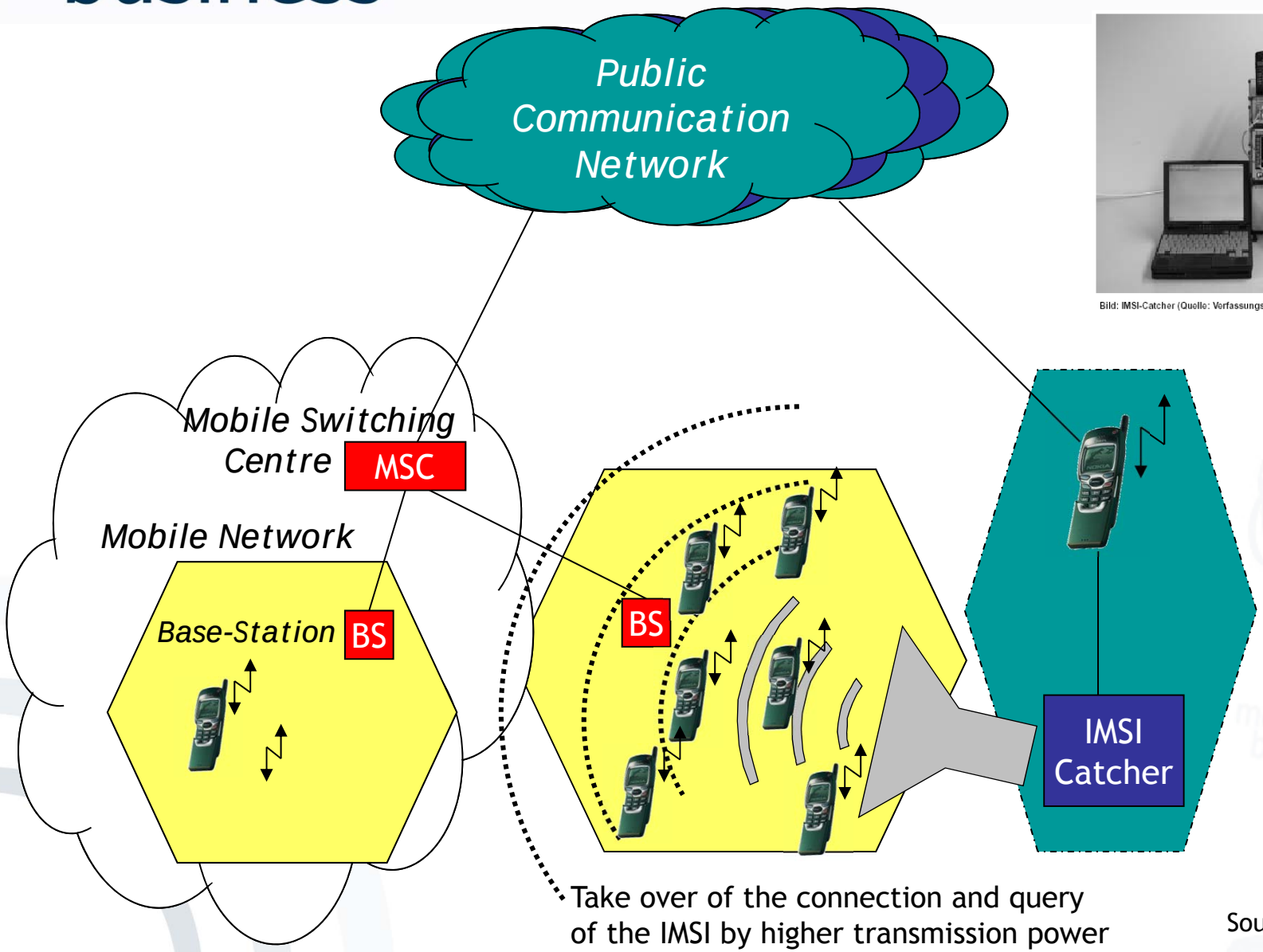
- ➲ The person to be observed can be identified via the IMSI of the SIM, which can be queried at the mobile operators databases (if the operator is in a cooperating country)
- ➲ Interception of the communication

- Problems
  - ...with the constitution due to the rerouting of phones of persons that are not being observed.
  - ...due to technical interferences between the IMSI catcher and normal base stations

Source: **[BlnBDI2002, Fox02]**

IMSI-Catcher: Functionality

Bild: IMSI-Catcher (Quelle: Verfassungsschutz)



IMSI-Catcher

Surveillance & Eavesdrop System

Take over of the connection and query of the IMSI by higher transmission power

Source: **[LDIN98]**

mobile business

Occasional Problems…

German newspaper: “O2 berechnet Überwachten das Abhören”

“Bei der Überwachung von mutmaßlichen Extremisten und Straftätern durch Polizei und Geheimdienste hat es einen peinlichen Fehler gegeben. Die Verdächtigen konnten auf der Telefonrechnung für ihr Handy erkennen, dass sie abgehört wurden.

München - Die Betroffenen hätten wegen einer technischen Panne kürzlich eine Rechnung des Telefonanbieters O2 bekommen, in der Verbindungen zu einer unbekannten Mailbox aufgelistet waren, berichtet die "Süddeutsche Zeitung" unter Berufung auf Sicherheitskreise. Rund 50 Personen seien die Kosten für gegen sie gerichtete Abhöraktionen in Rechnung gestellt worden. […] Nach Angaben der Zeitung werden derzeit in Deutschland fast 20.000 Telefonanschlüsse von der Polizei und den Geheimdiensten abgehört. Besonders nach den Terroranschlägen vom 11. September 2001 in den USA habe die Zahl zugenommen.”

Source: **[SPOL02]**

Situation of the Telecommunications Security Administrator

- The security administrator is the mediator between the company and the customers interests and the government's interests:
  - Responsibility for the security of the infrastructure
  - Contact person and in charge of dealing with surveillance requests in the case of urgency ("danger ahead")
  - Conflict between potential "breach of the secrecy of telecommunications" and "the obstruction of investigations"

Costs of Surveillance

Connection-queries search account databases

- **Example:** „All calls to phone number *n* at the point of time *t*“ searches the complete account database (due to data protection data is stored as „*a calls n at time t*“).

➲ *Results in tremendous costs for the servers and the database licences.*

The interception of phone-calls causes costs:

- Provision of online access
- Purchasing of cryptography hardware (Elcrodat) and maintenance personnel with security clearance
- 24h-availability of the infrastructure

Enforced Registration of Prepaid-SIMs

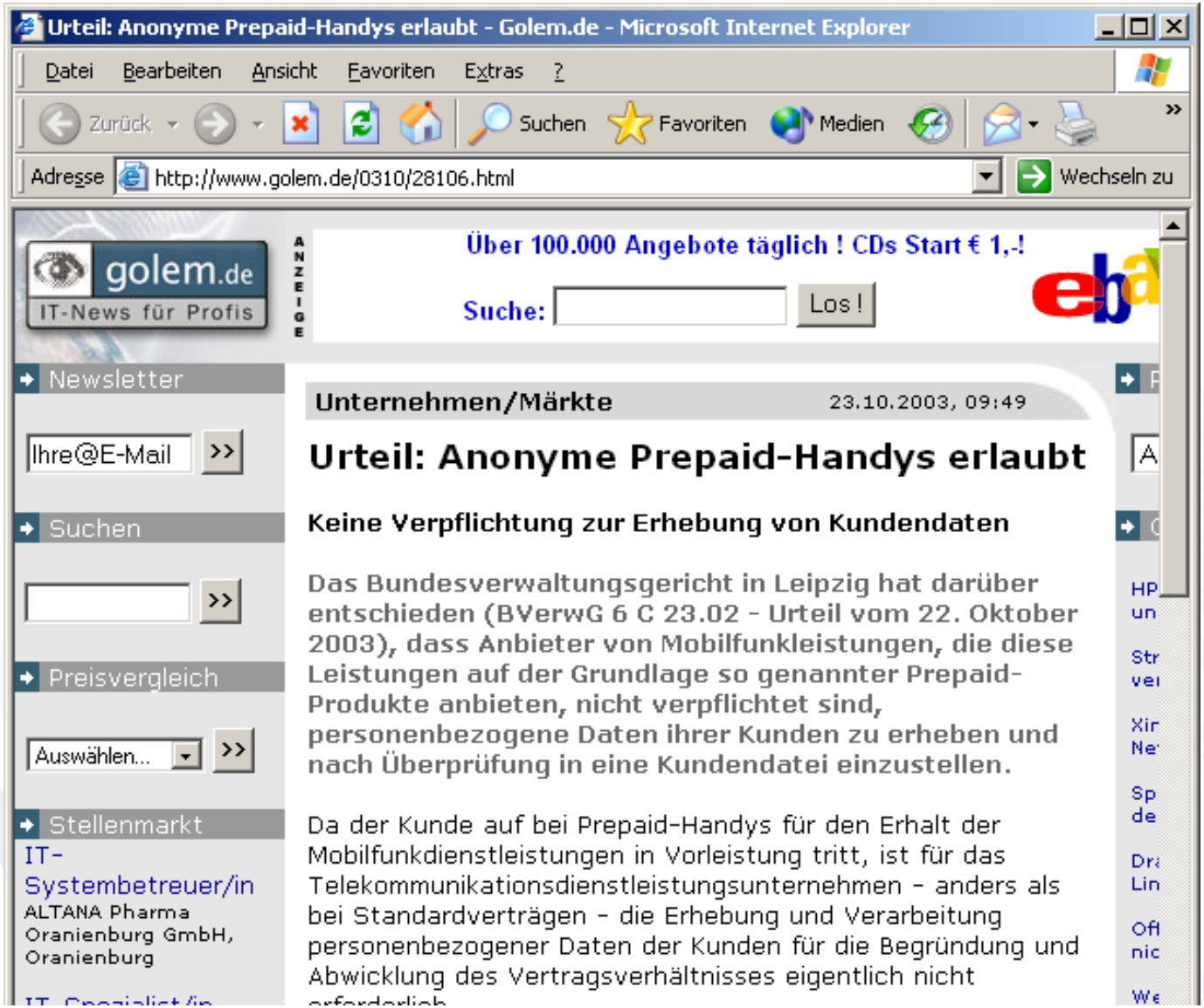
- Since 1997, the Federal Network Agency demands:
  - Buyers of a Prepaid-SIM have to identify themselves by showing an official photo identification
  - The ID number of the identification document has to be stored in an adequate way by the provider
  - Name and address according to the proof of identity, the related number as well as other identification credentials for telecommunications have to be transferred to the directory immediately (§ 90(1) TKG).
  - The telecommunication services may only be activated once the identification process is finalised.
- Providers took legal actions:
  - Won at first instance
  - Lost at second instance
  - Won at third instance
  - ➲ Finally, the law was changed.

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies ("Bedarfsträger") and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Denial of the Enforced Registration of Prepaid-SIMs in 3rd instance | 1



Denial of the Enforced Registration of Prepaid-SIMs in 3rd instance |2

- Revision of the providers (especially Vodafone) at the Federal Administrative Court Leipzig
- Decision on the 22nd of October 2003
- Guideline:

"Die Pflicht der Anbieter von Telekommunikationsdiensten, im öffentlichen Strafverfolgungs- und Sicherheitsinteresse Kundendateien zu führen und in diese bestimmte, dem automatisierten Abruf durch die Regulierungsbehörde für Telekommunikation und Post unterliegende Daten aufzunehmen, betrifft nur diejenigen Daten ihrer Kunden, die sie zuvor nach Maßgabe des für die Vertragsabwicklung Erforderlichen in zulässiger Weise erhoben haben. Die Anbieter sind nicht darüber hinaus zur Erhebung der einschlägigen Daten bei den Kunden verpflichtet."

Source: **[BVwG03]**

Prepaid-SIM Conflicts

- Increased information surveillance not in proportion with the investigations' success rate? [AIDK03]
- Telecommunications data retention
  - Without an explicit cause, telecommunications data retention is unacceptable and unconstitutional according to the Federal Constitutional Court of Germany (BVerfG, 1 BvR 256/08, 2.3.2010).
- Prepaid-SIM registration is required by the legislator.
- Ineffectiveness of these measures due to foreign anonymous prepaid cards?
- In future: Who controls and surveys the location data?

Usage of communications data

- **Constitutional complaint (“Verfassungsbeschwerde”) against TKG succeeded**
  - § § 111-113 TKG to some extent violate constitutional rights according to the Federal Constitutional Court of Germany
  - Constitutional complaints are an extraordinary remedy for the protection of constitutional rights.

24.02.2012 09:58 « Vorige | Nächste »

Karlsruhe beschränkt Verwendung von Telekommunikationsdaten UPDATE

vorlesen / MP3-Download

Die Regelungen zur Speicherung und Herausgabe v
PIN-Codes an Ermittlungsbehörden und andere staa
verfassungswidrig (Az. 1 BvR 1299/05). Das hat der
Bundesverfassungsgerichts in einem am Freitag ver
entschieden. Die Regeln verletzten zum Teil das Gru
Selbstbestimmung.

[Update: Schluss macht Karlsruhe mit der nach Ansicht der Kammer "verbreiteten aber umstrittenen Praxis", §113 auch für Auskünfte über den Inhaber einer IP-Adresse heranzuziehen: Die Regelung "berechtigt [...] nicht zu einer Zuordnung von dynamischen IP-Adressen", entschieden die Richter, auch weil dies einen Eingriff ins Fernmeldegeheimnis darstelle. Der Gesetzgeber hat hier bis Juni 2013 Zeit, eine verfassungskonforme Neuregelung zu schaffen.

Kassiert hat das Gericht zudem eine in §113 Satz 2 geregelte spezielle Auskunftspflicht der Provider gegenüber Strafverfolgern und Geheimdiensten, die Zugangssicherungscodes wie Passwörter oder PINs betraf. Das ist nach Ansicht der Richter nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar, "weil sie nicht den Anforderungen des Verhältnismäßigkeitsgrundsatzes genügt". Der Zugriff auf diese Daten sei in dem derzeit geregelten Umfang "für die effektive Aufgabenwahrnehmung dieser Behörden nicht erforderlich". Die Vorschrift erlaube den Behörden Zugriff, ohne die Voraussetzungen dafür zu regeln. Auch hier hat das Verfassungsgericht eine Übergangsfrist bis Ende Juni 2013 angeordnet.

Source: **[Heis12]**

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Term “Data Protection”

- **Definition:**
  Measures for the protection of stored and transferred personal data against manipulation or misuse; Federal Data Protection Act in place since 1978 (amendment in 1990).
- Originally for the protection of the citizen against governmental institutions.
- Businesses are regulated with regard to special aspects (telecommunications, medicine) of data protection.
- Increased need for regulation due to the use of information technology (data warehouses, globalisation of information processing).

Data Protection Principles in the Context of Communication Services

- **Data minimisation:**
  The service should be offered with a minimum of needed data.
- **Information of data subject:**
  The person whose data is being stored should know what has been stored.
- **Acceptance not without consent:**
  The data subject is to be asked in advance.
- **Right to be forgotten and to erasure:**
  The individuals' right to ask service providers to erase personal information. [EuCo2012]

Data Protection vs. Privacy

- Both terms are related but not synonymous and have many definitions.
- 2 popular ones:
  - **Data protection:** the protection from harmful and unsolicited usage of data linked to the personal sphere of a person
  - **Privacy:** the right to be left alone, e.g. to be unwatched or anonymous [WB1890]
- More work is needed on a complete understanding of privacy.
- Nevertheless the topic is important, as one can see from related incidents and activities to address the issue.

Why privacy?

- **Ensuring the rights of freedom:**
  - Right of informational self-determination as a fundamental human right, derived from the Constitution (Grundgesetz) - "Volkszählungsurteil" [BVG83]
  - Protection against too extensive governmental control

Societal and individual perspective

- **Societal perspective**
  - Foundation of Democracy
  - Freedom of Speech
- **Individual perspective**
  - Free personal development
  - Ownership of personal data of any kind
- But in an information society it takes effort for individuals to protect their privacy

Privacy Online vs. Offline

- **Offline Privacy**
  - In the offline world individuals are able to maintain their privacy intuitively.

- **Online Privacy**
  - In the online world, privacy
    - has to be maintained through complex privacy settings or identity management
    - often cannot be maintained at all by individuals because personal data is collected even without their knowledge

Challenges for Privacy in the Online/Mobile World

- The Internet does not forget or is sometimes not allowed to do so (data retention)
- The Internet allows to easily connect social roles or partial identities, which would have been separated in the offline world
- Profiling is easy and can be done automatically – managing personal information is complex and has to be done manually

Privacy Protection

- Data Protection (EU / Germany)
- Technical Data Protection
- Privacy by Design
- Identity Management

EU General Data Protection Regulation (GDPR)

- The EC adopted a new EU legal framework on the protection of personal data.
- The regulation entered into force on 24 May 2016. It has been applied since 25 May 2018.
- The European Commission says that the regulation “puts the citizens back in control of their data, notably through”:
  - A right to be forgotten: Users will have the right to demand that data about them be deleted if there are no "legitimate grounds" for it to be kept.
  - People will have easier access to their own data, and will find it easier to transfer it from one service provider to another.
  - **Putting people in control**
    - Organizations must notify the authorities about data breaches as early as possible, "if feasible within 24 hours”.
    - In cases where consent is required organizations must explicitly ask for permission to process data, rather than assume it.
  - Privacy by design and by default – privacy friendly default settings to be the norm.

[EuCo2016]

GDPR Principles I

- **Lawfulness, fairness and transparency:** personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** personal data must collected for specified explicit and legitimate purposes.
- **Data minimisation:** personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** personal data must accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

[EuCo2016]

GDPR Principles II

- **Storage limitation:** personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** personal data must be processed in a way that ensures appropriate security of the personal data.
- **Accountability:** The controller shall be responsible for and be able to demonstrate compliance to the principles mentioned above.

[EuCo2016]

Principle of Accountability in the GDPR

- The controller shall be responsible for and be able to demonstrate compliance to the regulation to:
  - maintain certain documentation,
  - conduct a data protection impact assessment for more risky processing (data controllers should compile lists of what is caught), and
  - implement data protection by design and by default, e.g., data minimisation.

[EuCo2016] [Allen2016]

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

EU Directives related to Personal Data and Privacy |1

- **Directive on Privacy and Electronic Communications** (E-Privacy Directive)
  - **Directive 2002/58** on Privacy and Electronic Communications with regard to data retention, spam and cookies
  - Amended by **Directive 2009/136** introducing several changes, e.g. more protection on the use of cookies: **Websites are now required to obtain the consent of users before cookies can be installed on a user's hard drive.**

EU Directives related to Personal Data and Privacy |2

Directive 2009/136

"Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing."

EU Directives related to Personal Data and Privacy |3

- "Cookie Legislation" differs across Europe.
- Current ruling in Germany: **Opt-in** needed for cookies collecting personal information, but **opt-out** is sufficient for all other types of cookies → grey area!

[Cook2015] [Baum2014]

- 2011: Questionnaire from EC on the implementation of the respective article of the ePrivacy directive was answered by German federal government: Existing legislation sufficient to comply with the directive, no need to change the law.
- 2014: Statement upheld

[Bund2011] [Tele2014]

EU Directives related to Personal Data and Privacy |4

German Bundestag opposition's legislative initiative in 2012:

Aiming to make German laws compliant with EU regulation.

Deutscher Bundestag

Suchwort eingeben

Der Bundestag | Dokumente | Mediathek | Kultur & Geschichte | Presse | Besu

- Pressemitteilungen
- Aktuelle Meldungen (hib)
- Kontakt
- Akkreditierung
- Parlamentsfernsehen
- Termine
- Bilderdienst, Bildarchiv
- Mitschnittservice

Startseite > Presse > Aktuelle Meldungen (hib) > Februar 2012 > SPD-Vorstoß zum besseren Schutz vor "Cookies" erfolglos

SPD-Vorstoß zum besseren Schutz vor "Cookies" erfolglos

Ausschuss für Wirtschaft und Technologie - 29.02.2012

Berlin: (hib/HLE) Ein Vorstoß der SPD-Fraktion zum besseren Schutz von Anwenderdaten im Internet ist ohne Erfolg geblieben. Der von der Fraktion eingebrachte Gesetzentwurf zur Änderung des Telemediengesetzes (17/8454) wurde am Mittwoch in der Sitzung des Ausschusses für Wirtschaft und Technologie von der Mehrheit der Koalitionsfraktionen CDU/CSU und FDP abgelehnt. Neben der SPD-Fraktion stimmten auch die Linksfraktion und die Fraktion Bündnis 90/Die Grünen für den Antrag.

Die SPD-Fraktion wollte mit der Gesetzesänderung erreichen, dass Anbieter von Telemediendiensten sogenannte Cookies nur mit Einwilligung ihrer Kunden auf deren Computern speichern dürfen. Zur Begründung verweist die SPD-Fraktion auf eine EU-Richtlinie, nach der Deutschland verpflichtet gewesen wäre, den Einwilligungsvorbehalt bereits bis spätestens Mai des vergangenen Jahres einzuführen.

Bisher muss der Diensteanbieter nur über das Setzen von Cookies unterrichten. Vor der durch Cookies ermöglichten Profilbildung sei der Kunde bisher nur durch eine Widerspruchslösung nach dem Telemediengesetz geschützt, hatte die SPD-Fraktion argumentiert. Danach könne ein Diensteanbieter zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, wenn der Kunde nicht widerspreche.

[DeBu2012]

EU Regulations related to Personal Data and Privacy |5

- **Regulation for Privacy and Electronic Communications** (e-Privacy Regulation)
  - Originally scheduled to come into effect starting 25 May 2018 together with the GDPR
  - EC commission states that this improves the privacy in electronic communications:
    - e-Privacy Directive only applies to traditional telecom operators, while the e-Privacy Regulation applies to providers of electronic communication services, e.g. WhatsApp, Skype, Viber, Facebook Messenger.
    - Privacy is guaranteed for both content and metadata of electronic communications (`metadata´ replaces the current definition of `traffic data´ from e-Privacy Directive).
    - Non-privacy intrusive cookies that improve Internet experience, e.g. to remember shopping cart history, and cookies counting the number of visitors of a website will not be blocked by default.

Source: **[EuCo2017]**

e-Privacy Regulation Overview

- The paradox of (protected) electronic communication
- Electronic communication and the need for protection
- The OTT market and the need for a level playing field
  - Location data and OTT user profiles
  - Wifi/Bluetooth tracking
  - Privacy settings & security risks
  - Internet of Things

Addressing the paradox of (protected) electronic communication

- Electronic communication is more and more in need of protection of privacy and confidentiality.
- Offering properly protected communication is (often) not properly honored by the market:
  - Unprotected communication is offered for free.
  - Regulation so far covers only one market segment ("traditional" telcos).
  - No level playing field

➢ Including Over-the-Top communications services (OTTs) into the scope of the regulation is essential for effective protection.

➢ It needs to be done thoroughly.

Electronic communication and the need of protection

- Privacy protected communication is not only an fundamental right (EU Charter Article 8) individual for the individual, but an essential prerequisite for a working democracy.
- Communication metadata are a well structured data sets, that can very easily be exploited by attackers with computing capabilities.
- Communication content needs to be transferred, often into another domain, so it is inherently at risk.

➢ GDPR would not be enough to cover this.

Communication services not a product on its own (anymore)

- Simple (unprotected) digital communication can technically be provided as a byproduct or free service especially if one considers user data as a resource.
  - OTTs offer “free” communication in exchange for personal data (WhatsApp, Facebook, Instagram, …).
  - Prices and margins for communication services go down (often to 0).
  - If there are no trust guarantees we end up with a “Lemons Market”, the loss of trust, and detrimental effects for democracy.
- Art. 3(1)(a) "irrespective of a payment" and (Art. 4(2) "ancillary feature") are important features to cover this development.
- But more is needed.

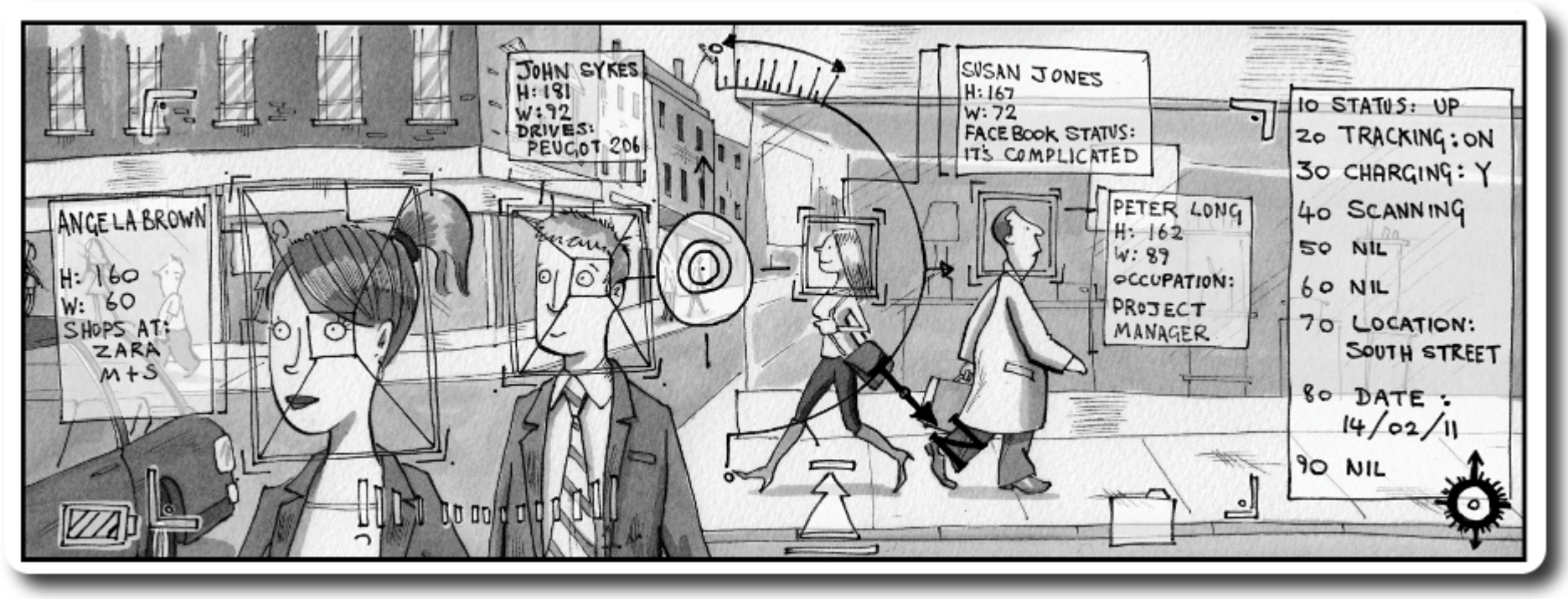
Aspects of the OTT market

- Incentive (triggered by e.g. via venture investors) to quickly collect large numbers of registered “users” and their (movement) profiles (users = resources ≠ customers)
- Application segments not (yet) clearly defined, e.g.
  - Messaging part of social network (Facebook) experience?
  - Household management part of Google experience?
- Trend towards market domination by a single or very few players “owning” data (re)sources
- Is this situation a solid basis to protect constitutional values?

➢ Providers of better (protected) services need better protection to move towards a level playing field.

➢ OTTs need to be covered more comprehensively:
  - ➢ Location data
  - ➢ Web-tracking, offline-tracking (via Wifi or Bluetooth)

Location data tightly coupled with OTT user profiles



- Needs to be considered in
  - Art. 4(3)(c): Definition of “electronic communications metadata”
  - Art. 8(2)(b): Collection zones with Wi-Fi/Bluetooth tracking

[www.thebigdatainsightgroup.com/site/article/big-data-talk-005-big-data-big-brother]

Location data Definition

- Art. 4 (3)(c): " 'electronic communications metadata' means […], including […] **data on the location of the device** **generated in the context of providing electronic communications services**, […]"
- Too narrow:
  - Telcos are covered.
  - OTTs are not covered!

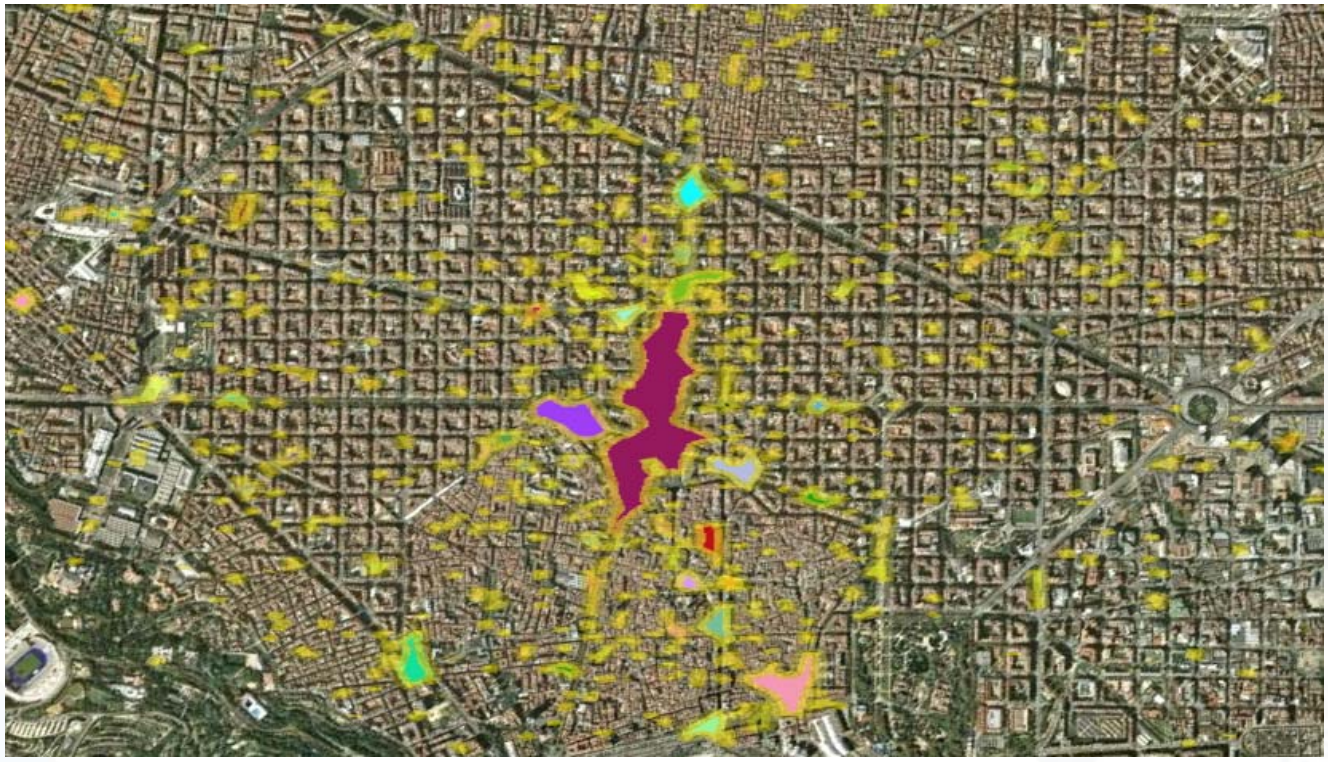
➢ Only limited protection for users (and the borderline is hard to understand for users)

➢ Competitive disadvantage for telcos (European players)

➢ **Delete the text in red.**

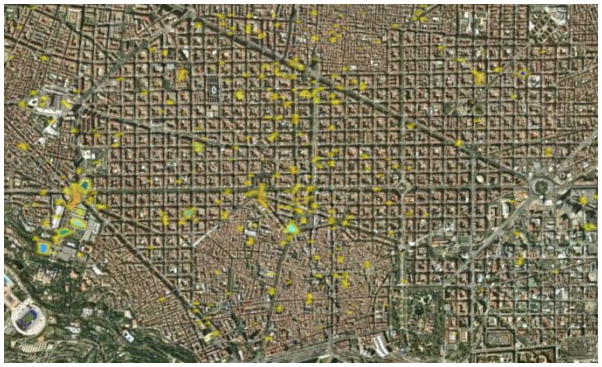
mobile business

Location data, Recital (17)
Heatmaps (Geo-spatial Clustering)

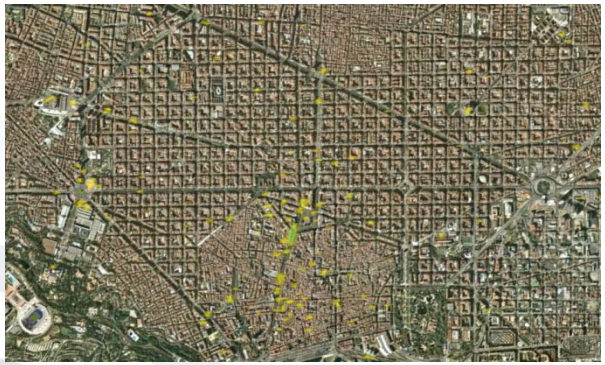
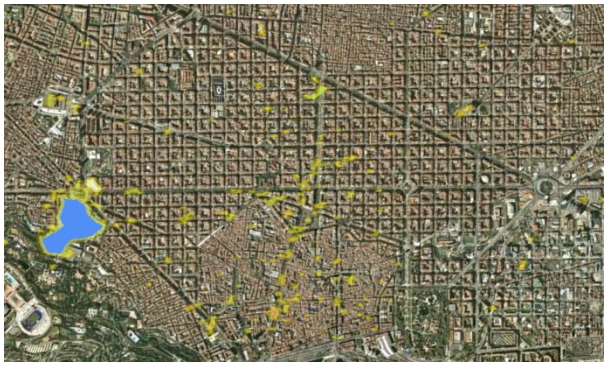
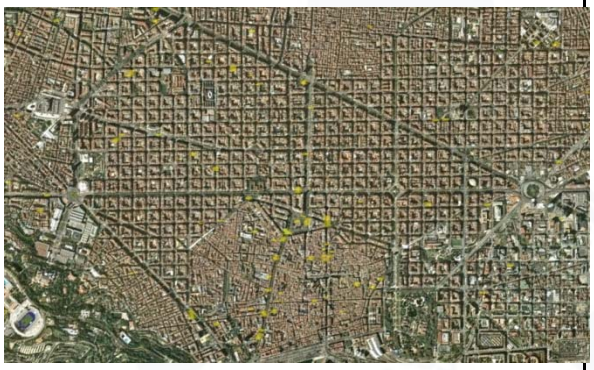


Location data, Recital (17) Traffic Movements

Locals


Tourists

- Traffic movements can be shown with anonymous data also.
  - No (pseudonymous) identifier needed
  - Change Recital (17)

Art. 8(2)(b): Collection Zones with Wi-Fi/Bluetooth tracking

- Person responsible for collection must indicate measures end-users may take to minimize or stop the collection.
- Gives the impression that organisations may collect information emitted by terminal equipment to track the physical movements of individuals (such as “Wi-Fi/Bluetooth-tracking”) without the consent of the individual concerned.
- The party collecting these data could apparently comply by means of a notice informing users to switch off their devices, when they do not want to be tracked.

➢ Contrary to a basic goal of the telecommunications policy of the European Commission to provide high-speed mobile internet connectivity with strong privacy protections at a low cost to all Europeans, across borders.

ePrivacy Regulation
State of negotiation

- European Commission (2017-01-10): Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC) (Regulation on Privacy and Electronic Communications)
- European Parliament (2017-04-11): Hearing on the e-Privacy reform (www.europarl.europa.eu/committees/en/libe/events-hearings.html?id=20170328CHE01221)
- European Parliament (2017-06-09): Draft report on the proposal by the Committee on Civil Liberties, Justice and Home Affairs (www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-606.011+01+DOC+PDF+V0//EN&language=EN)
- On 22.11.2019 the Permanent Representatives Committee of the Council of the European Union rejected the latest draft of the ePrivacy Regulation once again. The future of the ePrivacy Regulation is now uncertain (https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/)
- On 05.01.2021 the Portuguese presidency of the EU Council proposed a new draft version that convinced most member states.
- The trialogue negotiations with the European Parliament are expected to start soon.

ePrivacy Regulation Draft by the EU Council

The draft is criticised by data protection officials (e.g. Ulrich Kerber):

- Regulation proposes the reintroduction of data retention.
- “Cookie Walls“ would be permitted.
- The right to object and the data protection impact assessment have been removed.
- A recourse to the guarantees of the General Data Protection Regulation is excluded.
- Personal data can be processed for other purposes without user consent.

Source: **[BFDI2021]**

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

The Implementation of Data Protection

- **Germany:** Federally organised data protection
- Responsibility in Germany:
  Federal Commissioner for Data Protection and Freedom of Information (BfDI)
- Each state in Germany has its “Länder” Data Protection Commissioner.
  - Specialisation on certain fields, e.g. in Schleswig-Holstein (ICPP) on Privacy in the Internet

- **Additionally:**
  Data protection officers within governmental administration and within companies

The origin of data protection in Germany

- Data protection in Germany (*Datenschutz*) originates from concerns over too much information and power in the hands of large (governmental) institutions (“Big Brother”)
- Data protection and Privacy are based on the right of informational self determination derived from the constitution in the “Volkszählungsurteil“ [BVG1983]
- Germany has one of the most advanced infrastructures for Privacy but still no established German language term for Privacy beyond the misleading *Datenschutz*
- Some (more or less established) related terms are:
  - Privatheit
  - Privatsphäre
  - Schutz der Privatsphäre

Telecommunications Act (1)

Telecommunications Act (TKG) (1997, modified 2021)

- § 91 extends data protection to all professional providers of telecommunication services, incl. company telephone systems, hotels, Internet, etc.
- TKG also enables the Telecommunications *Data Protection Ordinance (TDSV)* and implements the statutes of *Directive 95/46/EG.*
- Remember: TKG also regulates the telecommunications surveillance (via TKÜV).
- Regulates
  - storage of data,
  - creation of invoices,
  - foreign usage of personal data

  ➲ Demands data minimisation when storing data.

Telecommunications Act (2)

Telecommunications Act (TKG) (1997, modified 2021)

- Explicit consent by the user of processing personal data as well as the right to withdrawal.
- *Services:* Regulates call forwarding, caller ID, storage of mailboxes.
- *Utilisation:* Regulations for directory-assistance services, phone books und directories.
- Defines *monetary fines* up to 500.000 €.
  The Federal Network Agency (Bundesnetzagentur) is authorised to control the data protection.

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Identity Concepts

Mental vs. Procedural View |1

- **Mental identity** (ipse)
  - Researched by social/psychological sciences
  - Dynamically changing configuration reflecting, and shaped by, interactions between an individual and its environment
  - Private and endless task to go deeply in ones own description:
    - “Only I can be responsible for acts done by me.”
    - “I remain myself by being faithful to my promises.”

Source: **[BB2001]**

Identity Concepts
Mental vs. Procedural View |2

- **Procedural identity** (idem)
  - Used by technical/administrative sciences
  - Collection of formalized characteristics, which enable identification and authentication necessary for social and economic relations, as well as dealings with the authorities.
    - E.g., a person's name, marital status, date of birth, height, colour of skin or eyes, number of children, nationality, educational and professional qualifications, etc.
  - The choice of these characteristics may depend on the context, i.e. controlling authority, functional needs, etc.

Identity Concepts
View of Identity (Control)

- *Tier 1 (T1):* True (‘My’) identity
- *Tier 2 (T2):* Assigned (‘Our’) identity
- *Tier 3 (T3):* Abstracted (‘Their’) identity
- The different tiers can be distinguished by the factor ‘control’ :

  Who controls the identity?

Source: **[Durand2003]**

Identity Concepts
Tier 1: True Identity

- *A Tier 1 (true – 'My') identity is my true and personal digital identity and is owned and controlled entirely by me, for my sole benefit*

- T1 identities are both timeless & unconditional

Source: **[Durand2003]**

mobile business

Identity Concepts
Tier 2: Assigned Identity

- *A Tier 2 (assigned – 'Our') identity refers to our digital identities that are assigned to us by corporations (e.g. our 'customer accounts')*
  - *Our* job title (assigned to us by our employer)
  - *Our* cell phone number (assigned to us by our mobile phone operator)
  - *Our* United Mileage Plus number (assigned to us by United Airlines)
  - *Our* social security number (assigned to us by the Government)
  - *Our* credit card number (assigned to us by our credit card companies)

Source: **[Durand2003]**

Identity Concepts
Tier 3: Abstracted Identity

- *A Tier 3 (abstracted – 'Their') identity is an abstracted identity in that it identifies us through our demographics and other reputation like attributes, but does not need to do so in a 1:1 manner*

- T3 identities speak to the way in which companies aggregate us into different marketing buckets for the purposes of advertising or communicating with us
  - E.g., we're either a 'frequent buyer' or a 'one time customer' etc.
- T3 identities are typically based upon our behaviour in our interactions with business
- The entire CRM market caters to T3 identities

Source: **[Durand2003]**

Identity Concepts
Working Definitions

- *Identity:*
  The characteristics (attributes) representing an acting entity
- *Partial identity:*
  A subset of the characteristics of an identity

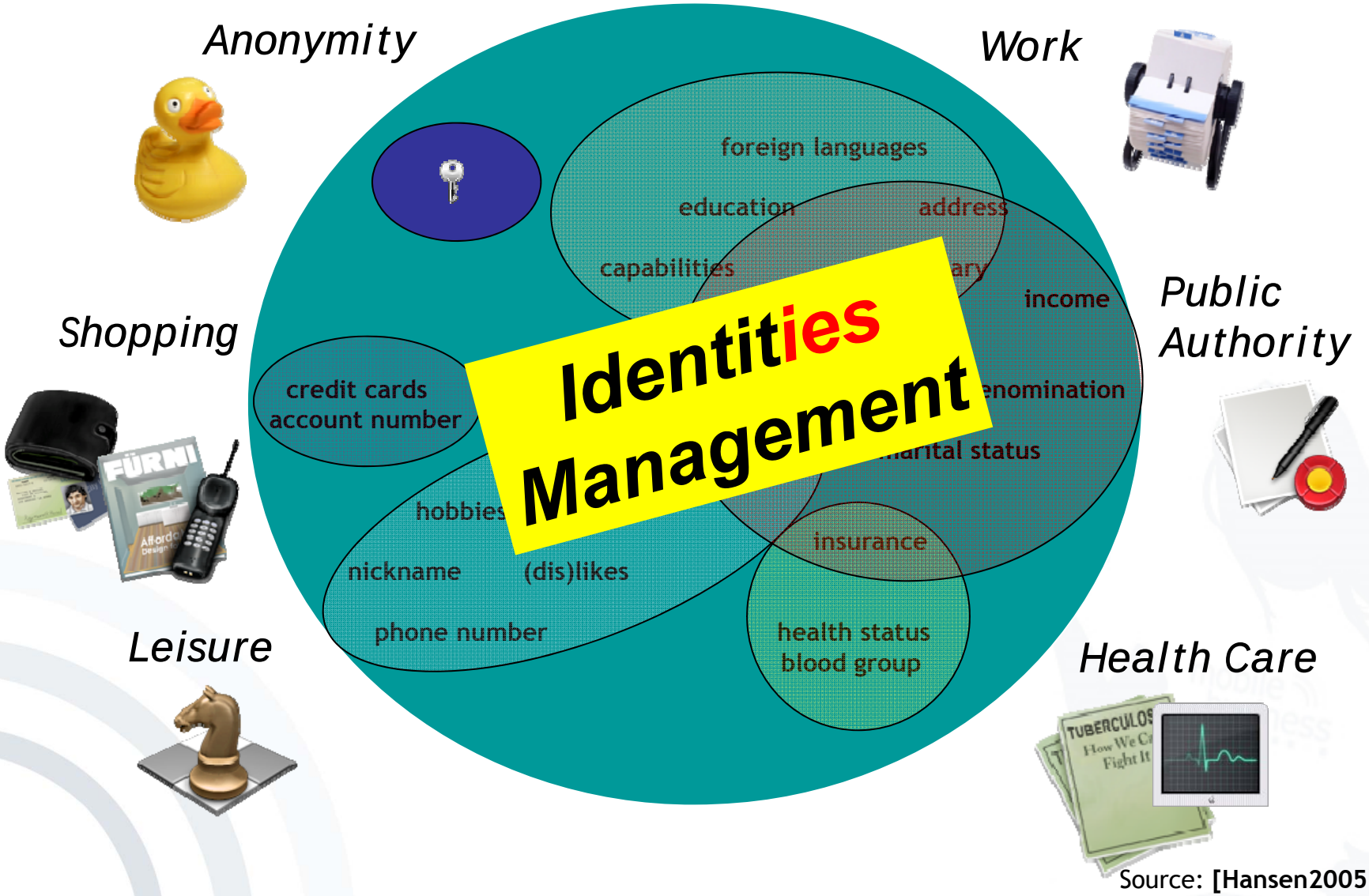
- *ISO/IEC 24760-1 "A framework for identity management":*
  - **Identity** (partial identity): Set of **attributes** related to an **entity**

Why are partial identities important ?

- Different partial identities are assigned to and abstracted from an entity
- The identity of an entity consists of partial identities distributed over different partners of the entity

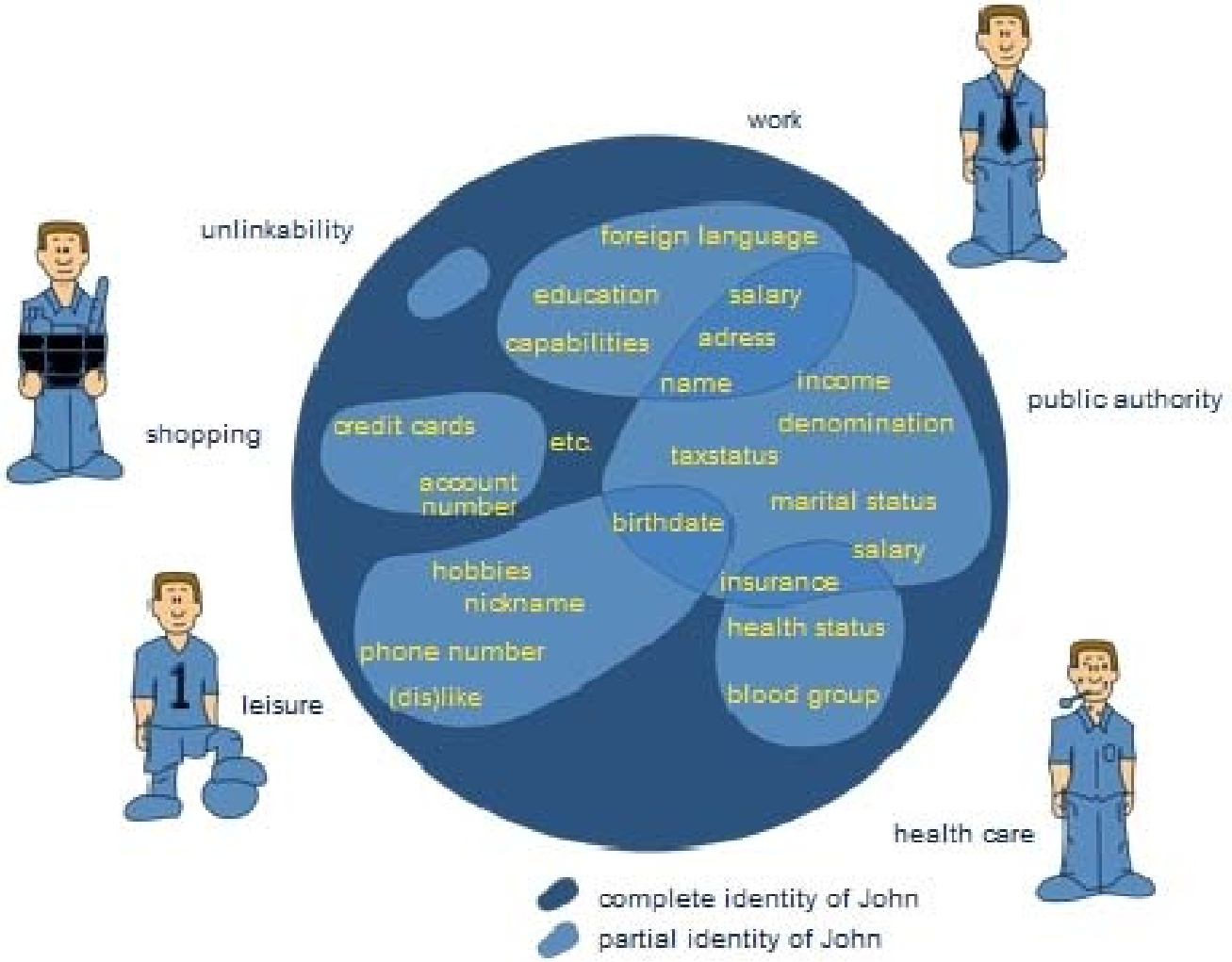
Source: **[BMH2005, ISOIEC24760]**

Identity Concepts
Partial Identities Illustrated | 1



Source: **[Hansen2005]**

Identity Concepts
Partial Identities Illustrated |2



Source: **[PRIME2006]**

Identity Concepts
Mobile Identities

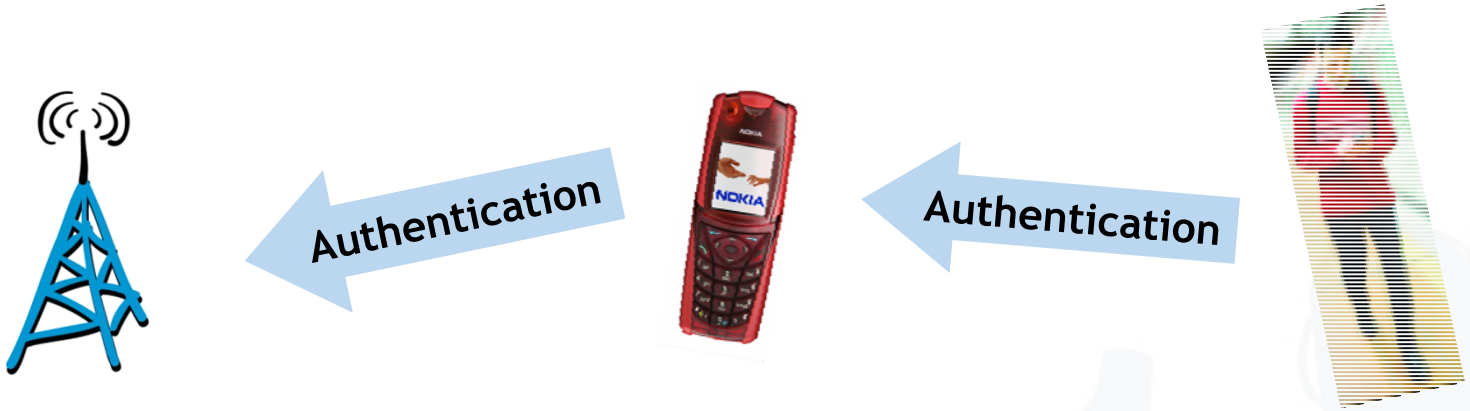
- What makes an identity mobile?
  - Location data / Context of the user
  - Temporal aspect
    ➲ mobile identities change during their lifetime.
- Partial identities for different aspects
  - Private life?
  - Business life?

- **Working definition:**
  Mobile identities are (partial) idem identities extended with location information

Source: **[Royer2006]**

Identity Concepts
Mobile (digital) Identities

- A concept that **links** a "token/device" from the *digital/syntactical world* to an object in the *real/semantical world*



- Accompanied by a set of **properties** and attributes

mobile business

Agenda

- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Identity Management (IdM)

Identity Management (IdM) is often used as a *buzz word* that can have many meanings such as:

- The management of accounts for employees, customers or citizens
  - These accounts contain those parts of an identity relevant for an organization (attributes, access rights, roles, …)

  → Trend towards federations between organizations
- The collection and analysis of data about individuals allowing for the extraction of useful knowledge on these individuals (profiling)

  → E.g., for marketing or law enforcement purposes
- The possibility of an individual to manage its procedural identities with different organizations (partial identities) and in this way allowing

  → To build a ‘healthy’ virtual socio-psychological identity

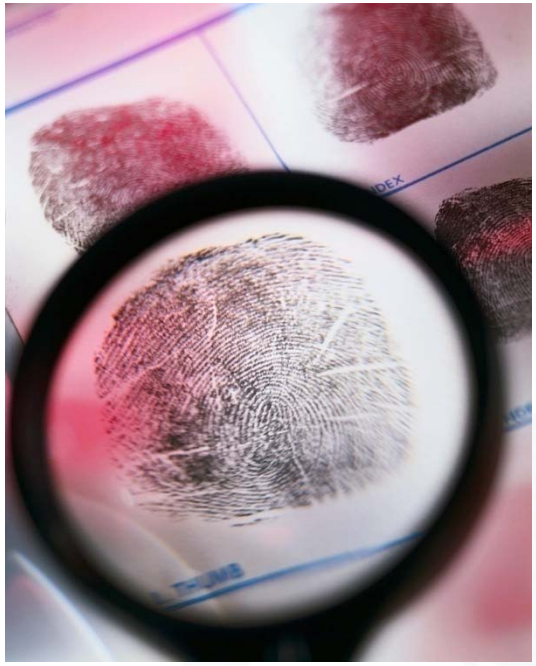
Identity Management
Identity Management Systems (IdMS)

- Tools that support IdM activities
- We distinguish
  1. Pure IMS main objective is support of identity management functionality, e.g. MS Passport, Liberty, Shibboleth, PingID, password managers, form fillers
  2. Systems/applications with another core functionality, but basing on some identity management functionality, e.g. GSM, PGP, eBay
  3. Systems/applications independent from identity management functionality, with some identity management functionality as add-on, e.g., HTML browsers, chat clients

Source: **[BMH2005, Rannenberg04]**

Identity Management
Identity Management Functions

- Provisioning, Enrolling, Choosing
- Binding with Attributes
- Certifying
- Changing
- Unbinding of Attributes
- Deleting
- …?



Identity Management
Types of IdM (Systems)

Type 1		Account Management: *assigned identity* *(= Tier 2)*	by organisation
Type 2		Profiling: *derived identity* *abstracted identity* *(= Tier 3)*	by organisation
Type 3		Management of *own* identities: *chosen identity* *(= Tier1)*	by user himself supported by service providers

➲ There are hybrid systems that combine characteristics

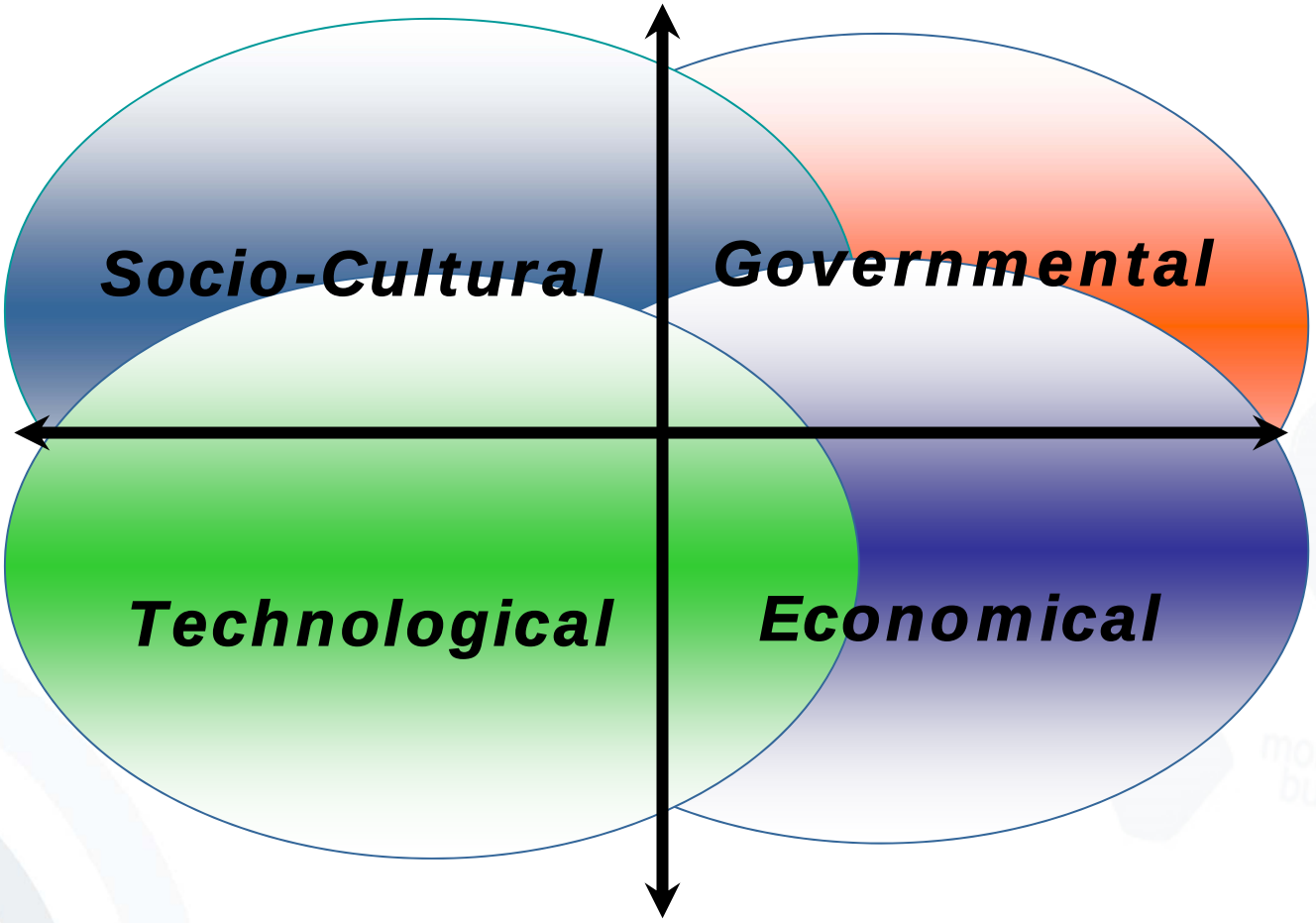
Source: **[BMH2005]**

mobile business

Agenda

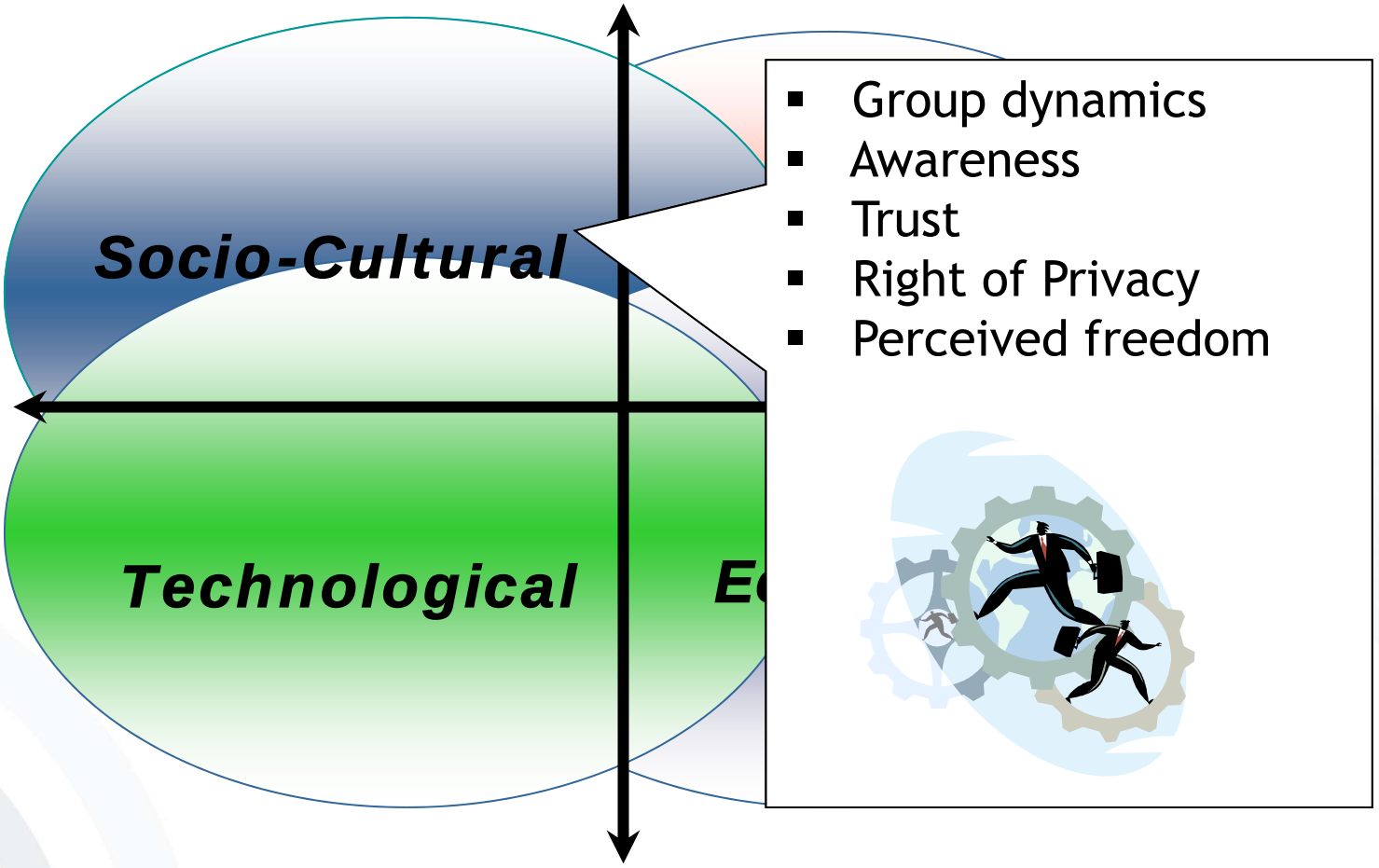
- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies (“Bedarfsträger”) and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Interdisciplinary aspects of Mobility and Identity



Source: **[RR2006]**

Interdisciplinary Aspects Dimension: Socio-Cultural

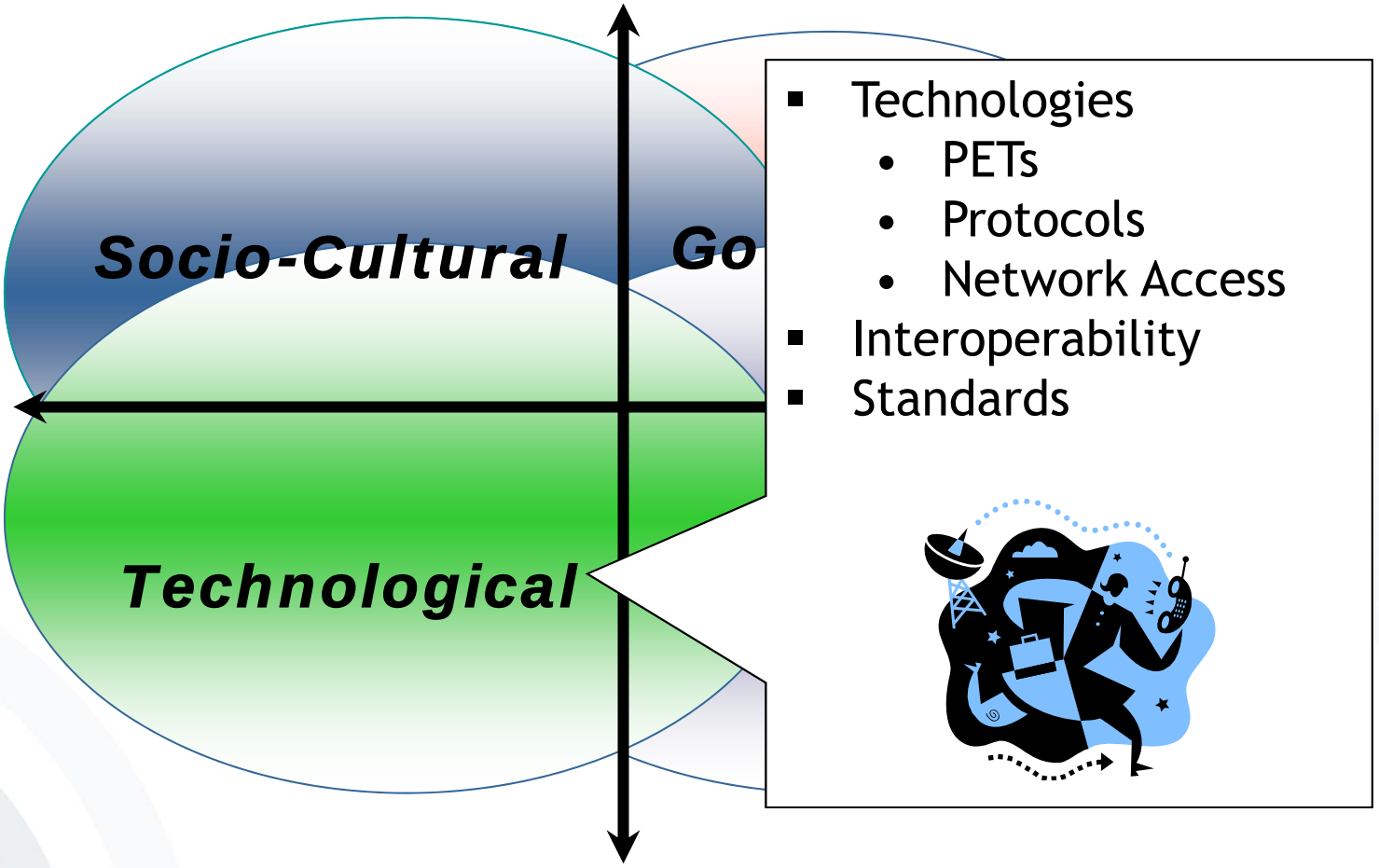


Socio-Cultural Impacts

- *Concepts being observed*
  - *Idem Identity*, categorisation
  - *Ipse Identity*, sense of self

- Analysis of conceptual and sociological issues of the impact of idem-identification on ipse-identity, in the case of mobile devices
  - E.g.: how someone establishes communication using mobile devices
  - E.g.: how we/others perceive ourselves/us

Interdisciplinary Aspects Dimension: Technological

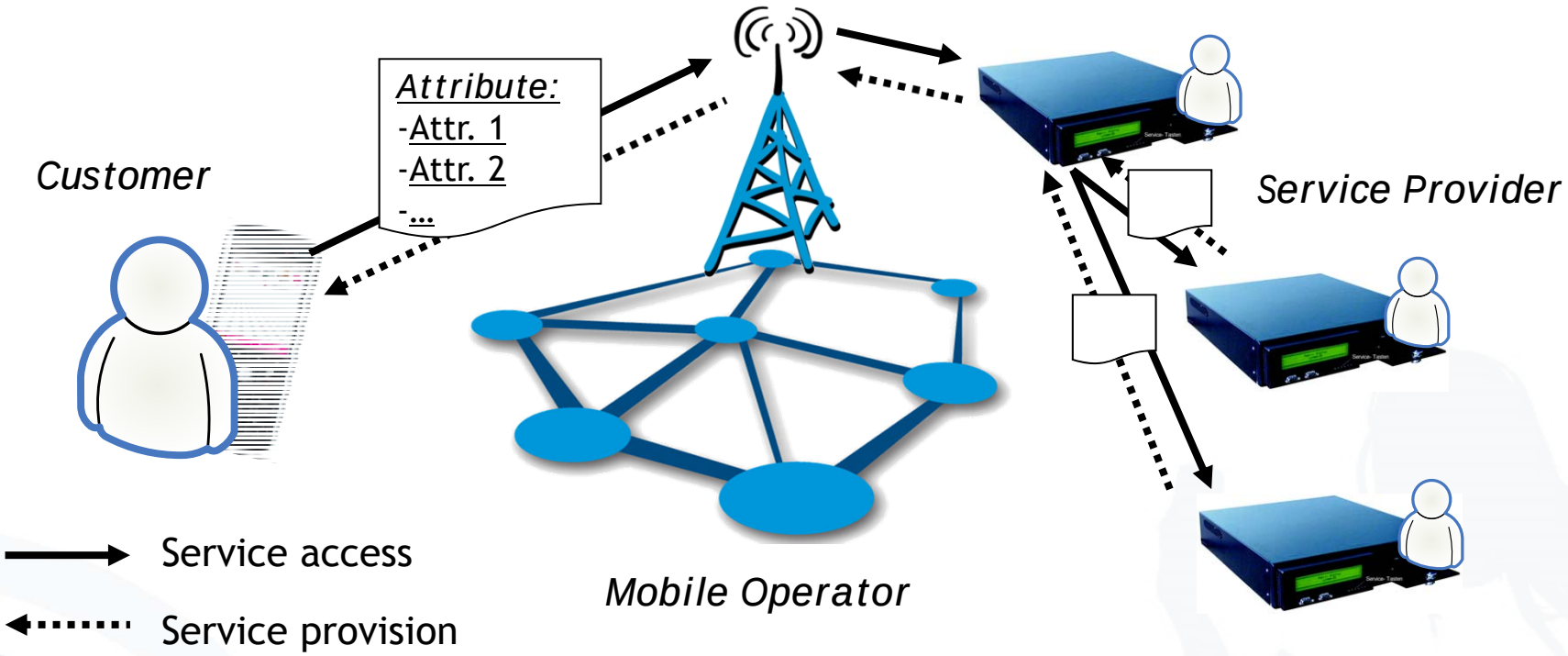


Mobile Identity Management

- Management of identities through the use of mobile devices
  - Management of social interactions in life, rather than Management of mobility

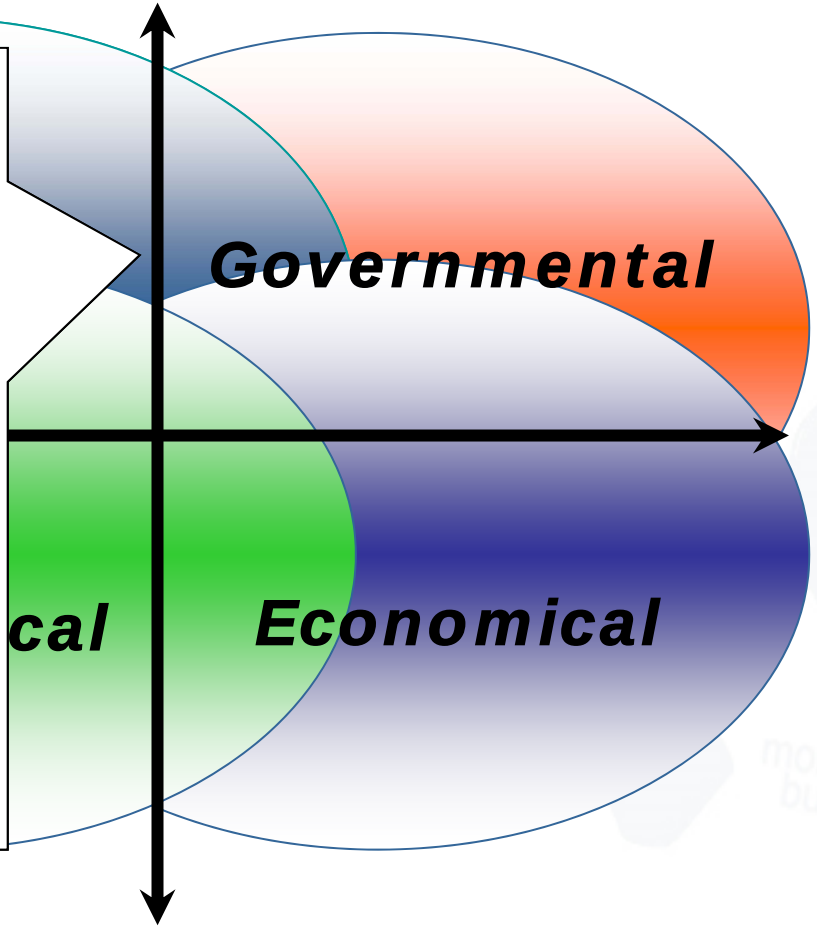
- Management of Mobile Identities
  - Usage of location data

Transfer of Attributes



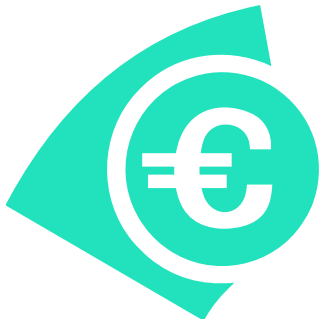
Interdisciplinary Aspects Dimension: Governmental

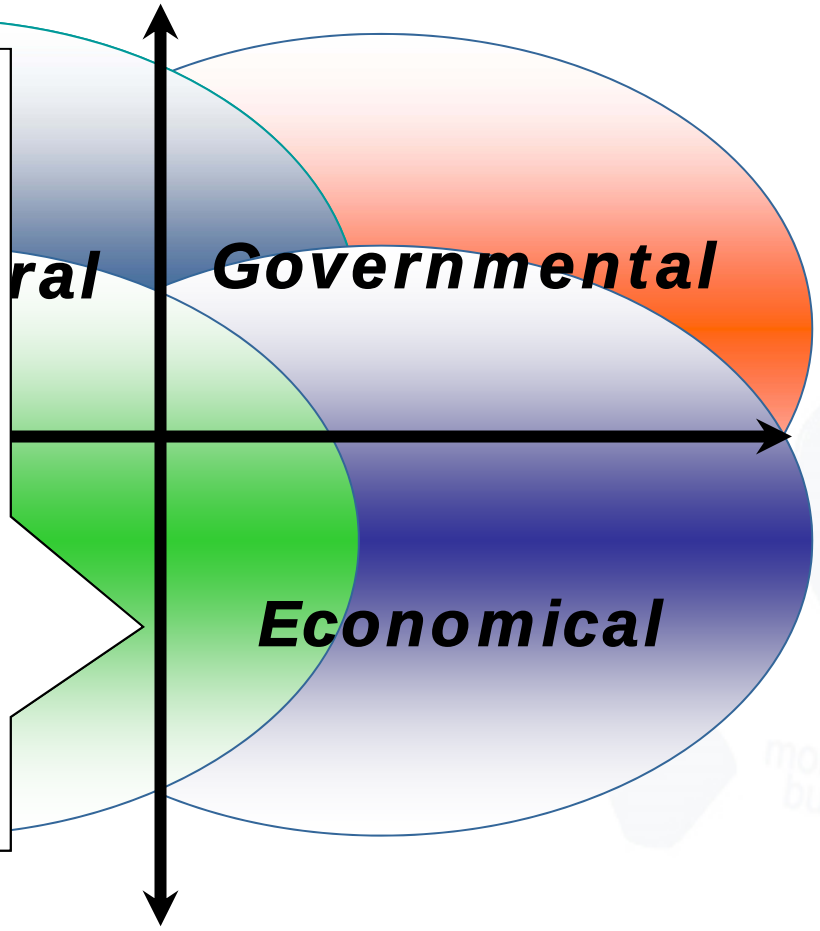
- Laws
- Directives
- Regulations



Interdisciplinary Aspects Dimension: Economical

- Costs and Benefits
- Technology Diffusion
- Return on Investment
- Business Value of IT
- Price of Convenience
- Technology Acceptance
- Business Models





Design Principles for mobile Identity Management

- General success factors:
  - Locality principle
  - Reciprocity principle
  - Principle of understanding

- Protecting the privacy of a user:
  - User controlled linkage of personal data
  - Data minimisation
  - Awareness of data being disclosed
  - Sufficient usability towards the user

References | 1

[AlDK03] Albrecht, H.-J., Dorsch, C., and Krüpe, C. *Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation*, 2003. Available at http://www.mpg.de/868492/pdf.pdf (Last accessed 27-04-2015)

[Allen2016] Allen & Overy: The EU General Data Protection Regulation is finally agreed, www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

[BB2001] Bogdanowicz, M., and Beslay, L. *Cyber-Security and the Future of Identity.* IPTS Report 57, 2001. Available at www.jrc.es/home/report/english/articles/vol57/ICT4E576.htm

[BfDI04] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2004). *BfD-Info 5 - Datenschutz in der Telekommunikation*. Available at http://www.soliserv.de/dateien/BfD-INFO-5-01.pdf (Last accessed 08-04-2008)

[BfDI2021] Kerber, U., BfDI kritisiert Position des Rats zur ePrivacy-Verordnung, https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2021/03_Ratsposition-ePrivacy-VO.html (Last accessed 14-05-2021)

[BfJ2021] Bundesamt für Justiz. *Telekommunikationsüberwachung.* Available at https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html (Last accessed 20-05-2021)

[BlnBDI2002] Der Berliner Beauftragte für Datenschutz und Informationsfreiheit. *Bewertung des IMSI-Catchers aus Sicht der T-Mobil.* Anlagenband ("Dokumente zu Datenschutz und Informationsfreiheit 2001") zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. 12. 2001. Available at www.datenschutz-berlin.de/jahresbe/01/anl/11d9.htm (Last accessed 01-06-2007)

[BMH2005] Bauer, M., Meints, M., Hansen, M. (eds.). *FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*, 2005. Available at http://www.fidis.net/resources/deliverables/hightechid/#c1787

[BNA09] Bundesnetzagentur, Jahresbericht 2008, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2008/Jahresbericht08Id15901pdf.pdf?__blob=publicationFile&v=2 (Last accessed 13-05-2015).

[BNDG07] BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch Artikel 4 u. 10 Abs. 3 des Gesetzes vom 5. Januar 2007 (BGBl. I S. 2). Available at www.gesetze-im-internet.de/bndg/BJNR029790990.html (Last accessed 08-04-2008)

References | 2

[BWG1983] Bundesverfassungsgericht: Entscheidung BVerfGE 65, 1 – Volkszählung; Urteil des Ersten Senats vom 15.12.1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden. Available at www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm (Last accessed 02-03-2007)

[BVG83] Bundesverfassungsgericht: Entscheidung BVerfGE 65, 1 – Volkszählung; Urteil des Ersten Senats vom 15.12.1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden. Available at www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm (Last accessed 02-03-2007)

[BVwG03] Bundesverwaltungsgericht Entscheidung BVerwG 6 C 23.02, 2003. Available at www.bundesverwaltungsgericht.de/enid/d90753334a813794b15cc66003046de0,0976e07365617263685f646973706c6179436f6e7461696e6572092d0933353031/8o.html (Last accessed 08-04-2008)

[CCCB07] Chaos Computer Club Berlin. *Telekommunikationsüberwachung*, 2007. Available at http://berlin.ccc.de/wiki/Telekommunikations%C3%BCberwachung (Last accessed 08-04-2008)

[CMS2021] CMS. ePrivacy Regulation - chronological overview. Available at https://cms.law/en/deu/insight/e-privacy (Last accessed 13-06-2021)

[DeBu2012] Deutscher Bundestag - Verfassungsorgan der Bundesrepublik Deutschland (2012), www.bundestag.de/presse/hib/2012_02/2012_099/01.html (Last accessed 2012-05-03)

[Durand2003] Durand, A. *Three Phases of Identity Infrastructure Adoption.* Available at http://blog.andredurand.com/?p=146

[EuCo2012] European Commission (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (Last accessed 07-04-2017)

[EuCo2016] European Commission (2016). *REGULATION (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).* Available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (Last accessed 11-05-2017)

[EuCo2017] European Commission (2017). *Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions.* Available at http://europa.eu/rapid/press-release_IP-17-16_en.htm (Last accessed 24-04-2017)

References | 3

[Fox02] Fox, D. *Der IMSI-Catcher.* Datenschutz und Datensicherheit (DuD), (26:4), pp. 212 – 216, 2002. Available at www.datenschutz-und-datensicherheit.de/jhrg26/imsicatcher-fox-2002.pdf (Last accessed 08-04-2008)

[Hansen2005] Hansen, M. PRIME & FIDIS: European Projects on Identity and Identity Management, 2005. Available at www.digimagine.de/Hansen-Idmanage-20050308-print.ppt (Last accessed 02-03-2007)

[Heis12] Heise Online. *Karlsruhe beschränkt Verwendung von Telekommunikationsdaten.* Available at www.heise.de/newsticker/meldung/Karlsruhe-beschraenkt-Verwendung-von-Telekommunikationsdaten-1442139.html (Last accessed 03-05-2012)

[Heis21] Heise Online. TKG-Novelle: Bundesrat billigt "schnelles" Internet für alle mit Auflage. Available at https://www.heise.de/news/TKG-Novelle-Bundesrat-billigt-schnelles-Internet-fuer-alle-mit-Auflagen-6041456.html (Last accessed 14-05-2021)

[ISOIEC24760] ISO/IEC 24760-1:2011/2019. *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.* 2019 version available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[LDIN98] Der Bayerische Landesbeauftragte für den Datenschutz (1998). *Aufbau des IMSI-Catchers.* Available at www.datenschutz-bayern.de/technik/orient/imsi.html (Last accessed 08-04-2008)

[PRIME2005] PRIME. General Public Tutorial. Available at https://www.prime-project.eu/tutorials/gpto/

[Rannenberg04] Rannenberg, K. *Identity management in mobile cellular networks and related applications.* Information Security Technical Report; Vol. 9, No. 1; 2004; pp. 77-85; ISSN 1363-4127.

[Royer2006] Royer, D. (ed.). FIDIS Deliverable D11.1, 2006. Available at www.fidis.net/resources/deliverables/mobility-and-identity/#c1793 (Last accessed 08-04-2008)

[RR2006] Royer, D., and Rannenberg, K. *Mobilität, mobile Technologie und Identität.* Datenschutz und Datensicherheit (DuD), (30:9), pp. 571 – 575, 2006.

[SPOL02] Spiegel Online. *Überwachungs-Panne: Verdächtige hatten Abhörkosten auf Handy-Rechnung*, 2002-10-30 (20:09). Available at www.spiegel.de/panorama/0,1518,220595,00.html (Last accessed 08-04-2008)

[StPO] Strafprozessordnung. Available at www.gesetze-im-internet.de/stpo/index.html (Last accessed 08-04-2008)

[WB1890] Warren, S.D., and Brandeis, L.D. (1890). The Right to Privacy, *Harvard Law Review,* (4:5). Available at www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html (Last accessed 08-04-2008)