



*Institut für Rechtsinformatik*

# Legal Implications of Big Data

24th Eicar Annual Conference 2016  
(17.10.-18.10.2016)

RA Benjamin Schütze, LL.M. (Wellington)  
Senior Research Associate



Leibniz  
Universität  
Hannover



## Table of Contents

1. ABIDA (Assessing Big Data)
2. Introduction
3. Definition of Big Data
4. Legal Implication
  - a. Data Ownership / Contractual Implications
  - b. Data Protection and Big Data
  - c. Competition Law and Merger Control

## ABIDA (Assessing Big Data)

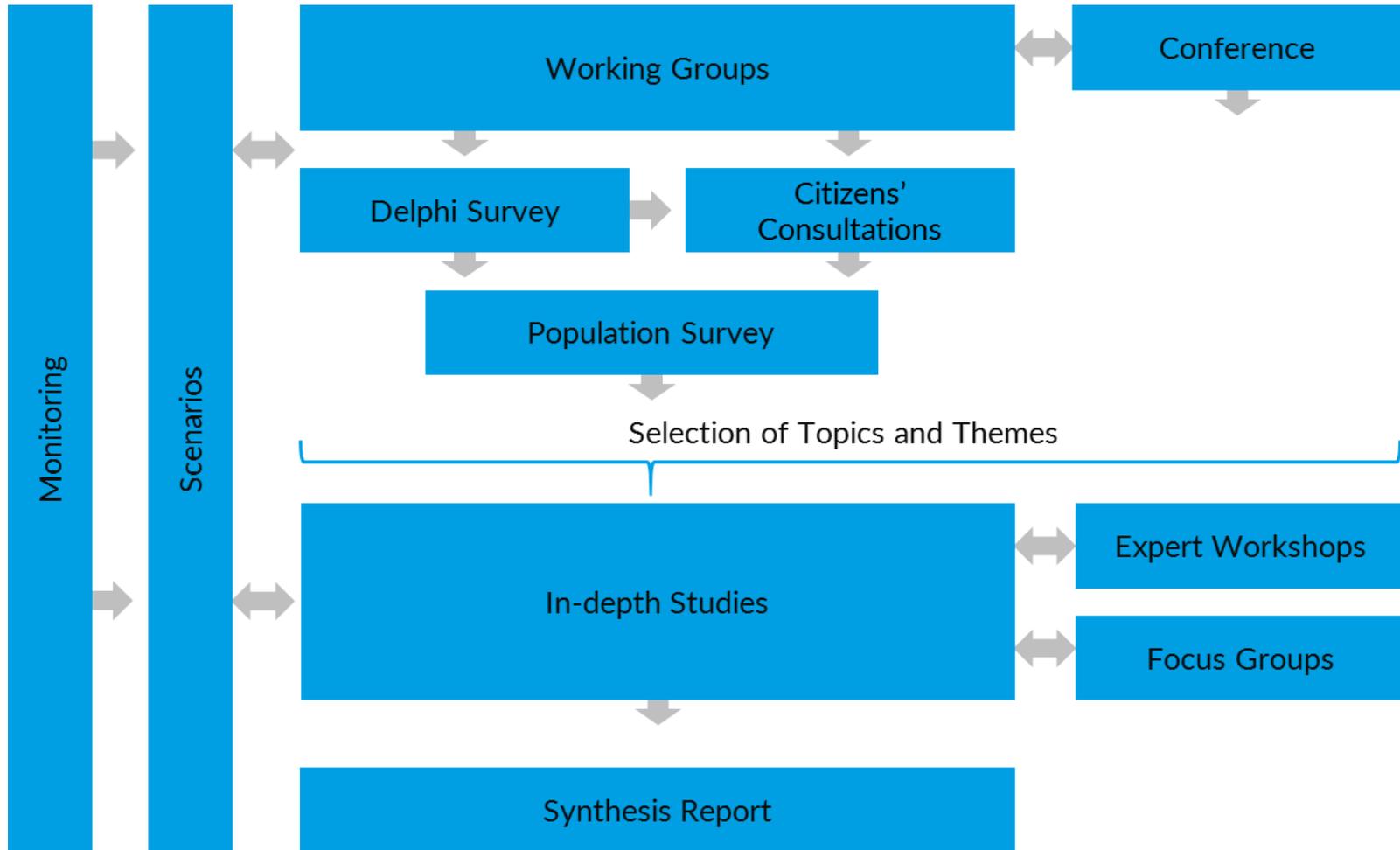
- ABIDA approaches Big Data from an interdisciplinary perspective. Sociologists, philosophers, economists, legal and political scientists work hand in hand.
- The project aims to gather existing disciplinary knowledge on Big Data and make it accessible to the public.
- The project examines the societal impact associated with Big Data by using the methods of technology assessment oriented to dialogue and participation.

SPONSORED BY THE





# ABIDA Project Structure





## Working Groups

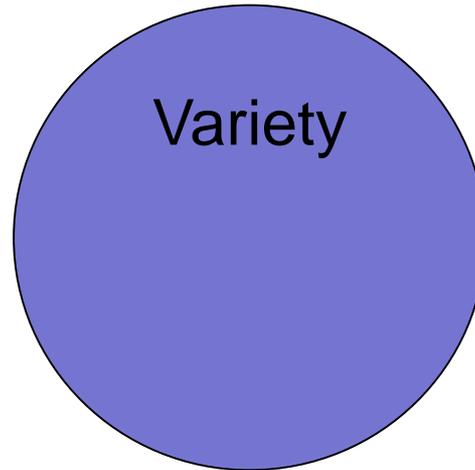
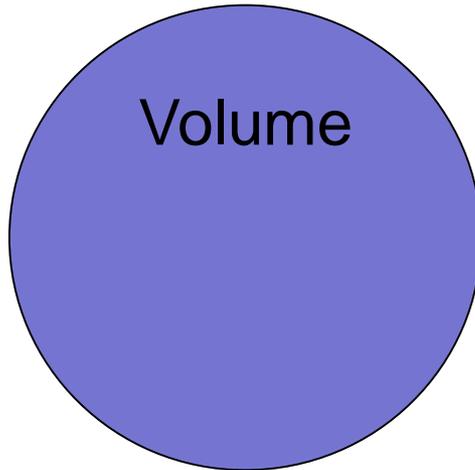
The purpose of the working groups is to combine and prepare existing disciplinary knowledge about Big Data.

There are five disciplinary working groups consisting of five to eight experts each:

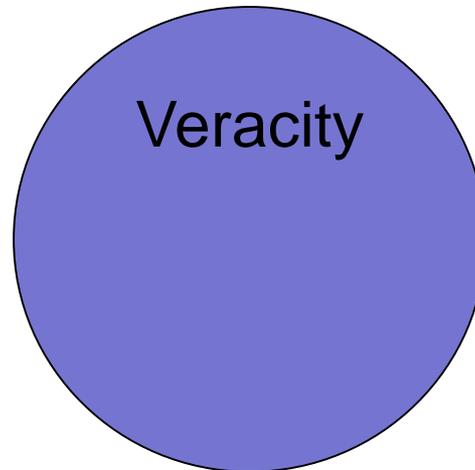
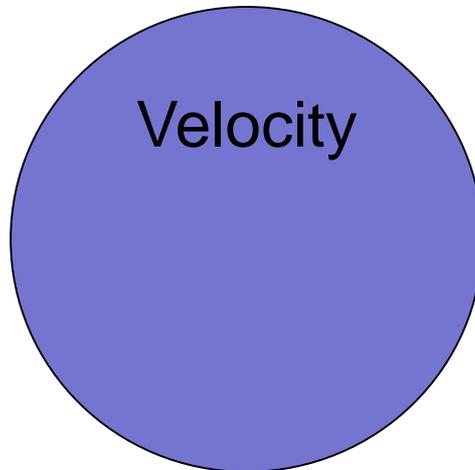
- **Law**
- **Ethics**
- **Economics**
- **Sociology**
- **Political Science**



## Big Data Definition

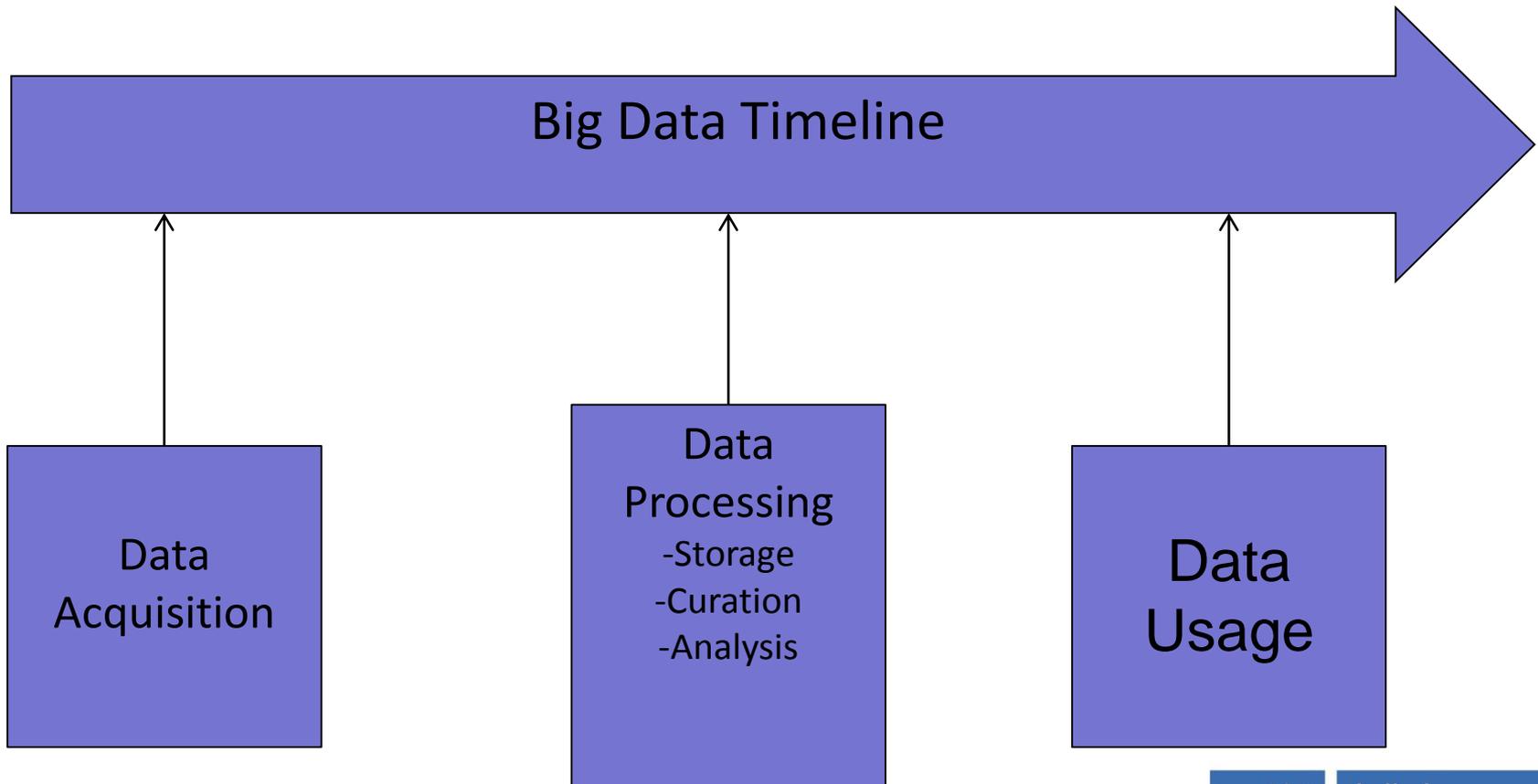


Laney, D., 3D data management: Controlling data volume, velocity, and variety. Technical report, META Group (2001).





## Steps of Data Handling



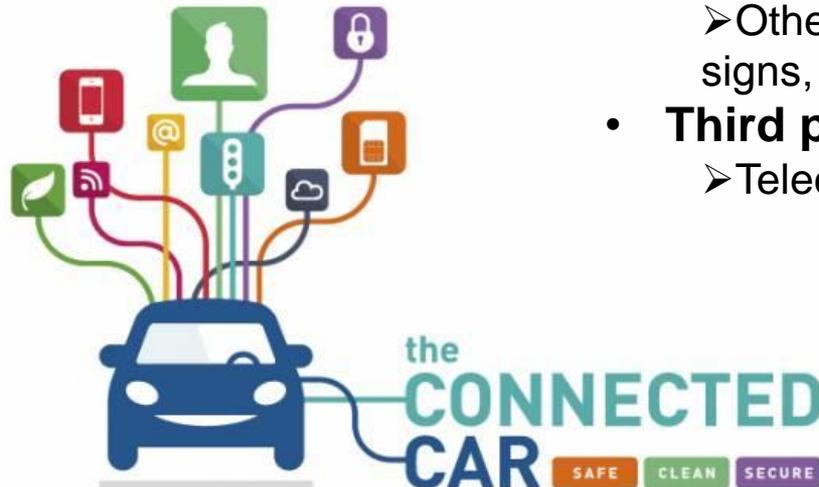


## Table of Contents

- Legal Implication
  - a. Data Ownership/Contractual Implications
  - b. Data Protection and Big Data
  - c. Competition Law and Merger Control

## Example: Connected Cars

- **Car related data:**
  - Position, speed, acceleration, brake handling, condition of the car (battery, brakes, engine, exhaust)...
- **Driver - / passenger related data:**
  - Identification: PIN, password, credit card, biometric data,
  - Car handling: driver, individual preferences, health data (fatigue, alcohol,...)...
- **Environmental data:**
  - Other cars, pedestrians, road and traffic signs, traffic incidents and accidents...
- **Third party related data:**
  - Telecommunication provider, app provider





## Connected Cars – Who might have a legitimate Interest in data?

- Owner
- Driver
- Car manufacturer
- Subcontractor
- Car navigation provider
- Insurance companies („pay as you drive“)
- ISPs (distribution and marketing channel)
- Government and public agencies (traffic control, toll collection, eCall, crime prevention)



## Data Ownership (1)

- Sec. 903 Civil Code (CC) – Power of the Owner

„The owner of a thing may, to the extent that a statute or third-party rights do not conflict with this, deal with the thing at his discretion and exclude others from every influence.”

- Sec. 90 CC “Only corporeal objects are things as defined by law.”
- Ownership of the data carrier = Data ownership?
  - P: Cloud-Storage and data centres



## Data Ownership (2)

- **Sec. 93 CC:**

„Parts of a thing that cannot be separated without one or the other being destroyed or undergoing a change of nature (essential parts) cannot be the subject of separate rights.“

- Parts of a thing also only apply to corporeal objects.

- **Sec. 903 CC applied by analogy?**

- Comparable interest?



## Data Ownership (3)

- **Sec. 823 (1) CC:**

- Protection of integrity of Data is widely recognized
- Protecting is limited, however, to destruction and modification of data.

- **Sec. 202a, 303a Criminal Code?**

Power to factually exclude others, is used as a point of reference and shall be granted to the person, who first stores the data („Skripturakt“) as a beneficiary (i.e. the data producer).

- Sec. 202a, 303a Criminal Code only protects access to and integrity of data.
- Scope of this concept transferred to civil law is therefore unclear



## Data Ownership (4)

- **Copyright:**

Art. 2 (2) CA “the author's own intellectual creations constitute works within the meaning of this Act.”

- Copyright is limited to data (or information) with a minimum of creativity and individuality and is limited to “human” creations
- Raw data generated by sensors or machines would not be covered



## Data Ownership (5)

### Database Protection (Sec. 87a CA)

Database right shall protect investment in generation and maintenance of a database. Sufficient or substantial investment must be made.

- Database right does not protect data as such, but only data that originates from a protected database. This again excludes sensor or machine generate data as long as such data is not collected in database
- According to CJEU case law, generation and collection of data must be strictly separated. Only an investment into the „collection“ of data shall be protected.
- Only reuse of „substantial“ parts of a database violates database rights.



## Data Ownership (6)

### Trade Secrets (Sec. 17 AAUC)

Protection of trade secrets and know how has some features of property.

- Does not grant an absolute right on data, but is based on factual secrecy and depends on technical, organisational and contractual measures sufficient to protect the confidential nature of the information
- No substantial changes under new Directive on Protection of know how and trade secrets (Directive (EU) 2016/943), that requires „reasonable steps under the circumstances“ to keep the information secret



## Data Ownership (7)

### Data Protection (DPA, GDPR)

Data Protection law is applicable to personal information only, i.e. data must be related to a natural person.

- It only provides a specific set of remedies, which as a precondition require that both legitimate interests of the data subject as well as the data controller are taken into account and weighted against each other
- In Germany there is some discussion as to whether extending data protection law into some kind of tradeable exclusive right, but this debate is still ongoing



## Data Ownership (8)

### Data Protection (DPA, GDPR)

- Proposal of a directive on certain aspects concerning contracts for the supply of digital content Art. 3 (Scope) reads: “This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data”



## Data Ownership (9)

### Contractual Agreements

Regardless of its unclear legal status, data may of course be subject to contractual arrangements. And concluding a data license agreement became a common practice. Contractual agreements, however, have a major disadvantages

- Due to privity of contract, only the parties to the agreement are bound by it



## Data Ownership (10)

### Create a new exclusive right?

- Is a new exclusive right really needed?
- Counterarguments
  - An exclusive right in data would be a paradigm shift in the protection of information
  - Unclear how a right in data shall be delineates from other intellectual property rights
  - How to specify a right to data and to who shall it be allocated



## Data Protection (1)

Data Protection Law in Europe is currently harmonized by Directive 95/46/EC (Data Protection Directive – DPD) DPD will be replaced by the General Data Protection Regulation (GDPR) in 2018.

Big Data poses significant challenges to the European data protection framework. Some of the key aspects are:

- Definition of personal data, anonymisation and pseudonymisation
- Purpose Limitation
- Informed Consent
- Transparency and Information Duties
- Profiling and automated decision making



## Data Protection (2)

### Definition of personal data anonymisation and pseudonymisation

- According to Art. 4(1) GDPR „an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person“
- According to Recital 26 DPD to determine whether a a person is identifiable “account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person”
- The more data is readily available, the lower the threshold at which the requirement “reasonable means” will be fulfilled



## Data Protection (3)

### Purpose Limitation

- One of the cornerstones of data protection principles. It means that data processing always requires a purpose that must be clearly defined before the data is collected (processed).
- It also means that data cannot be reused for another purpose that is incompatible with the original purpose
- Problem for Big Data analytics in case where data shall be used for purposes that have not been foreseen by the time the data has first been collected



## Data Protection (4)

### Informed Consent

- Consent is one of several legal grounds to process personal data. I may only operate as legitimate ground for processing if the data subject has unambiguously and freely given his/her consent.
- More challenging is that the data subject must also be informed about what they are consenting to (informed consent).
- Data subject must be given accurate and full information of all relevant issues such as nature of the data processed, purposes of the processing, further recipients of personal data and the right of the data subject.



## Data Protection (5)

### Transparency and Information Duties

- Stand alone principles of data protection that is connect to informed consent. But not only in cases where data processing is based on the consent of the data subject, it must be provided with clear and unambiguous information on how his/her personal information is processed.



## Data Protection (6)

### Automated decision making

- It means to take a decision that is based on personal information solely by automatic means. According to Art. 15 DPD, if such automated decisions are likely to have significant impact on the data subjects to which they relate, a certain level of legal protection is required to avoid inappropriate consequences with regard, for instance to, an individual's creditworthiness or performance on the job.
- Data subject shall have the right to review the decision.
- For Big Data scenario, the challenge is again to ensure transparency.



## Competition and Antitrust Laws

Fairly recently Big Data became subject of interest of antitrust and competition law legislators.

- So far competition authorities focused on search engines and social networks.
- **Merger Control** (Google/DoubleClick and Facebook/WhatsApp)
- **Misuse of market power** (German Federal Cartel Office/Facebook). Does Facebook use its dominant position to impose privacy terms that would otherwise not be accepted?



Benjamin Schütze – [schuetze@iri.uni-hannover.de](mailto:schuetze@iri.uni-hannover.de)  
[iri.uni-hannover.de](http://iri.uni-hannover.de)  
[www.abida.de](http://www.abida.de)

