Big Data & Ethics – some basic considerations

Markus Christen, UZH Digital Society Initiative, University of Zurich

Overview

We will approach the topic “Big Data & Ethics” in a three-step-procedure:

Step 1: Introduction-Exercise – your feelings related to Big Data applications in research and beyond (30’)

Step 2: Input-Talk: Big Data & Ethics (45’, followed by a break)

Step 3: Group work & group presentations: Applying the input in some (fictitious) research examples (90’)

Step 1 – Introduction exercise

Exercise: Your personal «creepiness» factor

How the exercise works:

1) **Each of you gets a card that shortly explains a (fictitious) Big Data application that you experience as research participant or consumer.**
2) **You briefly think how «creepy» you believe this application is.**
3) **Each of you will arrange «his/her» application along the «creepiness» scale and you briefly read your example and justify the position of the card.**
4) **In a second round you are able to re-arrange one card of which you believe that the card is at the wrong place (again justify your re-arrangement)**

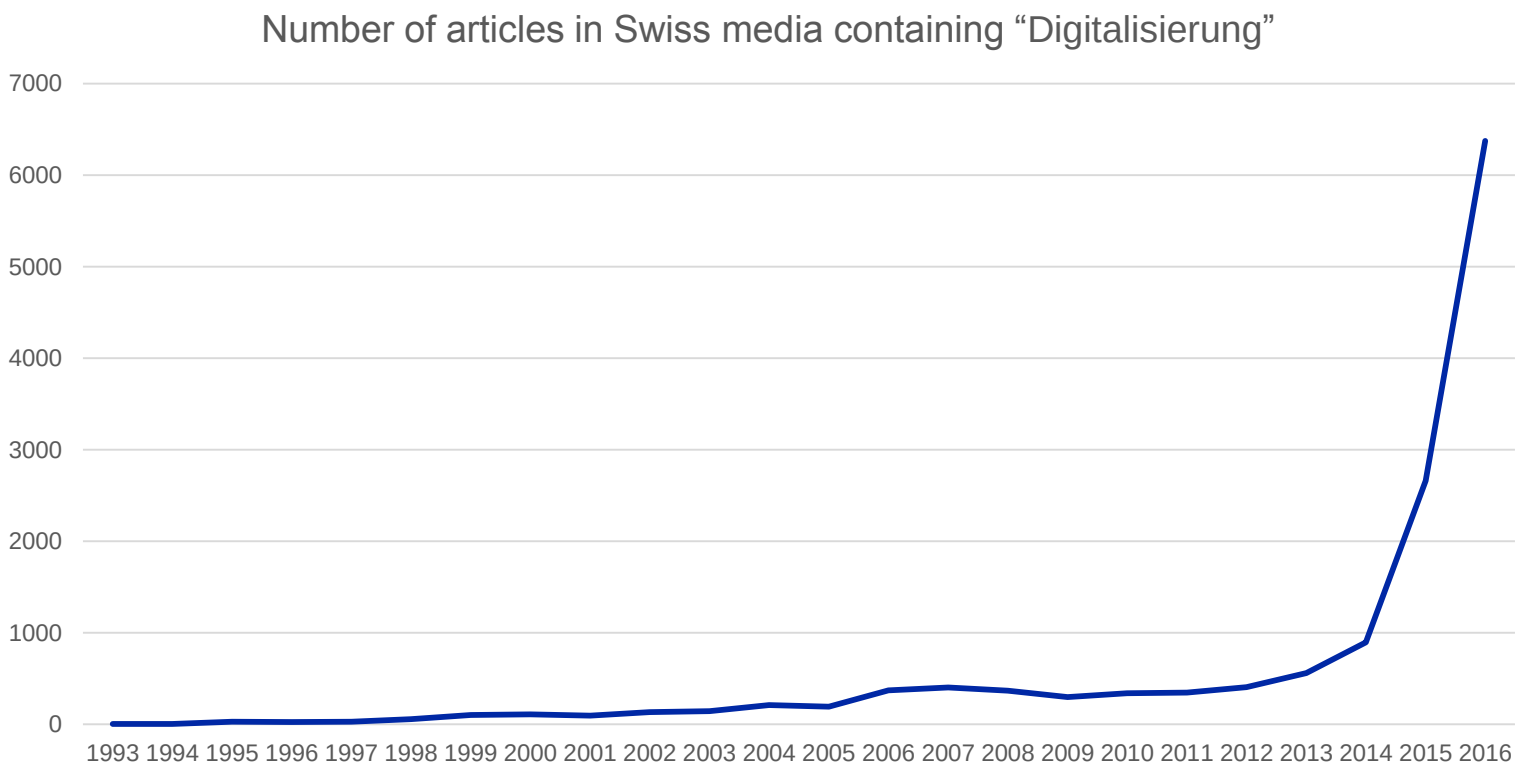
Part 2 – Big Data and ethics

Overview Input-Talk

- Some introductory remarks
- Basic legal considerations & problems
- Big Data in the scientific literature
- The “fundamental challenge”
- Ethical core concepts
- Translating ethics into scientific practice

Some introductory remarks

Context: Digitalization



Obviously, everyone is talking about «digitalization»

The discussion has some elements of a «hype»

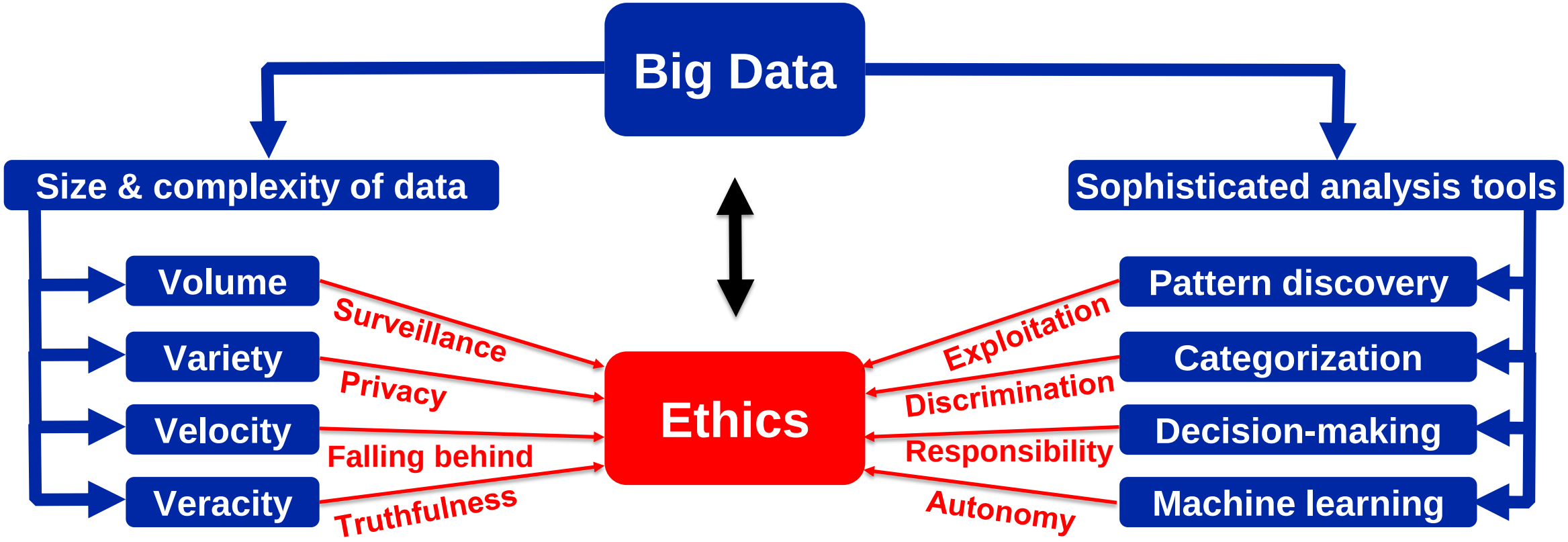
Source: Factiva; Search in CH newspapers, magazines, press agency releases containing «Digitalisierung»

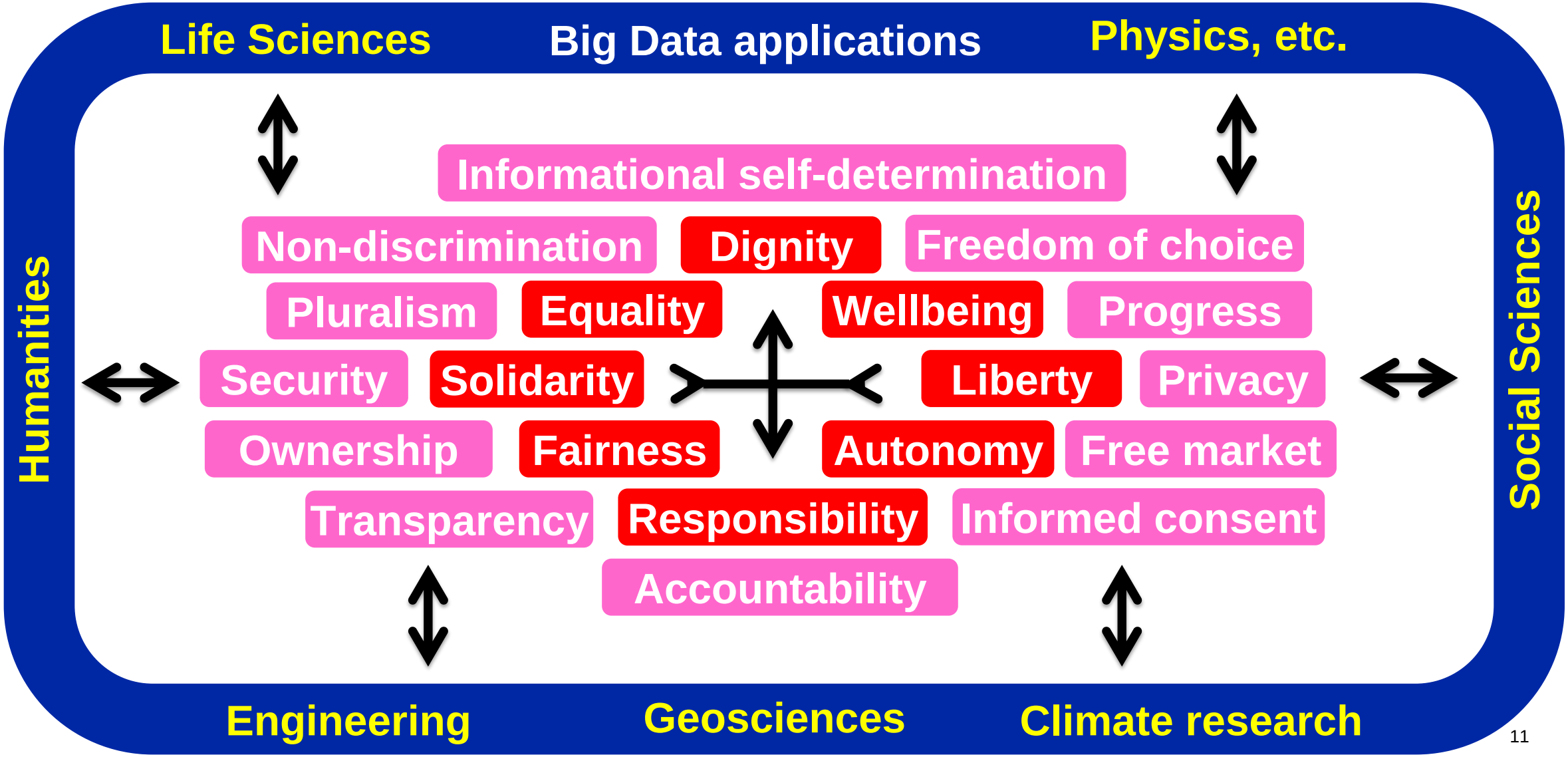
Big Data – between the extremes

Big Data is the «oil of the 21st century»; an enormous resource for innovation.

Big Data is a fundamental thread of freedom and privacy

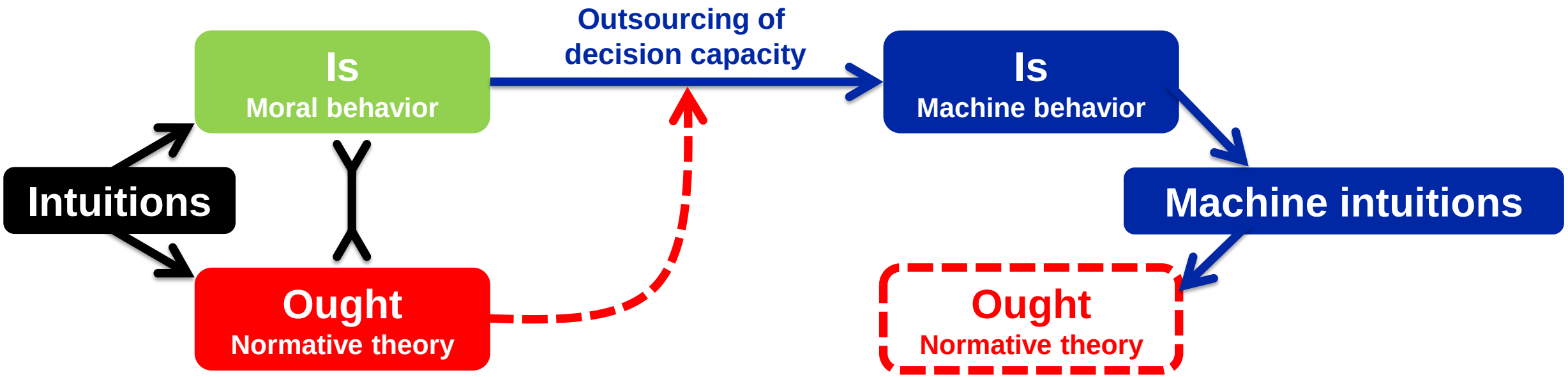
How Big Data interrelates with ethics




Life Sciences
Big Data applications
Physics, etc.
Humanities
Social Sciences
Informational self-determination
Non-discrimination
Dignity
Freedom of choice
Pluralism
Equality
Wellbeing
Progress
Security
Solidarity
Liberty
Privacy
Ownership
Fairness
Autonomy
Free market
Transparency
Responsibility
Informed consent
Accountability
Engineering
Geosciences
Climate research

"Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves."

Chris Anderson, Wired, 2008



Basic legal considerations & problems

Legal framework (1)

The legal framework of data protection relies on a foundation that has been created in the 1970s(Switzerland: «Datenschutzgesetz», currently under revision; EU: «General Data Protection Regulation», will become effective in 2018).

A few core concepts:

- **Personal data:** all type of information that concerns a (identifiable) person.
- **Identifiable** is a person, when her identity can be referred through the data itself, using the context of the data or through the combination of data without disproportional efforts.
- **Data processing** concerns any way of dealing with data, independent from the tools or methods used, in particular the collection, storing, using, curating, disclosing, archiving or erasing of data.

Legal framework (2)

Further basic principles:

- **Recognizability:** The collection of personal data has to be recognizable for the person on which data is collected.
- **Consent:** The person has to provide informed consent to data acquisition and she can revoke her consent.
- **Purpose orientation:** The purpose of data collection has to be disclosed for the person and the data can only be used for this specific or for foreseeable purposes.
- **Appropriateness:** The data processing has to be accurate to the purpose of data collection and has to be acceptable to the person whose data is collected.
- **Data minimization:** It is only allowed to collect and store data for the envisaged purpose.
- **Exceptions** are possible due to a predominant public interest, but they usually require a specific legal grounding.

Tensions between the law and Big Data practice

Big data applications also use automatically collected data and the affected person is unaware of the existence and transmission of this data.	⟷	Breach of the principle of recognizability
The innovation content of big data applications lies often in the multiple application and recombination of data.	⟷	Breach of the principle of purpose orientation
Big data applications rely on the fact to collect much data and combine many kinds of data.	⟷	Breach of the principle of data minimization

Big Data in the scientific literature

«Big Data» is a young phenomenon

The expression «big data» is almost inexistent before 2011.

The first article that used the expression «big data» in its current understanding appeared 1998.

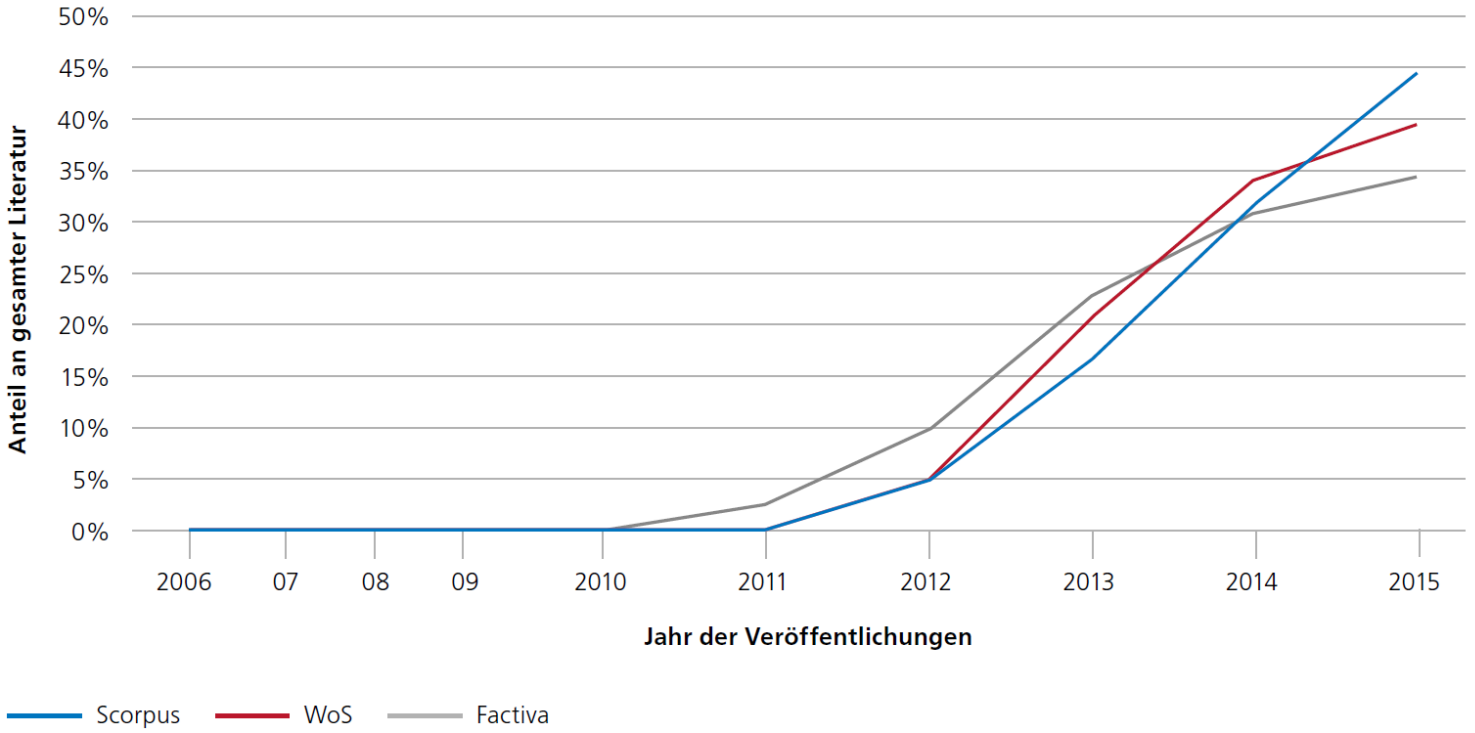
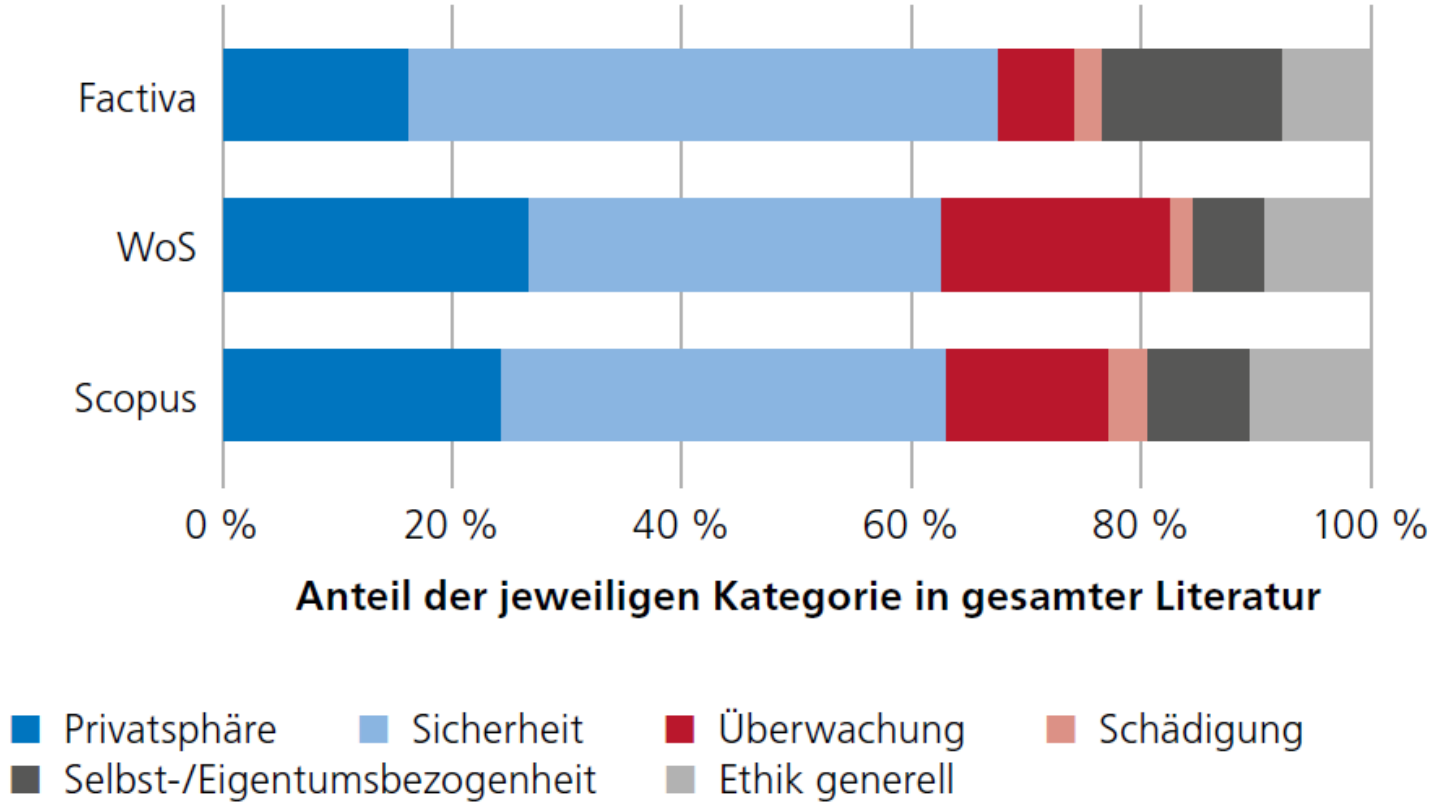


Abbildung 1: Anteil der pro Jahr veröffentlichten Big-Data-Papers gemessen an der Gesamtmenge aller Papers von 2006 bis 2015 pro Datenbank

Differences in the weight of ethical questions

The topics «data security» and «self/property relation» are much more present in the general media compared to the scientific literature, where classic topics of computer ethics such as privacy and surveillance are quite strong.



Ethical questions attract interest

When comparing the disciplinary profile of highly cited big data papers with those papers citing them, then the fraction of social sciences & humanities increases (from 6,6% to 13,2%), indicating that big data gains interest in those fields.

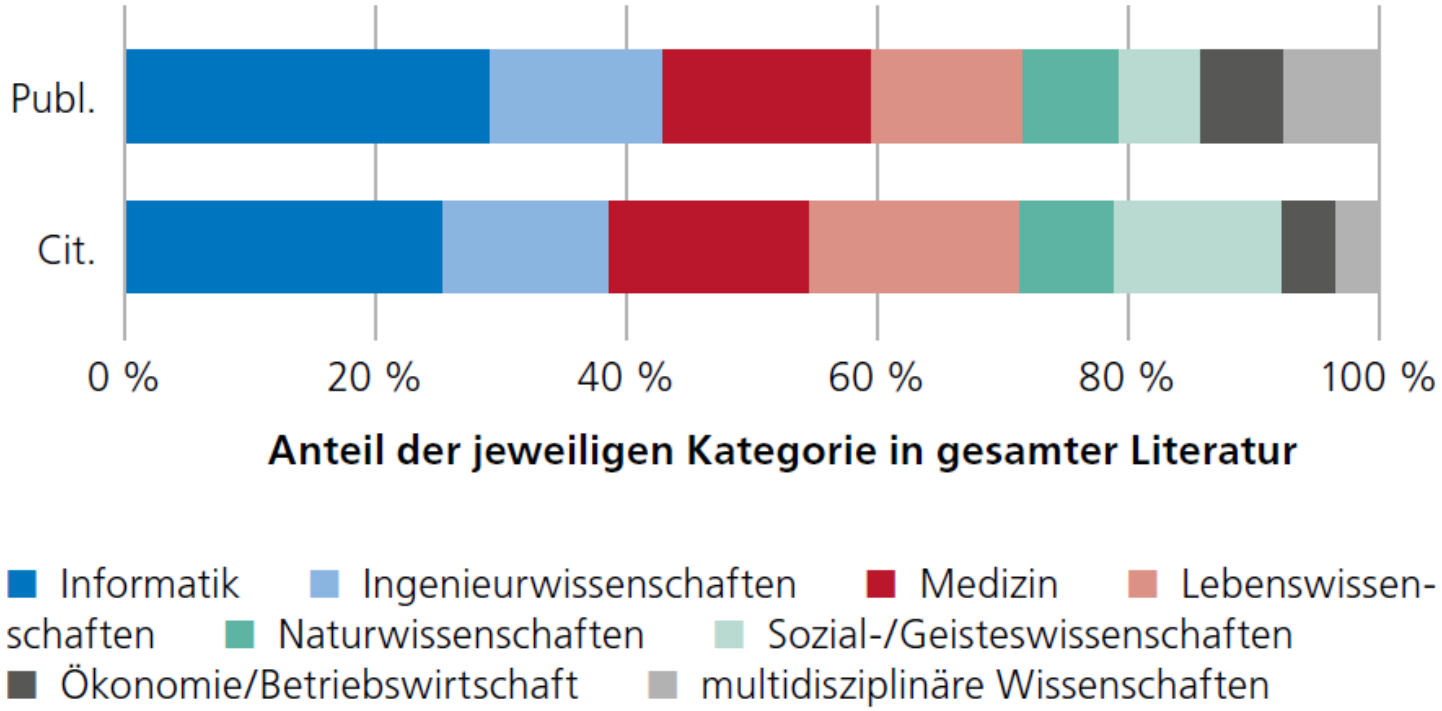


Abbildung 4: Inhaltliche Verteilung der hochzitierten Big Data Paper sowie der diese Arbeiten zitierenden Paper.

The “fundamental challenge”

Social spheres and their moral foundation

In 1983, the philosopher Michael Walzer introduced the theory of *spheres of justice*, which proposes that societies consist of different social spheres (e.g., medical, political, market, family and educational), whose characteristics are:

- Each sphere is defined by **different types of goods** that are central to that particular sphere (e.g.: health, seat in the parliament, income, family relationship, college degree).
- Within each sphere, those goods have their **own associated criteria, principles and mechanisms** concerning their distribution and allocation.
- The ethical problem is to **prevent mixing up** distributional criteria and goods from different spheres. For example:
  - Allocating seats in parliament on the basis of financial assets
  - Make health care dependent on family relationships or college degrees.

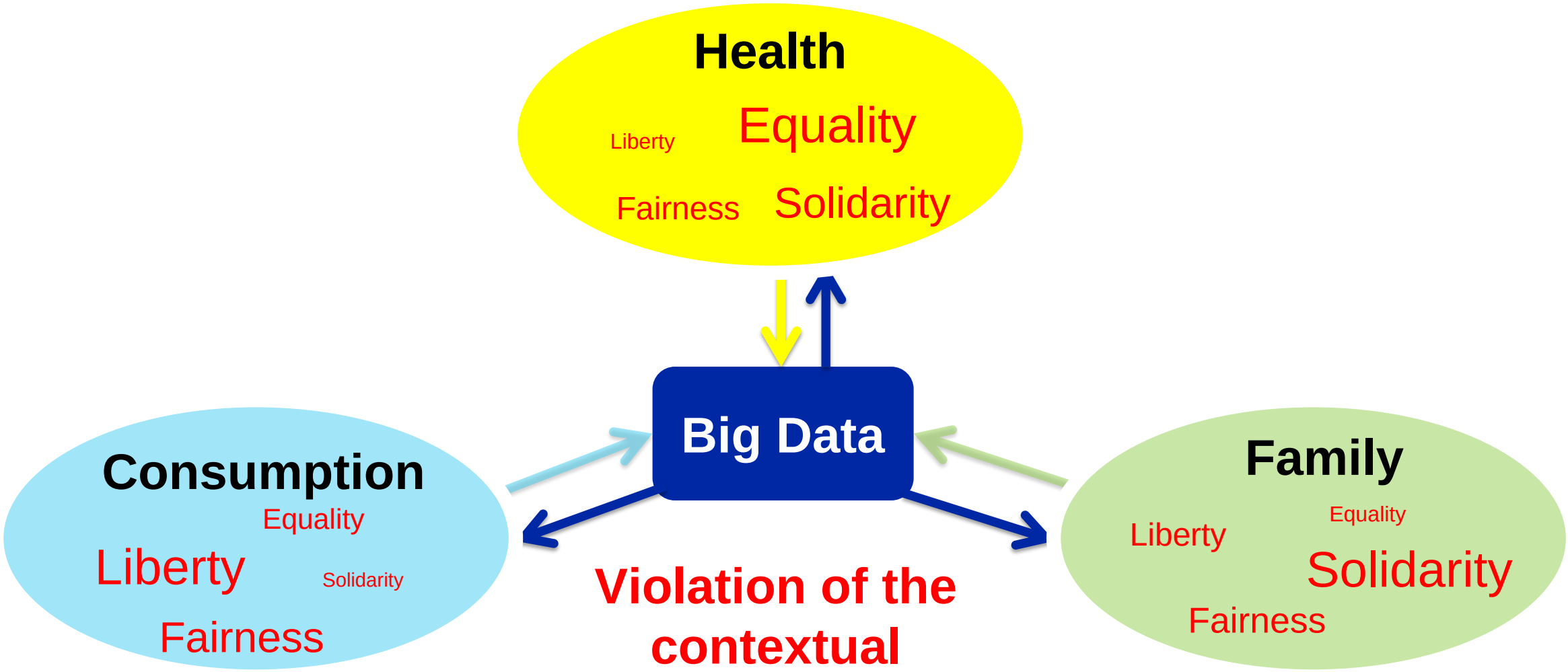
What is needed according to Walzer is an "art of separation" of spheres in order to prevent that a single good dominates all spheres.

The digital undermining of spheres

The general challenge is that since information produced within these spheres travels much faster and is more difficult to control than in the traditional offline world, we face a set of phenomena that threaten the integrity of social spheres and the cultural and social meanings expressed in them, including our values:

- **With respect to data collection:** The integration of heterogeneous data (the core business of data brokers) describing the activity of individuals in different social spheres enable detailed inferences on the individual.
- **With respect to actual behavior:** interconnected information technologies blur boundaries that societies use to demarcate different social contexts (social networks become banks, friends become marketeers, shop keepers become intelligence officers)

Of course the boundaries between spheres are to a certain extent relative to time and culture, but it is important to note that every age, society and culture does draw and treat these boundaries as of high normative relevance. This implies that changes to them need to be morally justified.


Health
Liberty
Equality
Fairness
Solidarity
Big Data
Consumption
Equality
Liberty
Solidarity
Fairness
Family
Equality
Liberty
Solidarity
Fairness
Violation of the contextual integrity of data!

Illusions of control and informed consent

The answer to this problem – information sharing in the context of digitally blurred social spheres – is usually that that the individual should have **control over his or her personal data**. However, this is problematic:

- When individuals use digital platforms, they are often in a position of **informational asymmetry**: they are not aware of the informational links between social spheres that are generated in this way.
- In the context of Big Data, the amount of information extracted from data might **exceed ex-ante expectations** of both users and platform providers.
- The orientation on autonomy puts the focus on the individual and **disregards the moral obligations of the other players** involved.

A "minimal ethics" focusing on autonomy and informed consent disregards the "empirical undermining" of autonomy and consent capacity and neglects other morally relevant values.

Ethical core concepts

Contextual integrity

Contextual integrity is inspired by the idea of *spheres of justice*:

- Societies consist of different social spheres. The major **ethical challenge** is to prevent the domination of a single good, distribution mechanism, principle etc. *across spheres*.
- "Translating" this idea to the **information sphere** (Nissenbaum 2004) means that the type of information that is revealed and the flows between different spheres have to be *appropriate for the context*.
- Van den Hoven (2008) considers four different moral reasons to constrain flows of information. Next to the prevention of inequality based on Walzer, he points to information-based harm (e.g., through discrimination), the exploitation in markets and moral autonomy.

A problem with this conception is ethical pluralism, i.e. even within a single sphere, people may disagree on what exactly the relevant values and principles are.

Autonomy as an (insufficient) “meta-value”

Due to ethical pluralism, **autonomy** has become a “meta value” in the sense that it justifies the acceptance of ethical pluralism (within some boundaries) and the right of the individual to act according to own (interpretations of) moral values within the different social spheres.

Autonomy furthermore provides the moral foundation of the idea that an individual executes **control** over relevant decisions, actions etc. within social spheres. This goes along with abilities to execute autonomy (and missing abilities may justify bypassing decisions made by the individual).

In this framework, **informed consent** becomes the key requisite when the individual is involved in activities which are outside of its direct control, but it involves the notion of “indirect control” (some prediction regarding the consequences of consenting)

Contextual integrity is likely to be the precondition for the “empirical” foundation of autonomy/informed consent: control & prediction.

Relevant values

In the following, it is proposed that the following three values provide a better outline of the moral landscape associated with contextual integrity:

Autonomy: Users ought to be aware of how their data records are used in order to promote their values and gain control over privacy-related choices.

Fairness: The benefits of knowledge and information ought to be fairly apportioned to all participants in interactions, so as to rule out inequality of opportunity and exploitation by some at the expense of others.

Responsibility: Users (both researchers and data providing research subjects) should be held responsible and accountable for the ways in which they use their personal information and the information about other people. If some subjects are wronged, it must be possible to attribute personal responsibility for the wrongs in question.

Fairness and discrimination-prevention

Some issues related to fairness:

- **Behavioral targeting:** Suppose that a service comes along with immediate benefits in non-material form (recommendations). One concern is that – based on consumer behavior –, the agencies learn habits and personal traits of users that can be used for price discrimination or "price gauging", or that some items might even not be offered
- **Statistical harm:** Unfair decisions have been observed in a number of settings, including credit, housing, insurance, personnel selection and worker wages, web advertising and recommendation (Romei & Ruggieri 2014).

Discrimination is not necessarily unethical per se, but have to be addressed and analyzed with respect to their justification and counteracted if unjustified.

Responsibility and accountability

Requiring consent is not merely an act to protect a person from unwanted harm. It also involves an explicit agreement to contribute to something that the person considers to be a valuable goal. Consenting has a positive motive (e.g., compassion) and entails the notion of responsibility:

- First, the consenting person trusts that the researcher will deal responsibly with this data – both with respect to preventing privacy breaches as well as with respect to the goal of the study.
- Second, the consenting person may be set in a position to control data use. One may consider a model of “data stewardship”, i.e. an institutional setting that allows tracking data usage and regularly report on how the personal data of people has contributed to research.

Ensuring trust and responsibility will have to be “materialised” through technological solutions that can be understood by both the users of Big Data technologies as well as those who provide the (Big) data.

Translating Ethics into Practice

General data management requirements

Independent of any ethical issues that emerge when data is created that allows inference on persons, there are some general data management requirements:

Data Access: Data from public funded projects should be open and accessible, which has several implications:

- Formal requirements (such that the data can actually be accessed and used)
- Need to find ways to credit for data production & data curation
- Culture change in institutions & single researcher

Data Security: Secure your data both from unauthorized access as well as from sabotage (ransomware)

Supporting autonomy

- Enable research participants to gain awareness on what guides their choices (privacy preferences), e.g. through a privacy preferences self-assessment tool that will provide a value profile that outlines the privacy preferences of participants with respect to their participation in research or data donation.

- Provide information (to participants and researchers) on what they potentially may disclose when providing certain types of data. This may include a security issues taxonomy; i.e. forensic and security assessment of relevant risks when using the platform, including the generation of operational security guidelines on (technology and non-technology related) behavioral and tool usage rules for researchers and participants.

The goal is to shift away the focus from (mere) informed consent towards empowering research participants and data donators.

Safeguarding fairness

- Provide a broader set of utilities (not only monetary compensation) like visualizing the contribution of research participants, e.g. through donated data, to certain scientific results.

- Create novel types of interactions (using, e.g., co-private protocols, Domingo-Ferrer 2011, and, more generally, co-utile protocols, Domingo-Ferrer et al. 2015) that allow collaborative contribution to a common good (like ensuring each other's privacy).

- Provide anti-discrimination tools, i.e. models and protocols of data acquisition and analysis for quantifying the risk of discriminatory decisions as a (possibly unwanted) consequence of data profiling and data mining.

The goal is to demonstrate that contributing to research is based on a fair exchange and mutual respect of the involved parties.

Enabling responsibility

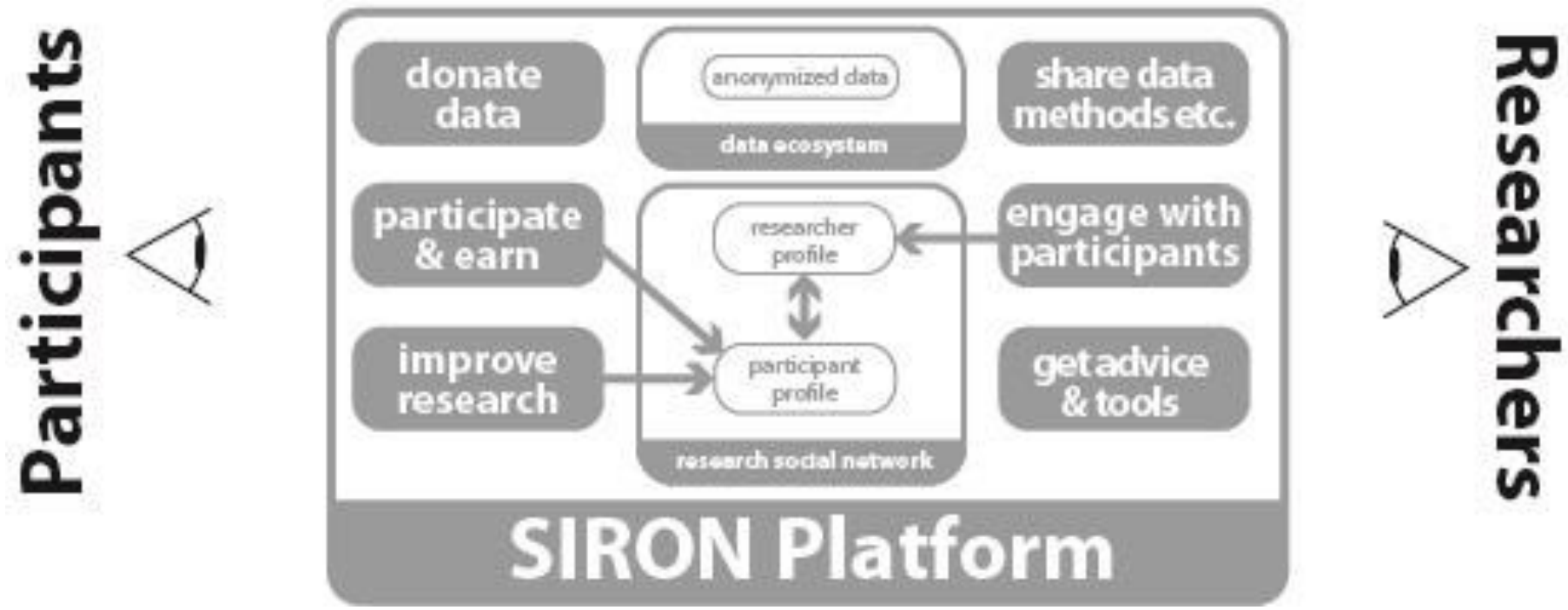
- Ensure longer-term relations between participants and researchers through an infrastructure (social network) that allows for bidirectional relations (e.g., for suggesting new research questions by participants).

- Empower the researcher both regarding legal / ethical requirements and technical instruments (e.g. for data anonymization) for doing responsible research with personal data. This may include profile anonymisation tools, including masking and synthetic data methods used in statistical disclosure control (micro-aggregation, noise addition, etc.).

- Empower the participant with the ability to verify how safe is the anonymization performed by the data collector/researcher.

The goal is to provide both the infrastructure and tools for stable relations between researchers and participants as a prerequisite for responsible research.

Outline of a research infrastructure



Part 3 – Group work & Presentation

Exercise

1) We will take two «most creepy» examples from the introduction exercise and we form two groups of 5 persons each.
2) Each group will discuss the example and creates a research project out of the example in a way such that they believe the research project is «sufficiently ethical». The group also develops a justification for the project and prepares a short presentation (30').
3) Each group also uses some time to identify potential counter-arguments against the other group (10').
4) Then, each group will present «their study» to the other group, trying to convince them (20' per group).