Ethical concepts and theories associated to privacy and data protection in the HBP

Markus Christen, Network Ethics of Monitoring and Surveillance (NEMOS), University of Zürich, Switzerland

HBP Privacy & Data Protection Workshop, Madrid, 30.09.2015

Overview

The fundamental challenge
- Social spheres and their moral foundation
- The digital undermining of spheres
- Illusions of control and informed consent
- Why is the fundamental challenge relevant for the HBP?

Ethical core concepts
- Contextual Integrity
- Autonomy as an (insufficient) “meta-value”
- Fairness and discrimination-prevention
- Responsibility and accountability

Translating ethics into practice
- Supporting Autonomy
- Safeguarding Fairness
- Enabling Responsibility

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.

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.

Is the fundamental challenge relevant for the HBP? (1)

The HBP is (partly) a “Big Data project”, aiming to increase availability and distributability of data. Thus, the more fundamental question emerges, whether the HBP would contribute to this “blurring” of spheres. Possible issues include:

- **Closed consent:** The typically obtained “closed” consent is conceptually incompatible with the explorative nature of Big Data driven research.
- **Open consent:** But also in open consent, the patient has to be informed at least to some degree on the potential use of the data. This “information framework” is often provided by disease categories (e.g.: DSM-5).
- **Information framework:** HBP research may undermine this information framework based on the conviction that many neurological and psychiatric disorders and diseases are ill-defined in terms of underlying mechanisms.

DSM also serves a societal role by providing the basis for mental health care and changes would immediately affect millions of patients and carefully balanced systems of providers and consumers.

Is the fundamental challenge relevant for the HBP? (2)

Providing broad consent for using data can transgress these boundaries in ways that generate indirect harm for the person who provides the data *even in cases when privacy is fully respected*. Some (hypothetical) examples:

- Researchers from fields unrelated to the disease of the patient may use the data to check for connections between health conditions and credit rating; resulting in a policy that impedes the patient in obtain certain bank credits.
- Researchers use the data in a way that results in a genetic test for brain diseases – and in this way offer the option of abortion. This may be against core-values of the patient when she reads about this type of research.
- Researchers may come to the conclusion that some form of a neurological disorder is associated with another disease that has a much stronger social stigma – and the patient is finally confronted with social exclusion resulting from the public dissemination of this reconceptualised disease space.

Those examples do not discredit the aim of the HBP, but they point to issues of ethical relevance.

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

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.