Tailoring responsible data management solutions to specific data-intensive technologies

Gemma Galdon Clavell and Iris Huis in 't Veld

The trend of data-driven decision-making and development of data-intensive technologies are almost inseparably linked to ethical, legal and social questions including identifiability and privacy. However, anticipating and mitigating these ethical, legal and social questions can be challenging. It requires a timely and thorough analysis of relevant implications and a complex balancing between societal values, needs and expectations and the technical and financial restrictions of technology developers. The important question for technology design and policy is: *how* can technological externalities and impact be effectively assessed and taken into account in responsibly designing and implementing technology? Drawing on tools and methodologies developed elsewhere and combining them, this paper proposes a four-part societal impact assessment framework tailored to data-intensive technologies, sensitive both to the technological and economic concerns of engineers and decision-makers and to societal values and legislation. The framework is a hands-on approach to responsible research and innovation in order to create the robust socio-technical data-intensive technology of the future.

1. Introduction

Society is becoming increasingly data-driven. Storage capacities allow us to create and use bigger data sets to put to new extraordinary uses and technology enables us to quantify and record phenomena that were not quantified before (Mayer-Schönberger & Cukier, 2013). The big data mind-set seems promising to understand and respond to situations and is therefore entering domains like healthcare, advertising, public safety and education. Data offers a broad range of opportunities, however, the existence and use of so much data poses a threat to human rights van values like the right to privacy. Recent trends in data exploitation like open data, the idea that data should be open to use without restrictions, are requiring a rethinking of how to protect human rights and values.

The use of data, especially when ‘open’ or shared, needs conditions that protect the human being the data relate to. Finding data management solutions that maximize benefits and breaching rights and values must include both policy and technology design. As the design philosophy of Privacy by Design advocates, privacy should be embedded in the design of technology as the default setting (Cavoukian, 2011). Engineering appropriate mechanisms of data protection is a robust solution since it avoids putting the burden of making responsible data management decisions on individual response agents. However, solutions cannot be solely be found in technology design, the future use of data should also be responsible regulated. Data management policy should determine the appropriate steps for the generated and processed data. For example: who should have access to the data, who is accountable and when will data be deleted?

Understanding and responding to the challenges of data-intensive technology can be challenging. Appropriate solutions must be found in an early stage and must take a broad range of concerns into account. Also, approaches to responsible data management cannot follow a “one size fits all” approach, but should rather be tailored to specific situation and threat. Take for example re-identifiability, which is not the same in different situations. The initiative of responsible research and innovation is a remarkable paradigm to push for the protection of human rights and values and along the line, several initiatives have attempted to contribute to creating robust socio-technical systems. This includes risk assessment methods, privacy impact assessments, data security trainings, a renewed data protection directive and methods to promote public engagement in technology. However, these attempts often zoom in on a specific problem and do not cover the requirements for ethical, legal and social thinking from A to Z. Also, there is a gap between the understanding of the implications of technology and the actual implementation of practical solutions. In this paper we will propose a hands-on approach for tackling ethical, legal and social issues in data-intensive technology. Useful methods developed elsewhere are combined in a framework that allows someone to start asking the right questions in order to create socially sustainable data-intensive technologies.

2. Eticas framework

The Eticas framework is an attempt to provide decision-makers with the entry points to raise the right questions and match them with tailored solutions both for policy and design. It consists of four pillars that must not be seen as distinct, but they are heuristics to cover all aspects that are important in considering the ethical, legal and social aspects in technological innovation. Even though there is a suggested order, the pillars are related and working with the pillars can be

iterative. The framework is constructed based on experience with working in many technological projects in different fields and domains. This approach to applied ethics has proven to be a robust and applicable one in several EU projects. Below the pillars will be briefly explained.

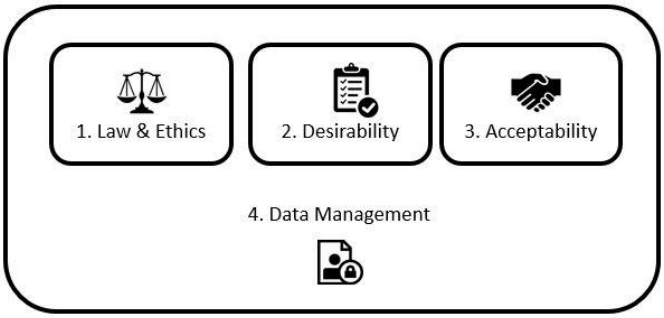

Figure 1: the four pillars of the Eticas framework

2.1 Law and Ethics

The first pillar relates to the legal and moral standards guiding a project and results in the preconditions for a project in a specific field. What are the relevant legislations and what are the social values that are involved in the specific context? This analysis involves desk research and literature review. A good place to start is considering fundamental rights. Fundamental rights are basic rights and freedoms to be respected regardless of nationality, sex, national or ethnic origin, race, religion, language, or other status. These rights are protected by documents such as the Universal Declaration of Human Rights (1948) and the Charter of Fundamental Rights of the European Union (2000). Among the rights to be protected, are: the prohibition of discrimination and equality before the law; the right to respect for private and family life, and for the protection of personal data; the right to liberty, freedom of movement and security; the right to due process of law; and the right to freedom of expression, to peaceful assembly and freedom of association. Considering that data-intensive technology is concerned with the processing of (personal) data, data protection and privacy legislation are often guiding in the legal framework. Currently, the main legal document regarding personal data protection in the EU is the Directive 1995/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, which is the common reference for the national regulations of the EU Member States. The Data Protection Directive lays down enforceable principles of good practices regarding personal data, among which are fairness, finality, data minimization, data quality, conservation, confidentiality, security and notification to the supervisory authority. However, the

Directive 1995/46/EC will be replaced by the European Data Protection Regulation (GDPR), which is expected to come into force in 2018.

While the law does cover societal values, only considering legislation is not sufficient in complying with ethical and social concerns. Technology develops in a rapid speed which creates space that are not covered by legislation but do affect societal values. To make sure that society at large benefits from technology, insights from philosophy of technology and ethical concerns specifically must be taken into account. This includes looking at how technology mediates values like democracy, equality, dignity, freedom and autonomy and to determine where the lines of legitimacy can be drawn. This is often technology and context specific.

2.2 Desirability

Desirability refers to the justification of the need for a technology or its specific functionalities. An important step in the assessment of desirability is a clear *problem definition*. The problem is usually the discrepancy that exists between an existing situation and a desired situation. Stating clearly what this difference is contributes to the coherence of any new project being considered. While problem definition sounds like an obvious step, it is often ignored or taken for granted in many new initiatives. Technology is often seen as the solution to social problems, however, not all problems yield to technology (Sarewitz & Nelson, 2008). The often unjustified belief in technology to solve social problems is referred to as technological solutionism (Morozov, 2014). In order to avoid technological solutionism, the question is whether the proposed solution is *effective* in solving the perceived problem; does it the technology embody the cause-effect relationship that connects the problem to the solution (Sarewitz et al., 2008)? Besides, the effects of the technology have to be taken into account in a c*ost-benefit analysis*. A cost-benefit analysis can be financial but also includes social costs. Following this, choices have to be made that maximize benefits and minimize social and financial risks. Finally, desirability also includes the measurability of the effects of a technology. In this regard it is Important that the effects of the technological fix can be assessed using unambiguous criteria (Sarewitz et al., 2008). The pillar of desirability is thus focussed on a critical assessment of whether the technology and its impact are effective, able to assess unambiguously and balances costs and benefits. The outcome can be an alternative solution, either technological or even in a domain of social or policy changes. A desirability analysis can also result in adjustments in the proposed solution.

2.3 Acceptability

The pillar of acceptability plays a significant role in responsible research and innovation as it involves the inclusion of public opinions and values in a technological innovation or research project. Gaining insights in how stakeholders perceive technology can be done from a theoretical perspective, drawing on insights from for example domestication theory (Silverstone & Haddon, 1996), technology acceptance (Davis, Bagozzi & Warshaw, 1989) or diffusion of innovations (Rogers, 2003). Public perception of technology can also be understood by discourse analysis: for example by looking at (social) media outlets to understand if there is a public debate and what the dominant arguments are. Acceptability is also about mapping stakeholder desires, expectations and concerns by directly engaging them. Social research methods, both quantitative and qualitative, can be used to form an understanding of stakeholders' opinions. When acceptability is researched, the outcomes can be implemented in the design process, creating a situation of co-design which contributes to the democratic ideals of science and technology.

2.4 Data management

While data management refers to the legal framework of privacy and data protection and ethical principles, it also encompasses broader considerations relating to individual control and consent, methods of anonymization, and how privacy issues can be designed into technologies and projects. The way in which data is collected, managed, processed and stored in research and innovation processes is often a 'black box', meaning that users have little information about these procedures nor about their rights in such processes. Unfortunately, non-compliance and lack of protection is the norm rather than the exception when it comes to privacy and data protection. Only when transparent policies and technological solutions are put in place, the black box of data management can be opened up. This pillar aims to identify the vulnerable moments in data management and matches those with appropriate directions where solutions can be found and tailored to the specific situation. This framework provides a life-cycle that support the mapping of the different stages of data processing, the vulnerable points where rights and values are at stake and the principles and precautions to be applied in order to protect those rights and values. The data management life-cycle points to five main points of vulnerability that are visualised in figure 2:

1. *Data collection*: the data is gathered under the condition that it will only be used for a legitimate purpose; that only the data needed for that purpose will be collected (data minimization); that the people to which the data concerns gave consent to it; that the data

is of good quality; that there are mechanisms in place for the people to opt-in and opt-out; and finally that the data is properly anonymized when possible.

2. *Data storage*: when stored, data should be kept under certain conditions, such as it should be secure; who has access to the data has to be carefully considered; it should be established who is accountable for the data; and the process should be frequently audited.
3. *Data analysis*: there are also principles for when the data is being analysed. Data should be anonymised when possible; the necessity of certain analysis techniques (e.g. profiling and sorting) should be considered, as well as the potential harm of the data produced by the analysis and possible misidentification of an individual by an automated algorithm. Finally, accountability and auditing mechanisms should be put in place to make sure that all analyses performed are consistent with the system's purpose.
4. *Data sharing*: there are different possibilities of data sharing, within the data controller, with data processors, with third parties and as open data. Whenever data is shared, the data life-cycle starts again, as it will be stored, analysed, shared and eventually deleted. Each type of data sharing requires specific precautions to be taken, including anonymization and the adoption of security, accountability and auditing mechanisms. It is also worth noting that data may be shared under emergency protocols. This can imply the suspension of certain rights and freedoms, depending on the specific threats. Nevertheless, this should not result in a 'legal vacuum' or non-compliance. Respect to non-derogable fundamental rights must be ensured, and the basic mechanisms of data management should be still in place.
5. *Data deletion*: when data is no longer needed for the purpose of which it was lawfully collected, it should be deleted (ideally, the deletion date should be defined at the moment of collection). Mechanisms must be put in place for requesting data deletion. Additionally, secure deletion mechanisms should ensure that deleted data cannot be retrieved and that there are not copies available (e.g. temporary storage and back-ups).

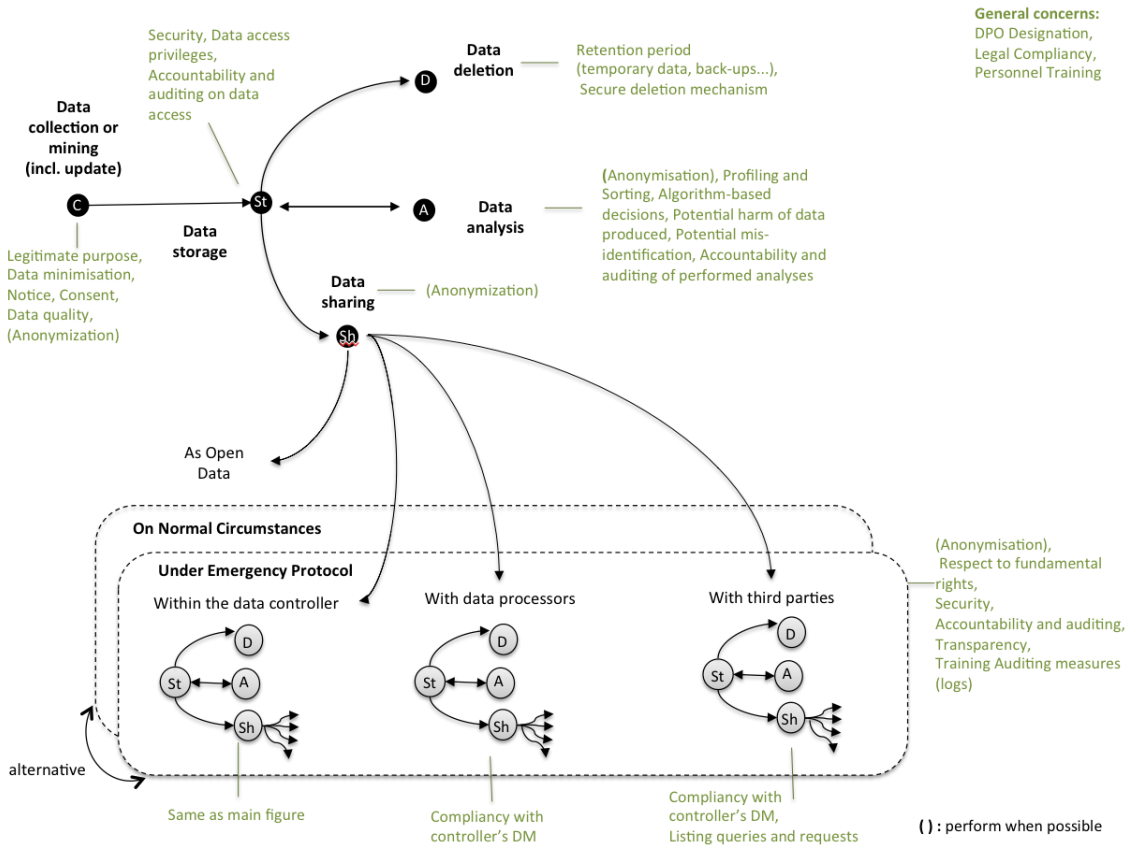

Figure 2: data management life-cycle

3. Conclusion

This paper proposed a framework for mapping the ethical, legal and social implications of data-intensive systems in order to respond to the challenges of evolving data-intensive technologies. Data-driven solutions have the potential to enhance many processes and provide new opportunities. However, when dealing with data, it should not be forgotten that the data relates to human beings with rights and values. Aspects of legality, ethics, desirability, acceptability and data management policy have to be critically considered in order to make sure that rights and values are respected. Responsible technology design and policy is not only about doing the right thing, it also makes sense from a business perspective because a product or services might be declines when it does not comply with social standards. Understanding and responding to challenges of data can be challenging, especially for technically trained people that might easily be lost in the field of ethics where they often do not feel comfortable. In this paper we proposed a framework that provides policy-makers and engineers with the tools to think about ethics and technology and to lead them towards value-sensitive and privacy-enhancing solutions like anonymization. The framework combines an analysis of the societal impact with the practical

technical and financial concerns of technology developer, using four perspectives: Law and Ethics, Desirability, Acceptability and Data Management. We have found this framework to be malleable; that is, it can be adapted to different systems and contexts, as well as to the resources of the organizations performing the assessment. Even though an order of assessment is suggested, the analyst can choose any entry point that he or she feels comfortable with and considers relevant. The assessment of one pillar will inevitably raise issues regarding other pillars, easing the navigation to other types of concerns. The framework also provides practical recommendations to tackle many of the issues identified, and contributes to finding privacy-enhancing solutions. The framework, however, is not a sure recipe for avoiding negative externalities. Its success depends on a genuine commitment from all stakeholders. This is particularly the case with technology designers, which should adopt a mind-shift from technology inventors to solution providers; that is, people that develop technologies that are proportionate to real problems, while considering the values, needs and expectations of the communities beyond their user base. In terms of future work, even though this framework has already been used in a variety of projects, we see it as an ever-evolving tool to accommodate technological advances and social changes. As such, we are continuously exploring existing tools and techniques and creating new ones to be used within the framework. In particular, we continue to work on improving ways to find out and assess public concerns and behaviours when confronted with the choice between short-term benefits and potential negative externalities in the (long-term) future, as well as their attitudes towards individual versus societal gains. With this framework, that incorporates a broad range of ethical, legal and social angles and builds on useful existing research methodologies, we hope to contribute to the future assessment of ethical, legal and social implications and the tailoring of value-enhancing responses to future developments in data-intensive technology.

References

Assembly, U. G. (1948). Universal declaration of human rights. *UN General Assembly*.

Cavoukian, A. (2011). Privacy by Design: Origins, Meaning, and Prospects.*Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards*, *170*.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, *35*(8), 982-1003.

European Convention (2000) Charter of Fundamental Rights of the European Union, OJ C364/01. Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Morozov, E. (2014). *To save everything, click here: The folly of technological solutionism*. PublicAffairs.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

Sarewitz, D., & Nelson, R. (2008). Three rules for technological fixes. *Nature*, *456*(7224), 871-872.

Silverstone, R., & Haddon, L. (1996). Design and the domestication of ICTs: technical change and everyday life. *Communicating by design: The politics of information and communication technologies*, 44-74.