Purpose Limitation

Merel Elize Koning

Privacy & Identity Lab
Digital Security
Institute for Computing and Information Sciences
Radboud University Nijmegen

1 Introduction

The global networked society is rapidly turning into a data-driven society in which personal data is collected, re-used and repurposed by automated means at a fast pace. This development enables data-driven surveillance that is based on big data and personal data profiling, and imposes challenges to democracy, the Rule of Law and the safeguarding of human rights and civil liberties, most prominently to the right to privacy and the protection of personal data. One of the core principles of European data protection regulation is the purpose limitation principle that demands that data is processed for priorly specified, specific and legitimate purposes and is not subsequently processed for any incompatible purposes that the ones that were specified.

As a PI.Lab PhD-candidate I focus on the purpose limitation principle and the broader privacy issues that surround this principle. The past four years I have conducted legal research on European data protection regulation, transnational data transfers, the effects of the entry into binding force of the Charter of Fundamental Rights of the European Union on Dutch data protection law, and privacy-enhancing technologies (PETs). This contribution is set out to give an overview of a selection of the results.

2 Legal theoretical framework on purpose limitation

My PhD-thesis is focussed on the topic of transnational private to public data transfers for surveillance purposes in the field of criminal law enforcement. I specifically investigate the jurisdictional aspects of transnational data transfers in the field of law enforcement, the effects of the purpose limitation principle on data processing for surveillance purposes and duties of good governance and State responsibility in public-private partnerships. These three research topics appear unrelated, but are, however, closely related through their connection with the Rule of Law.

2.1 Rule of Law in a data-driven society

For my research on the purpose limitation principle I traced the concept back to it's origin. Purpose limitation in data protection supports the idea of transparency and binding of the more powerful to predetermined conditions. The principle facilitates the division of power by division of data processing processes. This idea is closely tied to the Rule of Law. Like many important moral, political and legal ideals the meaning and significance of the Rule of Law is highly, perhaps essentially, contested. The European continental law tradition tends to build the Rule of Law on three values: equality, liberty and human dignity. These values are also common to international human rights treaties and provide a base for agreements such as the Universal Declaration of Human Rights. Together with the concepts of democracy and human rights, the Rule of Law forms the base for modern societies.

Some theorists explain the Rule of Law in a very narrow manner, and argue that governments should be able to point to some basis for their actions that is regarded valid by the relevant legal system. Others link the Rule of Law to a moral underlying and argue that, depending on the compliance with the values equality, dignity and liberty, legal norms can be called *good* or *bad* law or not law at all. The difference between these two conceptions is regarded static and exhausting by many legal theorist. I agree with professor Hildebrandt of the

PI.Lab and believe that the 'debate on the meaning of the Rule of Law has been mystified' by legal philosophers by framing its interpretation as either formal or substantive [Hildebrandt, 2015, p. 55]. In a data-driven society, with its declining ties with territoriality and increasing public-private partnerships, the focus on the establishment of the Rule of Law should be on procedure, practice and communication of law, rather than on it's end result. An effective remedy for those who are subjected to certain measures should be part of the Rule of Law. This conception migrates the responsibilities to provide an effective remedy from the human rights realm to the Rule of Law context, resulting in a structure of checks and balances for government action towards those who cannot call upon the protection of constitutional rights. This conception restores the power imbalances in a data-driven society with increased government and commercial surveillance on non-citizens.

2.2 Relationship between data protection and privacy

The Rule of Law ties in with human rights in a democratic society. My research topic – surveillance – restricts the right to protection of private life (privacy) and the right to protection of personal data in particular. Within the context of PI.Lab I found myself trying to explain to computer scientists the differences between and similarities of data protection and privacy multiple times. Privacy rights are often described as individualistic and enforced negative: preventing others from interfering with one's private life: the right to be opaque. Data protection on the other hand empowers the data subject to take steps: the right to demand transparency. However, alike most relevant things in life, these concepts are not zero or one neither black or white. The concepts intertwine, communicate and overlap in a grey zone. The interrelationship between the two remains topic of today's legal academic work. The past years I observed the following noteworthy aspects of the relationship between data protection and privacy. Firstly, the objectives of the data protection doctrine include the safeguarding of privacy and the right to protection of personal data. Secondly, the scope of the latter right is

widely regarded as the result of decades of case law on the right to private life and communication in automated data processing cases. Thirdly, The European Court on Human Rights has never acknowledged a general right to protection of personal data. It has, however, recognised aspects of the data protection doctrine under the scope of art. 8 ECHR on a case by case base over the years. Fourthly, the right to protection of personal data is explicitly codified in the Charter of Fundamental Rights of the European Union. The highest court of the European Union (EU), the Court of Justice of the European Union, interprets the Charter of Fundamental Rights of the European Union and therefore deals with data protection and privacy on a fundamental rights level. This court prefers a joint reading of art. 7 and 8 of the Charter: 'the right to respect for private life with regard to the processing of personal data'. Lastly, when referring to the objectives of a certain piece of data protection regulation, policy makers have frequently articulated the respect for rights and fundamental freedoms, and in particular the right to privacy.

2.3 Purpose Limitation

The EU data protection framework regulates personal data processing. The scope of the term data processing includes any operation that is performed upon personal data, whether or not by automatic means. The term personal data refers to any information relating to a directly or indirectly identified or identifiable natural person. From a EU perspective data-driven surveillance often relies on partnerships between criminal law enforcement agencies of member states and private commercial entities that are – at least partly – based in the United States (US) and that initially processed the data for a different purpose. The data flows of these public-private partnerships are subject to a patchwork of regulations on both sides of the Atlantic, most of which are currently being revised.

The data protection framework and revision that is currently negotiated in Europe is based on the same principles as the first data protection policy in Europe and the United States from the late 1960s and early 1970s. In academic

literature this set is referred to as the 'fair information principles'. It consists of the accountability principle, the purpose specification principle, transparency of data collection and processing principle, the use limitation or finality principle, the storage limitation principle, the accuracy of data principle, the security principle, and the access and correction rights for the data subject. Because of the international dimension of the data protection realm these principles are embedded in the domestic legislation of most Western countries.

The purpose limitation principle is a core trait of this legislation and is included in the negotiation mandate of most data protection treaties, including treaties in the field of criminal law enforcement. The principle plays an important role in the protection of human rights and the safeguarding of the free flow of personal data. It has two components: 1) the requirement that personal data processing must be for a specified, explicit and legitimate purpose; and 2) the requirement that any further processing must be compatible with the original purpose for which the personal data were collected. The principle demands prior transparency of intentions (purpose specification) and binding to pre-determined conditions (use limitation). These demands therefore show connection with aspects of the Rule of Law.

The purpose limitation principle fulfils an autonomous and a conditional function. The autonomous function sets a precondition and demands personal data to be collected for specified, explicit and legitimate purposes and not to be further processed in a way incompatible with those purposes. The principle is also connected to other data protection principles and has a conditional function for the data quality principle, data minimisation principle and accountability. As a result of the dual function and interconnection, erosion of the conception of the purpose limitation principle results in the erosion of all related data protection principles.

2.4 Departures from the purpose limitation principle

While researching the principle in EU law, I observed that the data protection framework does not allow for departures from the purpose specification component. This is due to the connection of the this component with the requirements of foreseeability under article 8(2) of the European Convention on Human Rights (ECHR). Derogations from the use limitation component, on the other hand, are somewhat common and regulated very precisely by the EU legislator. Four types of departure can be distinguished. First of all, data can be re-used for statistical, scientific and historic purposes. Secondly, incompatible re-use of data is allowed when it is considered a legitimate derogation that meets the criteria of article 8(2) ECHR. It therefore needs to be in a accordance with the law, necessary in a democratic society and in pursuance of a legitimate aim. In some sectors the European legislator limited the legitimate aims that can be pursued with the re-use of certain data. For example the re-use of metadata from the telecommunication sector is only allowed for purposes of national security, defence, public security, and the fighting of crime or of unauthorised use of electronic communication systems. The third derogation is re-use for incompatible purposes with the consent of the data subject. Consent should be explicit, specific and freely given. Eleni Kosta of the PI.Lab conducted extended research on the notion of consent in EU data protection regulation in the past [Kosta, 2013]. In some sectors - like the field of law enforcement – this derogation is limited and can only be use if the re-use benefits the data subject in order to avoid forced consent due to power imbalances. Last but not least is derogation via the consent of the data processor. This derogation is uncommon and primarily used in the context of international data transfers in the field of law enforcement. A number of instruments allow for the transmitting State to consent for re-use of the data by the receiving State for 'any other purpose'. This departure is least in-line with the spirit of the purpose limitation principle and leans towards general purpose processing. Currently the data protection Regulation is negotiated in the EU. It

is unclear if this will lead to the introduction of a fifth departure in the positive legal framework.

3 Purpose limitation in applied cryptographic solutions

3.1 Attribute-based credentials

Technology mediates today's data-driven society in which the demands for secure and privacy-friendly digital identity management is growing. Scientists, industry and policy makers have – at least in the past – approached the privacy and security aspects of identity management as being a trade-off between the two. Cryptographic solutions, like attribute-based credentials (ABC), however, allow for the design of more secure and yet privacy-friendly identity management systems. Governments are allocating funds to implement identity management systems and ABC make an interesting candidate. Members of the PI.Lab conduct innovative research in this field with the IRMA project. See pages XX of this book. With the PI.Lab team we took up the knowledge gap that existed on the wider implications of ABC. We observed that – good intentions of the designers aside – ABC implementations nevertheless introduce a range of societal issues with regard to privacy and identity [Koning et al., 2014]. My research focussed on the legal aspects of these issues and is discussed below.

3.2 Data protection by design and by default and the purpose limitation principle

So far, the data protection framework does not regulate the design phase of the systems that can process personal data. The new General Data Protection Regulation (dGDPR) might change this with the introduction of *data protection by design and by default*: a general obligation on the data controller to implement appropriate technical and organisational measures within the entire life cycle of the technology to ensure data processing to meet the data protection standards.

Data protection by design should be taken into account at the moment of determining the purposes and the means of the data processing as well as at

the time of the actual data processing itself. During the entire life cycle of the data there should be a consistent focus on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. The mechanisms should be state of the art and up to date with current technical knowledge and international best practices. They should mitigate the risks represented by the data processing. All data processing should be fair, lawful and transparent.

These requirements are partly embodied in the purpose limitation principle that is discussed in section XX of this contribution. Purpose limitation must be explained in terms of a substantive conception of legality. It does not only refer to the limitative enumeration of legal grounds on which data can be processed, but also to the data controller's duty to determine the purposes and to process personal data in accordance with the law, state-of-the-art techniques and cultural and societal norms. This criterion requires besides a legal assessment, a technology assessment, and hence has a potential propelling effect on the actual implementation of technological innovations.

In section XX I referred to the conditional function of the purpose limitation principle. The obligation to implemented data protection by default accelerates this function in relation to data data minimisation and storage minimisation. Data protection by design obliges the data controller to ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data. Personal data can only be processed if, and as long as, the purposes cannot be fulfilled by lesser means, such as processing information that does not (directly) involve personal data: pseudonymous data or anonymous data. Data protection by design also sees on the storage minim-

isation principle because personal data must be kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The ABC technology hardcodes the data minimisation principle. Once the scheme manager determined what is proportionate and necessary (within the limits of the Regulation) and approves the presentation policies, the data processed for one purpose is minimised to the authorised attribute types coded in the presentation policy.

However, function creep is a potentially serious issue for ABC because the credentials are authentic data and presented in a standard format. Re-use for incompatible purposes could be tempting on the side of the relying party. We also found that ABC are generally perceived as a privacy-enhancing technology. Because the system provides strong authentication and a 'good image' societal over-use could be a potential threat to the data processing minimisation principle. Besides this, the selective disclosure protocol of ABC empowers the data subject to control the first release of the personal data, however, after that first release the user is just as dependent on the service provider with regard to further use of the data as the subject is in current data processing. Further distribution of the data is not technically regulated by ABC systems. Additional policies must regulate further distribution.

3.3 ABC and pseudonymous data

The dGDPR proposes a special 'light' regime on the processing of pseudonymous data. Pseudonymous data should be distinguished from anonymous data, which is information that does not relate to an identified or identifiable natural person. The principles of data protection do not apply to anonymous data. The dGDPR defines pseudonymous data as personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution. This light regime particularly affects the legal regime on profiling: forms of automated processing of personal data

intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. Profiling based solely on the processing of pseudonymous data is not presumed to be significantly affecting the interests, rights or freedoms of the data subject. However, when profiling –whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources– permits the controller to attribute pseudonymous data to a specific data subject, the processed data is no longer considered to be pseudonymous. The use of ABC could have propelling effect on profiling. ABC can have a stimulating effect in terms of the quality of data that is revealed and the quantity of the data processing. Pseudonymous data is often used for big data and predictive analytics for profiling and targeting purposes. Profiling on the basis of this type of data is not presumed to be significantly affecting the interests, rights or freedoms of the data subject. However, one could question whether profiling with pseudonymous, but verified authentic attributes, will –in the long run– not affect the interests, rights or freedoms of the data subject. With an ABC system the data becomes more valuable and the technology does not regulate the combination or further use of attributes; neither do the policies. The proportionality assessment for the other purposes or further use for which the data might be collected via the ABC card, does not lay in the hands of the scheme manager. This entity only assesses the proportionality with regard to the authentication problem.

3.4 Concluding: Purpose limitation and ABC

Attribute-based credentials limit the information leakage, but this technology does not limit data processing. Due to its privacy-friendly image and verified high quality of data, prompt broad deployment of ABC seems tempting. Because of the authenticity of the data and the data protection 'light' regime on pseudonymous data, there is a high probability that information from the ABC will be further used for profiling purposes. The initial privacy-friendly intent influ-

enced the technical design, but the technical design now influences the 'further' processing purposes.

Concluding, ABC could on the one hand invite for incompatible re-use, while on the other, be considered a PET that – at least to a certain extent – implements technical means for compliance with the purpose limitation principle of the data protection regulatory framework. The interdisciplinary research lead to the conclusion that ABC can be considered *'data protection by design'* but it should not be considered *'data protection by default... by default'* because many aspects are either not covered by the technology or depend on the grace of the scheme manager.

4 Conclusion

The interdisciplinary environment of PI.Lab is a challenging and thought provoking one. It lets legal scholars, like myself, take a look under the hood of the 'technology vehicle'. These opportunities shed different light on legal concepts. The interaction with scholars from different disciplines appears to be fruitful for computer scientists as well. Questions such as: 'What problem are you trying to solve?' and 'Is that really a problem worthy of our time?' help to sharpen interdisciplinary research, like the ABC research of PI.Lab, as well as disciplinary-specific research, like the assessment I made on the relationship between privacy and data protection in the positive legal framework. Labs like the PI.Lab are crucial to good research in the 21st century.

References

Hildebrandt, 2015. Hildebrandt, M. (2015). Radbruch's rechtsstaat and schmitt's legal order: Legalism, legality, and the institution of law. *Critical Analysis of Law*, 2(1).

Koning et al., 2014. Koning, M., Korenhof, P., Alpár, G., and Hoepman, J.-H. (2014). The abcs of abcs: an analysis if attribute-based credentials in the light of data protection, privacy and identity. *Online proceeding HotPets*.

Kosta, 2013. Kosta, E. (2013). *Consent in European Data Protection Law*. Brill, Leiden.