GIMA MSc Thesis

Geographic data as personal data in four EU Member States.

Date: 14 – 08 - 2015

Supervisors: Dr. Ir. Bastiaan van Loenen and Prof. Dr. Jaap Zevenbergen

Student: A.J. de Jong

A.J.deJong2@students.uu.nl

Preface

Popular terms as Open Data and Big Data, privacy and personal data protection are frequently mentioned in the news. Geographic data is more and more opened up and differences in privacy legislation can be a barrier. This topic got my interest and I have researched it.

It was a very interesting topic, because it showed the different personal data interpretations of the EU Member States.

I want to thank Tineke Mateboer for checking my thesis and giving me advice. I also want to thank Thomas van Wageningen for checking the English spelling and grammar, and I want to thank Sebastiaan van Dam for the feedback on the English spelling and grammar. I want to thank Prof. Zevenbergen for the advice, Skype conversations and the feedback.
In particular I want to thank Bastiaan van Loenen for all the talks, feedback and advice. He was always willing to respond quickly and give some more advice on my research.

Summary

Directive 95/46/EC is the Directive to protect personal data in the European Union, this Directive is implemented in national legislation. The interpretation of this Directive is different in the various Member States, this hinders the internal market of the European Union.

The research shows the differences in EU Member States when it comes to considering geographic data as personal data. The used definition is the definition in Directive 95/46/EC on the processing of personal data. Governments play an important role in the opening of geographic data. Governmental bodies produce a lot of geographic data and with two Directives on the reuse of governmental data, the EU supports the opening up of data by supporting reuse policies. It is an obligation for governments to open up the data necessary for their public task, so the data can be reused.

The differences between Member States stem from the differences in interpretations on when geographic data leads to identifiability of a natural person. The research is based on four different EU Member States, The Netherlands, Belgium, Germany and the United Kingdom. Four key stakeholders (Data source holder, Legislator, Data Protection Authority and, Jurisprudence) are identified and their opinions or judgements on the interpretations of the extent to which geodata should be considered personal data are analysed. The focus of the thesis is on two types of geographic data: Mobile mapping, geographic data collected from a movable object is considered and secondly the INSPIRE themes of topographic maps and building registers are assessed.

The research found a variety of interpretations of data protection legislation to geographic data. The variety was found among the different cases (EU and Member States), the different stakeholders and the different types of geographic data. The EU, the Netherlands, Belgium, Germany and the United Kingdom are case-studies in this research.

An example of the differences is that in the Netherlands the Data Protection Authority states that panoramic images of streets are considered personal data. In the discussions on the processing of 360 degrees images of houses within the Parliament the legislation does not mention the use of Google Street View and jurisprudence judges that dissemination of these images is possible when certain features are blurred and there is no link to an address. This shows that there are differences between the actors inside the Member States on to which extent geographic data is considered personal data.

Another example is the studied topographic datasets. The datasets do not contain personal data, according to the Dutch Data Protection Authority, while the German Data Protection Authority and the Belgian Data Protection Authority judge that topographic maps of a large scale can contain personal data, and have requirements for the processing of topographic maps.

The patchwork of differences in data protection legislation can be harmonised by using a traffic light model. This model uses another definition of personal data. It has a focus on the context of processing of the data and categorizes the data from non-identified data to identified sensitive data, in this way access to the data is categorized. This categorization is based on an assessment of the processing of the data. This leads to a more harmonised interpretation of personal data definition.

Index

1 Introduction 1
1.1 Research Objectives 2
1.2 Research Questions 2
2 Research Methods 5
2.1 Used Methods 5
3 Theoretical background 7
3.1 Privacy 7
3.1.1 European privacy legislation. 8
3.1.2 Directive 95/46/EC 9
3.1.3 Discussion on the Directive 10
3.1.4 Reform of the data protection rules 12
3.2 Open data 15
3.2.1 Open government 15
3.2.2 Open Data 15
3.2.3 Directive 2003/98/EC 16
3.2.4 Directive 2013/37/EU 16
3.2.5 Barriers for use of open data 17
3.3 Geographic data 19
3.4 Introduction of the case studies 23
4 Europe 25
4.1 Personal data definitions and explanation. 25
4.1.1 Article 29 Working Party 25
4.1.2 EDPS 26
4.1.3 ECJ and ECHR 26
5 The Netherlands 29
5.1 Legal context 29
5.2 Mobile mapping 31
5.2.1 Legislator 31
5.2.2 Data Protection Authority 31
5.2.3 Jurisprudence 32
5.3 INSPIRE 35
5.3.1 Legislator 35
5.3.2 Data protection authority 35
5.3.3 Jurisprudence 36
6 Case Belgium 39

6.1 Legal context 39
6.2 Mobile mapping 40
6.2.1 Legislator 40
6.2.2 Data Protection Authority 40
6.2.3 Jurisprudence 41
6.3 INSPIRE 43
6.3.1 Legislator 43
6.3.2 Data protection authority 43
6.3.3 Jurisprudence 44
7 Germany 45
7.1 Legal context 45
7.2 Mobile mapping 46
7.2.1 Legislator 46
7.2.2 Data Protection Authority 46
7.2.3 Jurisprudence 46
7.3 INSPIRE 49
7.3.1 Legislation 49
7.3.2 Data Protection Authority 50
7.3.3 Jurisprudence 51
8 United Kingdom 53
8.1 Legal context 53
8.2 Mobile mapping 54
8.2.1 Legislator 54
8.2.2 Data Protection Authority 54
8.2.3 Jurisprudence 54
8.3 INSPIRE 56
8.3.1 Legislator 56
8.3.2 Data Protection Authority 56
8.3.3 Jurisprudence 56
9 Analysis 57
9.1 Harmonising the patchwork of data protection 65
10 Conclusion 67
11 Discussion 69
12 References 71
13 Annex A 79

1 *Introduction*

The main goal of this thesis is to understand to which extent geographic data should be considered personal data and to determine whether geographic data is considered personal data.

Open (geographic) data creates opportunities for companies operating in the European internal market. 70% of the open data collected by the government has a geographic component (Ministry of economic affairs, 2013). The economic benefits for (re)using open data are estimated between 27 and 140 billion euros for the European market (Ministry of economic affairs, 2013).

In 1957, the Treaty of Rome was signed, and the European Economic Community (EEC) was established, one of the goals of the Treaty was the creation of a common market. In 1992 the Treaty of Maastricht was signed and in 1993 the creation of a single market was realized. In this internal market companies are able to produce and sell products without barriers (European Commission, 2014). But, even on this day barriers for companies operating in the single market exist. The EU Directives are implemented by EU Member States in various ways, this difference combined with technological development can lead to barriers for companies operating in the single market. For example when a company operates in the single market and wants to sell a geographic data product, there are a couple of barriers. One barrier is the differences in the implementation of personal data protection legislation. When geographic data is considered personal data, there are strict conditions for storing, using and processing the geographic data. At first it may appear no geographic dataset can be considered personal data, but this is not necessarily true. Research shows that EU Member States implement the Personal Data Protection Directive in different ways (Korff, 2002 and 2010). To what extent geographic data is considered personal data differs between the different Member States. Also reusers of the data have problems with varying licensing, pricing and transparency values in Member States to create value added products on the European internal market (European Commission, 2011a).

An example of a difference is the way Google's Street View service is approached by the Dutch and Belgian Data Protection Authorities. The Dutch Data Protection Authority did not see a problem with Google Street View operating in Dutch streets (Trouw, 2008), while in Belgium the Google service was registered at the Belgian Data Protection Authority (De Standaard, 2009).

The differences in implementation of personal data protection legislation between EU Member States raises questions about to which extent geographic data is personal data and why the different datasets are considered personal data. In this research implementation of the EU Directive on personal data protection in respect to geographic data in four Member States is researched. This research gives recommendations for further harmonised personal data protection regulations in the European Union to support a common European market for geographic data.

1.1 *Research Objectives*

The goal of the research is:

To propose a harmonisation of implemented EU personal data protection legislation.

The harmonisation consists of taking away the barriers for an internal geographic data market in the EU. Personal data protection legislation acts as a barrier to the functioning of the internal market. With clearer legislation it becomes easier for companies to operate in the internal market.

The main goal has different objectives.

1. Understand the definitions of personal data and open data.
2. Understand the different implementations of the EU Directive 95/46/EC in different Member States.
3. Analyse to what extent geographic data is considered personal data in the EU Member States.
4. Propose solutions to harmonize the differences between EU Member States.

1.2 *Research Questions*

This leads to the following research question:

To what extent should geographic data in the EU be considered personal data, and how may the different interpretations of EU Member States be harmonised?

To answer the main research questions the following sub-questions are answered:

1. *What are personal data, open data and geographic data?*
2. *To what extent do the interpretations of the personal data definition of EU Directive 95/46/EC differ between the Article 29 Working Party, the European Court of Justice, European Court of Human Rights, and the Draft General Data Protection Regulation?*
3. *To what extent does the implementation of the Personal Data Protection Directives differ between and within EU Member States (perspective of data holder, legislator, data protection authority and jurisprudence)?*
4. *Where are mobile mapping data, and topographical maps considered personal data and why?*

The definitions of open data, geographic data and personal data can be found in the literature. In the beginning of the research these terms are briefly summarized.

The second sub-question gives an overview of four definitions of personal data. First, the EU Directive 95/46/EC, second the definition of the Article 29 Working Party, third the judgements of the European courts and finally the new draft EU regulation.

The third sub-question reviews the different implementations of the Data Protection Directives between EU Member States. The Data Protection Directive is a clear Directive, but the implementation differs between EU Member States. This has to do with the different definitions of privacy and personal data protection.

The fourth sub-question results in an overview of which datasets are considered personal data, and what factors are considered to open a dataset or keep it closed as personal data.

This research consists of two parts, first the thesis looks at the theoretical background, and starts with privacy. Second chapter is open data, and the third chapter is about geo-data. The second part consists of empirical research in which the case-studies are discussed. Also it

contains an analysis of the results and recommendations about how to harmonise the different interpretations between and inside the EU Member States.

The readers interested in European privacy legislation and personal data protection are referred to chapter 3.1 page 7. The case studies are described in chapter 7-11, the situation in the European Union on page 25, the Netherlands on page 29, Belgium on page 39, Germany on page 45, the United Kingdom on page 53. The analysis and conclusion are written on page 57 and page 67, and the references start at page 71 the last part is an Annex with the interview on page 79.

2 *Research Methods*

The methods are about the approach of the research. The goal of the research is to learn to what extent geographic data should be considered personal data based on the experience in four EU Member States. In this chapter the used methods are discussed, a roadmap of the research is given and the matrix for the empirical research is explained.

2.1 *Used Methods*

The research consists of different components: a theoretical background and an empirical part. The theoretical background (Chapter 3) consists of privacy and personal data protection theories, open data is discussed and the relevant geographic data and research matrix set-up are introduced. For the empirical part case-studies are analysed and an interview is used as a validation for the found differences in the perspectives.

In the academic literature there are different views on the use of case-studies. Case-studies are useful, when the topic is relatively new and the literature is not extensive enough to cover the research questions (Eisenhardt, 1989). When the research questions try to answer an explorative question, for example how, or what questions, the use of case studies is also recommended. When data is collected from cross-cultural and cross-border settings, case-study research is also very well suited (Ghauri in: Marschan-Piekkari and Welch, 2004). With the use of multiple cases a description of real world decision making can be modelled (Miles and Huberman, pp.185-186, 1994).

There is a distinction between two research methods, qualitative and quantitative. The nature of this research is qualitative. It leads to the creation of a new model to support decision making processes in assessing to which extent geographic data should be considered personal data. This approach makes the research of an inductive nature (Bryman, 2012, p.36).

To come to conclusions on how to harmonise different interpretations of EU personal data protection legislation between Member States the following four steps are taken.

1. The first step is conducting a literature review. It consists of three parts. First, privacy protection and personal data protection in the European Union is discussed. Second, the open data movement and third, different types of (open) geo-data are examined. In order to answer the main research question, empirical research on the way geographic data is defined in EU Member States is needed.

2. The second step is to draft an analysis framework to analyse the case studies. Criteria on how personal data is defined, how open data is defined and how the right to privacy is defined are derived from the literature and used to design a matrix. The matrix will serve as an assessment tool for the case-study research. The matrix consists of three columns. Starting with the perspective in the Member State. The first column is chosen, because it refers to the different perspectives in the Member States on the definition of personal data. The roles consist of data source holders, legislator, Data Protection Authority and jurisprudence. The second column consists of the question if the datasets are considered personal data, because it can answer the research question in which EU Member States geographic data are considered personal data. The third column gives the argumentation of the choices for or against personal data, this element is included in the matrix because it gives insight in the arguments and it shows the different reasoning inside a Member State and between Member States (Table 1).

3. The third step is the selection of the case-studies. An important factor in selection of case-studies is to take a critical look to the applicability of the case-studies. This

makes the relation between geographic data and personal data in EU Member States the unit of analysis, and thus a case-study approach applies (Bryman, 2012, p.68). Another aspect is the researched datasets. The research focuses on differences with regard to geographic data. The cases consist of mobile mapping data and some INSPIRE thematic datasets. Mobile mapping data is defined as data collected from a movable object. For example cars that take 360 degrees panorama pictures as used in the Google Street View service and aerial photographs. From the INSPIRE themes the topographic maps and also addresses and buildings are researched.

Country *Geographic dataset*	Personal data	Argumentation
Data source	Yes/No	Because
Legislator		
Data protection authority		
Jurisprudence		

Table 1: Example of a matrix.

3 *Theoretical background*

To understand the different concepts and theories, the theoretical background is discussed first. The different definitions of privacy and personal data are addressed and legislation to regulate processing of personal data in the EU is discussed. The following subchapter is about open data. Developments in the open data movement and different EU Directives are covered. Also the use and users of open data, and barriers for use of open data are mentioned. The last part is about geographic data, and the relevance of open geographic data.

3.1 *Privacy*

This part of the theoretical background, discusses privacy. First the history of the definition of privacy is reviewed. The second part is the European privacy legislation and the different EU Directives. Third the reform of the EU Directives is mentioned.

Privacy and the right to privacy have had different definitions throughout time and in different cultures. The first time notion of privacy as legal concept comes from the United States. Warren and Brandeis (1890), define privacy as the 'right to be let alone'. With the rise in use of data on computer networks, there was an increased interest in privacy in the 1960s (Gellman, 1996). With the technological advancement and availability of personal data, there has been a bigger focus on protection of personal data. The present day views on privacy are based on a liberal focus: people can make their own informed choices on what data is published and in what way. These views also contain a divide between public and private. In this way a person is autonomous and free from excessive intervention of the state (Scassa, 2014).

To define the broad concept of privacy, four dimensions are differentiated (Tan, 1999).

1. Informational privacy. Privacy on the handling of personal data.
2. Bodily privacy. Integrity of one's body against invasion.
3. Privacy of communications, covering peoples interest in communicating and the way of communicating.
4. Territorial privacy. Limiting intrusion on a certain area.

Privacy is seen as an individual right. Privacy laws are based on control models, in this way a person can control which information is shared and in what way. The autonomy of the individual is protected in this way. This is called the right to informational privacy (Kulk and van Loenen, 2012). Westin (1970, p.7) described this right to informational privacy as:

"The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

Another understanding of privacy is based on four pillars or privacy problems (Solove, 2008).

1. Information collection. Problems involving the gathering of information about individuals. Two forms of information collection are identified: surveillance and interrogation.
2. Information processing. Problems arising in the storage, usage and analysis of information about individuals. Five forms are discussed, aggregation, identification, insecurity, secondary use and exclusion.
3. Information dissemination. This group of problems consists of revealing personal data, or the threat of spreading this data and includes seven problems. Breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion.

4. Invasion. This category of problems differs from the previous three, because it does not always involve information. It includes intrusion, and decisional interference.

(Solove, 2008, pp. 101-161).

The definition of privacy and the definition of personal data and in which way these two definitions are related have caused discussion (Cuijpers and Marcelis, 2012, Schwartz and Solove, 2011 and Kuner, 2009). Kuner (2009) states that privacy and personal data protection are two different things, privacy is broader, but some overlap between personal data and privacy is possible. Cuijpers and Marcelis (2012) state that personal data protection has its foundation in the right to privacy.

Data protection and privacy are described as non-identical twins. Data protection laws focus on which data identifies a person and in what way data about a person is processed. The definition of privacy contains more aspects. It can be seen as a container definition surpassing the objectives of personal data protection. The definition of privacy includes the protection of personal space for example a home with protection for private, family and home life, moral and physical integrity and reputation. It is a broader concept and is independent of personal data protection, although some overlap does exist (Kuner, 2009).

The main focus in this research is on informational privacy. Informational privacy is of importance when the personal data legislation is discussed, because the informational privacy deals with personal data.

3.1.1 *European privacy legislation.*

Different developments in privacy legislation in Europe are discussed, because the research focuses on personal data protection in Europe. It starts with the Council of Europe following the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations in 1948. The Council of Europe set up a convention for the Protection of Human Rights and Fundamental Freedoms. The Council aimed at achieving greater unity between the Member States, this is pursued by maintenance and further realisation of Human Rights and Fundamental Freedom (Council of Europe, 1951, p.5). Article 8 of The European Convention on Human Rights states that every human has the right to respect of private and family life (Council of Europe, 1951, article 8.1).

“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others” (Council of Europe, 1951, 8.2).

This article gives the foundation for privacy legislation in the European Union. The Council of Europe stated that the increased use of communication technology led to shortcomings in the Article 8 definition of the European Convention on Human Rights. Due to these shortcomings Convention 108 was designed. Convention 108 is a convention signed by the Member States of the Council of Europe. It is called the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data. Convention 108 defines personal data as:

“Personal data" means any information relating to an identified or identifiable individual ("data subject"); (Council of Europe, 1981, article 2.a).

It states that automatically processed data can only be obtained lawfully, stored with a specific purpose, accurate, and updated and stored in a form in which the data subjects no longer than the required purpose can be identified (Council of Europe, 1981).

In 1992 the treaty of Maastricht was signed. This led to the creation of a political union and a common market. The common market and a political union also led to the need for new privacy regulation (Cate, 1995) which resulted in Directive 95/46/EC on processing of personal data and the free movement of this data. Through European history there is a clear shift from privacy legislation to personal data protection legislation, the newer Personal Data Protection Directives are discussed in the coming parts.

3.1.2 *Directive 95/46/EC*

Directive 95/46/EC is the legislation to regulate the processing of personal data. The main objective is to secure personal data protection for all EU citizens. It also aims at an equal level of data protection between EU Member States to facilitate the free flow of data between Member States on the internal market (European Commission, 2012a). The purpose of the directive is to harmonise personal data protection laws amongst the EU Member States. To reach this goal the Directive sets a minimum level of protection (Fromholz, 2000, p.468).

Directive 95/46/EC defines personal data as: "(a) 'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (European Union, 1995, article 2a).

National laws must guarantee that processed personal data is up-to-date, accurate, relevant, and not excessive (European Union, 1995). Also processing personal data that contains information about "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life" is firmly confined and can only be processed if the person has given written permission (European Union, 1995, p.40) (Cate, 1995, pp. 433-434).

The data processors also need to inform the data subjects that their data is processed, and in what way they can access their personal data and edit their data. The data needs to be protected and the processors need to be registered. In the Directive it is also stated that a person can't be subject to a decision that produces legal effect, for example work related effects, or credit rating only based on automatic processing of personal data. There must be an independent authority established by the Member State, and there must be possibility of civil liability against data processors and unlawful processing of data. The transfer of data to countries that do not offer enough protection is also prohibited (European Union, 1995).

The Directive also has led to some debate, especially the transfer of personal data to the United States of America is heavily debated. Some argue that the United States lack data protection laws. The increasing importance of data in society and the use of data in companies plays a key role in the debates (Cate, 1995).

Directive 95/46/EC states:

"Member States shall provide that personal data must be:

(a) Processed fairly and lawfully;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) Accurate and, where necessary, kept up to date ; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified ;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use" (European Union, 1995, article 6).

The Directive is legislation to tackle the increased use in internet and challenges to privacy, but with more computational power and increased internet the protection of privacy has become more challenging than in 1995. There is some discussion on Directive 95/46/EC.

3.1.3 *Discussion on the Directive*

The objectives of the Personal Data Protection Directive have only been partially achieved (European Commission, 2012a). Data collection and data sharing across borders has increased with the use of internet, this led to challenges for Directive 95/46/EC.

A challenge is the different implementations of the Directive 95/46/EC by the Member States, due to the differences in definition of privacy and personal data between Member States. The differences in enforcement, implementation and interpretation between EU Member States have also led to hindering of the internal market, and cooperation between public authorities. Facilitation of free flow of data in the internal market, one of the Directive 95/46/EC objectives, is compromised by these differences and have led to legal fragmentation with high costs, the administrative burden has been estimated at three billion euros (European Commission, 2012a).

Business transactions are often supported by information technology, this leads to a flow of personal information. Online services are accessible to all EU Member States, resulting in different flows of personal information across borders. The fragmentation in the personal data protection stems from the different interpretations of the broad definitions in Directive 95/46/EC (European Commission, 2012a).

Article 5 of the Directive states that "Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful" (European Union, 1995, article 5). To provide harmonised interpretation of the Personal Data Protection Directive by Member States a mechanism is needed. This mechanism could provide a more common interpretation of the Directive, it is created by expanding the powers of the Article 29 Working Party and the European Commission. Processing of data is treated differently by different EU Member States, the following definitions are problematic for the harmonised interpretation (European Commission, 2012a, p.13).

- Consent: defined in the Directive as "shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (European Union, 1995, article 2h). National laws differ on the interpretation of consent. Sometimes consent needs to be given expressly and even in writing, while other laws require implied consent (European Commission, 2012a).
- Sensitive data: processing of this data is prohibited, unless the data processor meets certain requirements. The sensitive data mentioned in the Directive are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life

(European Union, 1995, article 8.1). Some Member States have added categories, i.e. biometric data, or medical data. While other Member States have less categories.

- Notification: data controllers have the obligation to inform the Data protection authority (DPA) about the processing of data, but some exemptions are made. Some countries can make exemptions based on national law, this leads to differentiation and higher costs, the overall costs of notification are estimated at 130 million a year (European Commission, 2012a).
- Transfer to third countries: to transfer and process data outside the European Union, different requirements have to be met. First, the level of protection needs to be adequate. This definition differs between Member States. Second, there need to be 'standard contractual clauses', these are clauses developed by the EU for the transfer of data, some Member States oblige DPA to give permission for the transfer beforehand, this gives the data controller a chance to add requirements. Third, Binding Corporate Rules (BCR) have some shortfalls. BCR are rules to transfer data between companies with the same multinational mother company. Shortfalls are not all Member States acknowledge BCRs made in other Member States. The recognizing and approving of BCRs takes on average six months and up to two years in complex cases and is limited to data controllers not data processers. Also there is no certainty about applying BCR to a group of companies (European Commission, 2012a).

The lacking of enforcement of data protection rules in the EU is another problem. Mainly because funding for Data Protection Authorities is not sufficient, national DPAs have different power and rights between Member States to enforce legislation and give advice, and there is no cooperation between national DPAs. Also regulatory powers for the European Commission are lacking (European Commission, 2012a).

A part of the discussion focusses on the differences between Member States on the 'identifiability' of a person. Recital 26 of Directive 95/46/EC (European Union, 1995) describes identifiability as: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;" (European Union, 1995, recital 26).

The focus of the discussions is on the "all means likely reasonable" (recital 26 of Directive 95/46/EC). This definition is broadly implemented in the different EU Member States. Another definition in recital that led to differences in implementation by Member States is "any other person" (European Union, 1995, recital 26). An example of this form of identification is the use of biometrics. Biometrics are a unique identifier, but the knowledge and access to biometric databases are hard to obtain for the average person (Cuijpers and Marcelis, 2012).

This definition of possible identification leads to a stretch of the concept of personal data. Where data that does not necessarily lead to identification is considered personal data. This stretched definition is further used in opinions of the Article 29 Working Party (Cuijpers and Marcelis, 2012). When this stretched definition is used on an open source, for example the internet almost all of the data on the internet is personal data. Examples are HTTP cookies and ip-addresses. Because use of this data in combination with other data can lead to identification of a person, this is considered personal data by the Article 29 Working Party.

However, the processing of the data will not lead to identification, because the data does not have the purpose to identify a person and the data controller will not use the data to identify a person (Cuijpers and Marcelis, 2012).

The discussions focus mainly on the definition of personal data, and on the way Directive 95/46/EC influences technology. The discussions have led to a proposed reform of Directive 95/46/EC.

3.1.4 *Reform of the data protection rules*

The European Commission proposed a reform of the data protection rules. Some key features of this reform are the right to be forgotten and one set of data protection rules for the European Union (European Commission, 2012). The right to be forgotten means that a person is able to request the deletion of all the data about themselves: "The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of that data, where one of the following grounds applies:

(a) The data is no longer necessary in relation to the purposes for which they were collected or otherwise processed

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6 (1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19; (a) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;

(d) The data has been unlawfully processed" (European Commission, 2012b, article 17).

In practice this means that a search engine has to delete links to information concerning the data subject whenever the data subject requests this. The search engine can deny this request, when the data subject has a public role and the general public has an interest in the access to the information (European Commission, 2014b).

The new draft legislation is a Regulation instead of the previous Directive which means it is binding Legislation for the whole of the EU. A Directive is a legislative act with goals that all Member States have to achieve, but the Member States can decide on how to achieve the goals (Europa, 2015). The choice for a Regulation is based on the advice of the European Data Protection Supervisor (EDPS). The regulation is needed to tackle the problem of harmonisation in the EU Member States, in this way there will be less room for differences in interpretations (EDPS, 2011). The Regulation defines first the data subject, after that definition personal data is defined as information relating to a data subject.

"'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, locational data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) personal data' means any information relating to an identified or identifiable natural person (' data subject') ; an identifiable 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, unique identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social or gender identity of that person;" (European Parliament, 2014, article 4.1 and 4.2).

The proposed Regulation gives a new definition to pseudomized data, it defines pseudomized data as: "'pseudonymous data' means 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" (European Parliament, article 4.2a, 2014). Meaning the stretched definition of personal data by linking, combining and using of additional information is recognized by the European Commission.

The new proposed Regulation does not reform the personal data definition but rather extends the definition. It is mainly aimed at the protection of personal data and privacy on the internet. The proposed Regulation is also more specific, because it defines more factors for identification.

3.2 *Open data*

In this part of the research open data will be discussed, the history of open government, the definition of open data, the different EU Directives, and barriers for open data.

3.2.1 *Open government*

Throughout history citizens have called for more government transparency and accountability. This led to the open government movement, resulting in the establishment of the Open Government Partnership. In this partnership governments around the world cooperate in making their government more open and responsive to citizens. The partnership started in 2011 with eight members and has since grown to 64 members (Open Government Partnership, 2014).

More openness and transparency are still the main goals of the modern open government movement, in addition to these goals the open government movement strives for more citizen participation in governance, for example by using social media. Innovation and knowledge are also promoted, this promotion is done by governments releasing large amounts of data, available for reuse without costs or at marginal costs and few or no restrictions for reuse. These goals of open government can be divided in three pillars: open access, open data, and open engagement. There are some overlapping features of these three components, but all three have also distinct features, especially concerning privacy and data protection issues (Scassa, 2014).

3.2.2 *Open Data*

More and more government bodies publish open data on the internet. Open data means that data is opened to be reused by different government bodies and the public. Open Government Data (2014) gives the following definition of Open Data: Data that can be used freely, reused and distributed by anyone, without reuse restrictions (Open Definition, 2014).

Public data, which is data that has been collected or paid for by the government, can be opened up and reused. It is seen as an economic opportunity by the EU commission. The EU is pro use of Open Data and stimulates the reuse of PSGI through open data policies (European Commission, 2011).

There are four main reasons for governments to open up (geographic) data (Open Government Data, 2014).

1. Transparency: transparency is of importance for democratic processes in a country. It leads to a better understanding of the actions of a government.
2. Releasing economic and social value: data is becoming more and more important to modern societies. The government owns a lot of data, by opening up this data innovative new businesses are able to use this data. This creates new economic and social value.
3. Participatory governance: citizens can be informed about policy by the government and give feedback. By opening up governmental data citizens can participate in decision-making (Open Government Data, 2014).
4. Government efficiency: governments publishing open data, can focus on data self and not on overhead costs of acquiring and transferring data, and the marketing around data. Leading to more government efficiency (ePSI, 2012).

The European Union supports open data for the following four reasons (EU Open Data, 2014).

1. Reuse in services and applications. New value added application and services are created with open data.

2. Addressing societal changes. New and innovative solutions to societal problems come to light with the use of open data.
3. More efficiency for public bodies, because there is open access to data between the different public bodies.
4. More citizen participation in political and social life, this leads to a more transparent government.

The aforementioned reasons to open data, and societal pressure give a legitimation for opening up of data and more transparent governments. Opening up of data is seen as an opportunity by the EU. To regulate this opportunity the EU created two Directives.

3.2.3 *Directive 2003/98/EC*

To develop the potential of open data, the European Commission, adopted the Directive 2003/98/EC on the reuse of public sector information. Directive 2003/98/EC is based on two goals, one making public information available to third parties, at a low cost and unrestricted conditions and second establish a level playing field for the public sector operating in the data market, and private sector companies (Janssen, 2011, pp.446-447). Some documents are excluded from the rules of this Directive. In Article 1.2 different types of public sector information are mentioned (European Union, 2003, p.93). There is also a mention of the previous discussed Data Protection Directive 95/46/EC.

"This Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Community and national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC" (European Union, 2003, article 1.4).

Reuse of personal data is not strictly forbidden, but a case-by-case assessment is necessary to see if making data available for reuse is possible. In some cases anonymization of data is necessary (Janssen, 2011, p.447).

3.2.4 *Directive 2013/37/EU*

In 2013 the Directive 2003/98/EC was amended. The foundation for the amendment is stated in the Directive as: "Directive 2003/98/EC should therefore be amended to lay down a clear obligation for Member States to make all documents reusable unless access is restricted or excluded under national rules on access to documents and subject to the other exceptions laid down in this Directive" (European Union, 2013, p.2). The option in Directive 2003/98/EC is replaced in the PSI Directive 2013/37/EC by an obligation to make all documents reusable for commercial and non-commercial purposes, except the exemptions. (Article 29 Working Party, 2013).

The foundation for the change from option to obligation can be found in the general principle of the Directive. The general principal is amended into: "Subject to paragraph 2 Member States shall ensure that documents to which this Directive applies in accordance with Article 1 shall be reusable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV" (European Union, 2013, p.6).

The full right to reuse can lead to more and better access to public sector information in the European internal market. There is however a difference with open data, because the opening up of data for reuse still needs to be requested. The Member States are encouraged to open up data, but not obliged to actively give open access and support open access to the PSI (Janssen and Hugelier, 2013).

Reuse of data is the most important aspect of opening up of government data, reuse happens mainly on a computer. That is why data formats are of importance for the availability of PSI.

A machine readable format accompanied with meta-data (data characterizing the PSI) is supported by the Directive. Directive 2013/37/EU states: "Public sector bodies shall make their documents available in any pre-existing format or language, and, where possible and appropriate, in open and machine-readable format together with their metadata. Both the format and the metadata should, in so far as possible, comply with formal open standards" (European Union, 2003, p.6).

The Directive 2003/98/EC and the current Directive do not state any obligations towards a certain format, because this is an administrative burden for the Member States. Machine readability is an addition that leads to more reuse possibilities (Janssen and Hugelier, 2013).

The internal market functions when datasets can be obtained cross-border. In this Directive the following is stated: "Member States shall make practical arrangements facilitating the search for documents available for reuse, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible Member States shall facilitate the cross-linguistic search for documents" (European Union, 2013, article 9). To strengthen the internal market and increase the cross-border data flows article 9 is amended. According to the stakeholders in an EU questionnaire, reuse of PSI needed to be promoted in the whole EU (European Commission, 2011a).

This amendment is a step towards more cross-border transfer of open data. To facilitate this step Member States should take action to facilitate the cross-linguistic search for documents and make documents available and usable (Janssen and Hugelier, 2013).

To conclude, the focus of the European Union on opening up data for reuse is growing. With the amended Directive 2013/37/EU the obligation gives new impulses to public sector bodies for opening up data. The exemptions are also of importance, but can lead to certain barriers, which will be discussed in the next section.

3.2.5 *Barriers for use of open data*

From a user perspective there are different barriers for using and reusing open geographic data. Firstly, there is a difference between available open data and the required open data for companies and entrepreneurs to create value added products. Secondly there is no clear sight on the available geographic data. This is a result of the growth of different open data portals, which leads to the fact that not all open data can be found by potential users. Thirdly an important barrier in the European internal data market is the protection of personal data. (Ministry of economic affairs, 2013).

Huijboom and Van den Broek (2011) mention some barriers and drivers for implementation of open data. The biggest barrier is a closed government culture, the second biggest barrier is privacy legislation, the legislation to protect the privacy of citizens and the third barrier is the limited quality of data. For the first two barriers terms as confidentiality, fear of political escalation, and risk avoidance are mentioned. Governments do not want to disturb their own administration, and not risk the privacy of their citizens. Governments receive opportunities by opening up data (innovative business), but on the other hand opening up of data leads to threat of less privacy.

A barrier in the use of open data is Directive 95/46/EC on processing of personal data and the free movement of this data. Directive 95/46/EC demands that all data is processed fairly and lawfully and is collected and processed with a specific purpose (European Union, 1995). The Directive creates some exemptions to the PSI Directive (chapter 3.2.4).

The personal data issue is important also, because open data can be linked together in a mosaic effect. The linking of datasets in a mosaic effect can lead to identification of people.

Open data advocates in the United Kingdom, argue that the fear of losing privacy is not an argument to not opening up data (Rothenberg, 2012).

3.3 *Geographic data*

This section deals with geographic data, the opening of geographic data and differences in use of the types of geographic data. The European Commission gives geographic datasets the highest priority to be opened up (Figure 1) (European Commission, 2014).

Geographic data is data that has a link to a place on earth, or an address. For example coordinates, zip-codes and ip-addresses. One way of dividing geographic data is in two types: administrative and factual geographic data.

The administrative type of geographic data contains datasets with addresses, zip-codes and cadastral outlines. This type of data is virtually present, but not factual on the earth. The factual type of geographic data contains datasets with topographic maps, elevation and (aerial) photographs of the environment (Figure 2, 3, 4). This type of data has a factual place on earth (Van Loenen et al., 2008).

Another way of dividing is organising the different types of data threefold, based on the highest reuse rate (Fornefeld et al., 2008).

1. Topographic information (Figure 2).
2. Cadastral information, including addresses and coordinates.
3. Aerial photography (Figure 3).

(Fornefeld et al., 2008).

Another type of geographic data that is published and used across EU borders are themes from the Infrastructure for spatial information in the Europe (INSPIRE). The goal of the INSPIRE Directive is to create a European spatial data infrastructure (INSPIRE, 2014).

There are different themes about administrative types of geographic data, and about factual geographic data (INSPIRE themes, 2014).

Opening up of geographic data has an important place in the EU open data strategy. The market for geographic information is growing since the first PSI Directive in 2003. The importance of opening geographic data is shown by different researches. Geographic information is commercially the most interesting data (Van Loenen et al., 2008).

The datasets with the highest priority to be opened are geographic datasets according to reusers from Europe (European Commission, 2014a, p.5). But as seen in the previous section the opening up of data on the internal market comes with some barriers. In the next chapters different EU Member States cases are studied to research to which extent geographic data is considered personal data.

Category	Examples of datasets
1. Geospatial data	Postcodes, national and local maps (cadastral, topographic, marine, administrative boundaries, etc.)
2. Earth observation and Environment	Space and in situ data (monitoring of weather, land and water quality, energy consumption, emission levels, etc.)
3. Transport data	Public transport timetables (all modes of transport) at national, regional and local levels, road works, traffic information, etc. (*).
4. Statistics	National, regional and local statistical data with main demographic and economic indicators (GDP, age, health, unemployment, income, education, etc.)
5. Companies	Company and business registers (lists of registered companies, ownership and management data, registration identifiers, balance sheets, etc.)

(*) Sector-specific rules (e.g. EU railway law) make take precedence

Figure 1: Categories of datasets with the highest priority to be opened up. Source: European Commission, 2014, p.5.

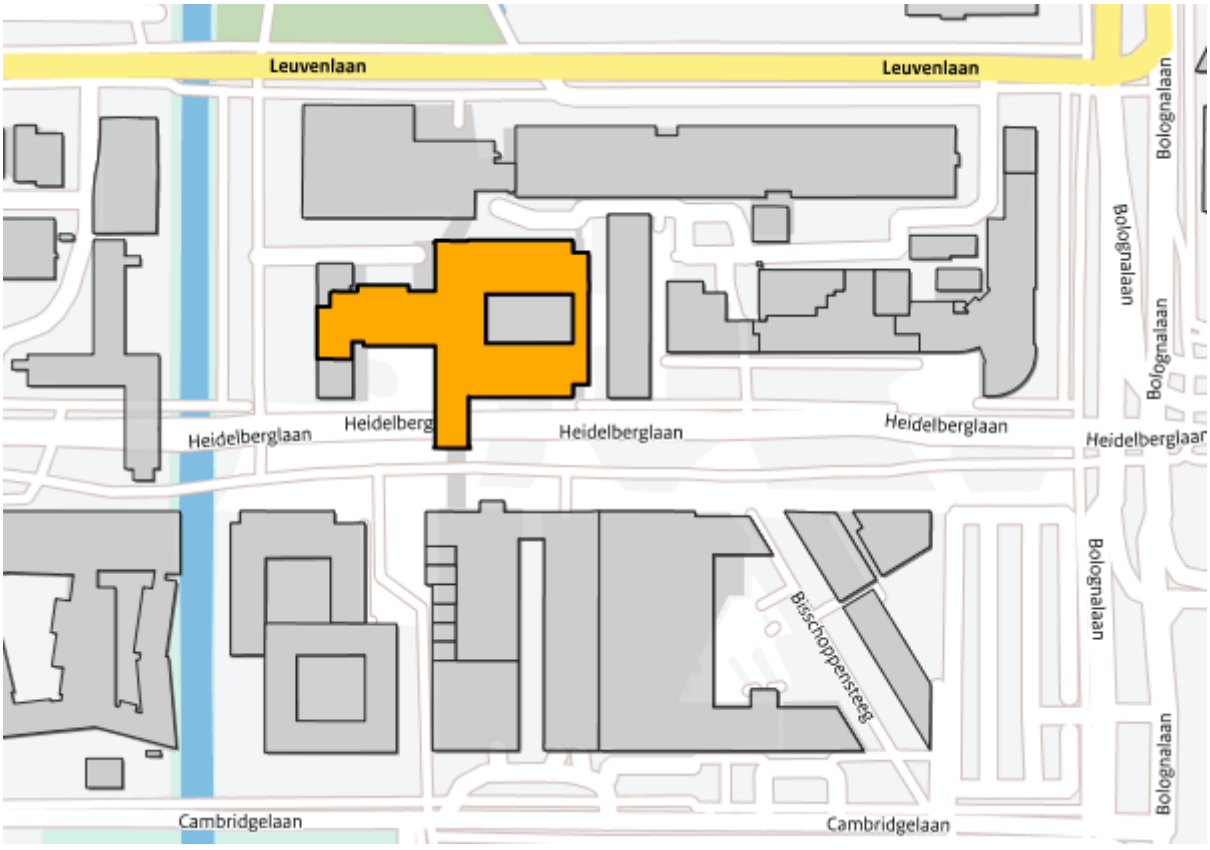

Figure 2: Key register of building in Utrecht Uithof area. Source: Bagviewer, 2015.

Figure 3: Satellite image with 40 cm resolution. Source: Mapbox, 2014

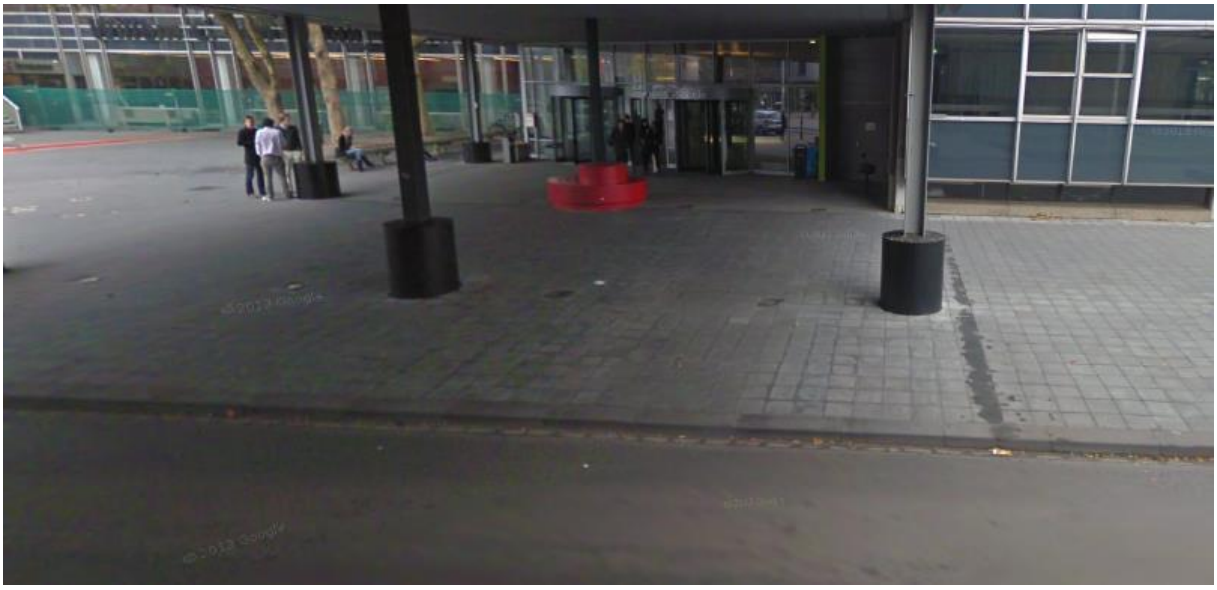

Figure 4: Street view image of Utrecht Uithof. Source: Google Street View, 2015.

3.4 *Introduction of the case studies*

To look at the differences between the EU Member States, different EU Member States have been selected as case studies. The selection is based on the differences in opening up of geographic data and the differences in interpretation of Personal Data Protection Directive.

The first case is the Netherlands. There is literature available on their open data policy implementation and because the researcher is located in the Netherlands it is also more convenient to reach stakeholders and personal data protection authorities. There is also a lot of open geographic data available. The case is used to give an insight into how personal data is defined and how geographic data is defined, and to what extent geographic data is considered personal data.

The second case is Belgium. The choice for Belgium is based on the differences in data protection legislation. It does not rank in the top of the Open Data Index, but at the tenth place of the privacy index (Privacy International, 2007). The culture resembles the Dutch culture, and the same language is spoken.

The third case is Germany. The choice for Germany is based on the German view on privacy, which is different of the rest of Europe. Germany has one of the strictest views on personal data protection. It is in the sixth place of the privacy index (Privacy International, 2007). An example is the resistance to Google Street View (Focus Magazin, 2009).

The fourth and last case is the United Kingdom, because it is part of the 'big three' of most powerful EU member states that took initiative for the Personal Data Protection Directive (Newman, 2008). In the UK, there is a less strict definition of privacy than in the Netherlands (Janssen, in van Loenen and Verdonk, 2011). It is the most open EU Member State (Open Data Index, 2014), this makes it a typical case to see in what way geographic data can be considered personal data.

The case studies are focused on INSPIRE data consisting of topographic maps and addresses and buildings registry's, and mobile mapping consisting of geographic data collected via photographs such as 360 panorama shots and aerial photography. For example Google Street View images, aerial photographs of homes and satellite images of homes.

Based on the literature there are different interpretations of the personal data definition. The differences exist between EU Member States. The analysed case-studies are analysed based on the differences between organizations. First the legislation is analysed, and after that the executers of the legislation, the data protection authority and courts. In this research the differences are interpreted and after the interpretation analysed and it proposes a solution to harmonize the different interpretations. In this way the internal market profits, and it eases cross border operations by businesses.

To create an insight in the different interpretations a matrix is used. The matrix consists of four different perspectives and three different parts. The perspectives are: jurisprudence, legislator, data protection and data source. And it focuses, on if the geographic data is considered personal data, the argumentation and whose responsibility this is.

1. The cases in the matrix are built up in the following way.

- The data source holder. The data source holder is the data processor, for this part the interview with Martin Te Dorsthorst is used (Annex A). The source holders are also found in the literature. This interview handles the interpretation of the personal data protection legislation. The interview is also used as validation for the found differences.

- Legislator. The perspective of the legislator consists of the national parliaments. The discussions on different legislations are used and researched.
- Data protection authority. The Data Protection Authority is an authority to protect personal data of citizens. The role of Data protection authority was institutionalized by the European Commission in Data Protection Directive 95/46/EC.
- Jurisprudence. Different courts have rulings on geographic data as personal data. The arguments for the rulings are discussed and analysed.
- An interview with Cyclomedia is conducted. This company operates on some European markets, and deals with different demands of governments concerning the protection of personal data. This is done to analyse the arguments for the use of imagery and the different interpretations between EU Member States. The interview serves as validation for the different perspectives found in the literature.

2. The matrix and interviews are interpreted and lead to recommendations for the Data Protection Directive in the European Union.

The introduction of the case studies gives a short insight on the motivation for the different cases. The coming part shows how the theory is used in the EU Member States.

4 *Europe*

For this case the different perspectives in the European Union are discussed. First some explanation with regard to the personal data definition in Directive 95/46/EC by the Article 29 Working Party is discussed. Second, the perspectives of the European Court of Justice (ECJ) and European Court of Human Rights (ECHR) with regard to personal data are given and discussed.

4.1 *Personal data definitions and explanation.*

In Europe different definitions are used and explained differently by different stakeholders and actors. In this part different definitions are discussed.

4.1.1 *Article 29 Working Party*

The independent European advisory body on privacy and data protection is called Article 29 Working Party. The Working Party analyses the definition of personal data, it is used by interpretation and application of the Personal Data Protection Directive in EU Member States.

The Working Party considers the definition in Directive 95/46/EC of personal data a broad definition, because it uses the terms 'any information'. Any information means any statement on a person is considered personal data, these statements don't need to be true (Article 29 Working Party, 2007, p.6). Not only information about a person, but also information about objects belonging to a person are considered personal (Article 29 Working Party 2007, p.9). Also the identification of a person is defined when it is possible to distinguish a person from a group. Sometimes a person is identifiable by combining different data (Article 29 Working Party 2007, pp. 12-13).

Directive 95/46/EC defines personal data as: (a) 'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (European Union, 1995, article 2a).

The definition of personal data can be broken down into four parts. The first part any information leads to a wide definition of personal data, because it does not matter if the information is true, or false, and what medium carries the information (Article 29 Working Party, 2007). Relating to gives information about the relations and the importance of the relations.

The third part is identified or identifiable and focuses on the discussion about indirect identification. The Directive states: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person;" (European Union, 1995, recital 26).

The fourth part is the natural person him- or herself. A person needs to be a living human being. The Working Party also discusses the possibilities of deceased people, unborn babies and legal persons (Article 29 Working Party, 2007, pp.21-23). It concludes that the Directive has a broad definition and this discussion can be used as a guideline with more focus (Article 29 Working Party, 2007). The broad definition of the concept of personal data leads to hinder in the digital internal market, because trans-border processing of data within the EU is impeded (Cuijpers and Marcelis, 2012). This is mainly caused by differences in interpretation of Directive 95/46/EC. Some EU Member States use the broad definition while other Member States have more strict definition.

An example of the differences in interpretation is if the price of a house is considered personal data. The Article 29 Working Party considers the price of a house not to be personal data, when the data is used to get information about the housing prices in a district. When the information is used to get information about the owner of the property, for example taxation information, the information has consequences for the owner and the price of a house is considered personal data (Article 29 Working Party, 2007, p. 9). The used definition: “any information relating to an identified or identifiable natural person.”

The price of a house is in this context referring to: “information relating to”.

When the price of a house is indexed and opened on the internet it comes under scope of the definition of personal data in Directive 95/46/EC (Article 29 Working Party, 2007, p.9).

The conclusion of the Working Party is that the definition leaves room for a broad interpretation of Directive 95/46/EC, but if data is considered personal data depends on the context of the processing of data.

4.1.2 *EDPS*

The European Data Protection Supervisor (EDPS) is an independent supervisory body committed to the protection of personal data protection for EU citizens and it advices and controls the EU institutions on the way personal data is treated. The EDPS can be considered the Data Protection Authority in the European Union. It gives advice to the European Commission on Data Protection Legislation. Recently the EDPS published an own draft of the General Data Protection Regulation in a mobile phone application for review by EU citizens. It gives recommendations on the Draft General Data Protection Regulation. A for this research interesting example is the recommendation to delete the clause that data collected for one purpose can be used for another purpose if the motivation for doing this overrides the interest of the data subject (EDPS, 2015, Article 6.4). It is interesting because this is argued by the EDPS in the opinion on open data (2012). EDPS states that open data is used specifically for new innovative apps and does not have a purpose, while for personal data protection purpose limitation, data should only be processed with a specific purpose, is a key principle. This makes data protection and open data hard to balance according to EDPS (2012).

The EDPS also places remarks at the introduction of Google Street View in Europe. The former Data Protection Officer Peter Hustinx warned Google in 2008 that the service could collide with European privacy legislation. He warned Google: "Making pictures on the street is in many cases not a problem, but making pictures everywhere is certainly going to create some problems. I'm quite sure they are aware of this" (EUObserver, 2008).

For the reuse of public data the EDPS recommends an assessment to decide on whether the personal data can be made available for reuse. This assessment should also show under what conditions and subject to the specific data protection rules the reuse can be permissible. The reuse is only possible with a purpose compatible of the original purpose of the data (EDPS, 2012).

4.1.3 *ECJ and ECHR*

Personal data and its definition is also of importance in European Court of Justice (ECJ) and European Court of Human Rights (ECHR) case law. The ECJ has as mission to ensure that “the law is observed in the interpretation of the Treaties” (Curia, 2015). It reviews the legal aspects of the laws of the European Union institutions. It makes sure that the EU Member States comply with Treaties ‘obligations and gives interpretation on the European Union legislation, as requested by the national courts and tribunals (Curia, 2015).

The ECHR is an international court with 47 judges of the Member States that have ratified the European Convention on Human Rights. It applies this Convention and makes sure that States respect the European Convention on Human Rights (ECHR, 2015).

In an ECJ case the used definition of personal data is narrower, than the previous discussed definition of personal data by the Article 29 Working Party. The definition used by the European Court of Human Rights (ECHR) is based on article 8 of the European Convention on Human Rights. It refers in cases to the right to private life and private correspondence. It defines personal data as: “"personal data" means any information relating to an identified or identifiable individual ("data subject");” (Council of Europe, 1981, article 2.a).

The European Court of Justice gives a more narrow definition, in the case ‘YS (C‑141/12) v. Immigration and Asylum Minister (*minister voor immigratie, intergratie en asie*l’). In this case, an application is made for a residence permit. The case-officer makes a document (‘minute’) and this minute is used for juridical analysis. On this minute:

“name, telephone and office number of the case officer responsible for preparing the decision; boxes for the initials and names of revisers; data relating to the applicant, such as name, date of birth, nationality, gender, ethnicity, religion and language; details of the procedural history; details of the statements made by the applicant and the documents submitted; the legal provisions which are applicable; and, finally, an assessment of the foregoing information in the light of the applicable legal provisions are mentioned” (ECJ, 2014, paragraph.14). This assessment is the legal analysis.

Until 14 July 2009 the Minister made the minutes available upon request, but in the current situation the results were not made available. In the two cases (Case C-141/12 and C-372/12), questions were raised about whether or not the minute with data about the applicant and legal analysis were considered personal data, in accordance with Directive 95/46/EC, art.2. The data relating to the applicant is considered personal data, but the legal analysis was under discussion. The Greek, Portuguese, and Austrian governments and the European Commission state that the legal analysis refers to a specific natural person and should be personal data. In contrast to the Dutch, French, and Czech governments who argue that it is not personal data. The ECJ ruled that although, the legal analysis contains personal data, itself is not personal data. “The data in the legal analysis contained in that document, are ‘personal data’ within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified” (ECJ, 2014).

To research the available case law on personal data and geographic information at the European Court of Human Right, the HUDOC search engine is used (HUDOC 2015). To research the available case law at the European Court of Justice the Curia search engine is used (Curia 2015). To research the possible case law different search queries were performed (Table 2). There was no case law with the used queries.

Mobile Mapping	INSPIRE
“Mobile Mapping”	“INSPIRE”
Personal data Google Street View	Personal data geographic information
Personal data satellite images	Personal data INSPIRE
Personal data digital images of homes	Personal data topographic data
Google Street View	Personal data building
Digital images of a home	Topographic maps
Satellite images of a home	“Maps”
“Satellite”	

Table 2: Used search queries.

5 *The Netherlands*

To research the protection of personal data and to learn to what extent geographic data is considered personal data different perspectives are used. Starting with Dutch legislation, the perspective of the Dutch Data Protection Authority is discussed and the perspective of the Dutch jurisprudence as last. These perspectives are used on two different types of data. First mobile mapping data, and second INSPIRE data.

5.1 *Legal context*

The Netherlands treats data protection as a 'sui generis right', this means that it has no specific characteristics, and the right of privacy and personal data protection is protected in the Dutch constitution. In Dutch law and case law personal data protection can be linked to specific rights, for example the right to privacy and the right to personality (Korff, 2002). The e-privacy Directive 2002/58/EC is implemented into Dutch national law by an amendment to the telecommunication law.

The personal data definition given in Directive 95/46/EC is used in most EU Member States. This definition is also translated in national law in the Netherlands. Personal data is defined in the Dutch Wet Bescherming Persoonsgegevens (WBP). Personal data is defined as:

"persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;" (Wet bescherming persoonsgegeven, 2000, Article 1A).

This means that every datum (*gegeven*) relating to an identified or identifiable natural person is considered personal data. The word datum is chosen as definition because, this resembled previous legislation in the Netherlands. When a datum is presented, it is of importance to decide if it contains information about a person. In most cases, it is clear when factual data and opinions contain information about a person. Examples are in certain context telephone numbers, zip codes with house numbers, and license plates. For example, if the data helps to determine the way a person is assessed and treated in society it is considered personal data.

But in other cases, it is unclear. Data not relating to a natural person and without societal consequences for a natural person in the context of processing, are not personal data. For example stolen goods, or identity cards that are not used for the processing of personal data and thus don't have consequences for the societal position of a natural person, are not considered personal data. It does not matter that use of these goods can lead to identification, for example with use of cadastral registration. It changes when dissemination of this register happens, and the register becomes searchable by natural persons (Kamerstukken, 1998, pp. 45-47).

The second part of the article consists of identifiable data. A person is considered identifiable when the identity of a person can be determined without disproportionate effort. Two factors are important with identifiability. First, the possibilities to identify a person by the controller and second, the nature of the data. Identification of a person is possible based on the physical, physiological, psychological, economic, cultural, or social identity of a natural person. When a person is (almost) directly identified, the nature of the data is direct identifiable data. For example name address, date of birth. Other data have an indirect identifiable nature. The data can be used for identification under conditions or in combination with other data. Examples of indirect data are social security numbers, or DNA (Kamerstukken, 1998, p.48).

The second part relevant to the criterion of identifiable are the known and available means for a controller to identify a person. These consist of all proportionate means by the

controller to identify a person. An example is that the statistical bureau has more possibilities to identify a person than a single researcher, because of their expertise, contacts, and technical amenities. Data is not personal data when there are measures to prevent identification of that person. For example, data that is encrypted with a code (Kamerstukken, 1998, p.49).

In the Netherlands the data protection authority is the College Bescherming Persoonsgegevens (CBP). The mission of CBP is to supervise if the processing of personal data is according to the law, and gives advice about laws protecting personal data (CBP, 2014). CBP defines personal data in accordance with the WBP. All data that can provide information about a natural person must be considered personal data. It mentions some examples of personal data: name, address, residence, telephone numbers, license plates, and postal codes with a house number (CBP, 2015).

5.2 *Mobile mapping*

The mobile mapping case in the Netherlands has different perspectives. First, there is some information about legislation and discussions in the parliament. Second, different cases and views from the Data Protection Authority are discussed and third, jurisprudence about a case of personal data on Google street view and Google earth is mentioned.

5.2.1 *Legislator*

The Dutch Parliament discussed Google Street View in 2010. The discussion focused on the dissemination via the internet of images of persons in public places. Also, the storage of the images, opt-out options for citizens, and notification to the public were discussed. The first questions were about the invasion of the right to privacy of persons when their pictures were taken in public places. The minister concluded that there was no invasion of the right to privacy, when the faces and license plates were blurred. The images of homes of people were not discussed. The next question was about the storage of images. Google stores the images for a year to develop techniques to blur faces and license plates, the Minister referred to the CBP for supervision of compliance to the WBP. The Minister states that Google is careful in the collection and processing of images and that it is not in conflict with the law. Google does not have an obligation to offline inform the citizens of city or town, because all the information on the website is clear and the local press can help disseminate the message. The Minister states that the information Google provides on the duration of the opt out option is clear. It takes 48 hours and the procedure can be found on the Google website (Kamerstukken, 2010).

5.2.2 *Data Protection Authority*

The Dutch data protection authority ruled in 2001 that digital images of geographic content are in some cases considered personal data. When data is personal data, WBP is applied. This law applies when geographic data is used to review unique objects, and the review has consequences for the owners of that object or building, for example taxation or valuation. When this data is collected and processed the data protection law has to be taken into consideration (CBP, 2001).

An example of a use case is when a company makes photographic images with a 360 degrees view of the neighbourhood. Three close-ups of an object are made based on municipality, street, and address, linked with cadastral information. The views are from the outside enriched with some basic information about the object. Interested parties in these images are housing associations, utility companies, municipal, and provincial governments. The application of the images has consequences for the inhabitants of the objects. The goal is to create and maintain an optical key register of all the objects and owners (CBP, 2001). The images, are also used for valuation of property and the taxation of property (Cyclomedia, 2014).

For the Dutch law all data that gives information about an identifiable natural person is considered personal data. Data about objects is of importance when the owners of the objects can be identified without disproportionate effort and the application of the images has consequences for the owners of the property (taxation and valuation). This is considered processing of personal data, also the parties using the images are the responsible parties according to the WBP (CBP, 2001 and Kamerstukken, 1998). The collection of the images and making them available to aforementioned applications can be considered collection of personal data. The images are collected with the purpose of the applications, and the collection is focused on the application (CBP, 2011).

5.2.3 *Jurisprudence*

With the use of Google Street View and Google Maps it is possible to view satellite photos or panoramic pictures of streets. There has been a lawsuit in the Netherlands about Google Street View. The plaintiff found out that searching on the plaintiff's name in combination with the place of residence showed the following information: Name of the plaintiff's foundation, the names of the plaintiff, the address, zip code, name of the residence street and the telephone number. Via the use of Google Street View the house of two natural persons with a foundation on the address is visible. After complaints of the plaintiffs Google only displayed the street and house number. Google Maps only shows a satellite image, and the Street View images are partly blurred. The premise and all the objects on the premise that were present during the time of recording are not recognizable (Rechtspraak, 2013).

The plaintiff wants Google to delete all personal data from Google Maps and Google Street View on penalty of a fine. The plaintiff states that Google invades the plaintiff's right to privacy by displaying personal data. Based on the WBP, the plaintiff contends that the infringement ceases. Google defends that there is no infringement and that the balance of interest in the WBP should be in their favour (Rechtspraak, 2013). For processing of personal data the data subject should give permission, and the plaintiff states that the pictures of the address are considered personal data. The WBP states that processing is only possible if it is necessary for the protection of the legitimate interests pursued by the controller (Google), unless the interests or the fundamental rights and freedoms, especially the right to privacy of the plaintiff prevails. Plaintiff states that their right to privacy should prevail over the commercial interests of Google. Based on article 40 WBP Google should make another balance of the different interests.

Google states that an address and blurred image are not personal data. The data is used to identify property and not to identify a natural person. Google invokes the right on freedom of information and freedom of entrepreneurship (Rechtspraak, 2013).

The judgment followed with the statement that according to the WBP the processed data needs to be relating to a natural identifiable person. It cites the explanatory memorandum of the WBP that data without societal consequences for the data subject and not relating to a natural person are not considered personal data. On the blurred picture there is no link to the plaintiff, also the satellite image of the property does not show that the plaintiff lives in that building. The display of the address and the images are not personal data, because it lacks information about the inhabitant. Google also does not facilitate possibilities to link this information to the inhabitant. The name of the street and house number is only a location of a property and not address data. Address data would mean the data would be considered personal data (Rechtspraak, 2013).

In another case satellite images were used by the fiscal investigation and information service (FIOD) to gain evidence. A lawyer privately purchases two Bubble Club chairs, and deducts the costs as office expenses from taxes. The FIOD suspects that these two chairs were not delivered to the office, but to the suspect's home. The FIOD used Google Earth to zoom in on the backyard of the defendant and two yellow chairs were found in the backyard, resembling the Bubble Club chairs. The defence of the suspect argues the use of zoom of Google Earth on a private space is an unlawful way of investigating, and an invasion of privacy. The house and garden of a person, are places where a person has 'a reasonable expectation of privacy', in accordance to article 8 of the European convention of human rights. The use of Google Earth is not mentioned in the Law Special Investigative Powers (BOB). The defence also claims that using Google Earth can be seen as an invasion of the private life of the defendant (Rechtspraak, 2011).

The public prosecutor argues that using Google Earth can be seen as 'surveillance on the digital highway' and this is not an unlawful detection method. The reporting officer states that she has used a public internet source, zoomed in on the garden and added the snapshot to the file. The court ruled that nowadays, the use of Google Earth cannot be seen as an exceptional technical tool, because it is available for anyone with an internet connection. The court rules that only a limited infringement has been made on the privacy, and based on Article 2 in the police law there was a juridical basis to use Google Earth (Rechtspraak, 2011).

Concluding, the single case found in this research states that aerial images should be considered personal data, but in the specific instance the processing only had a limited impact on the natural person involved. Therefore the aerial image could be used for investigating purposes.

Netherlands: *360 degrees images*	Personal data	Argumentation
Data source	Yes	When the photograph contains the face of a person, considered personal data.
Legislator	No	The processing of Google Street View images are not considered personal data when a person's face and license plate of a car is blurred.
Data protection authority	Yes	If the images, are used in the context of identifying, or the images have societal consequences for a person the images are considered personal data.
Jurisprudence	360 degrees images No	Images of a home are blurred and the images lack a link between the inhabitant and the property.

Table 3: Overview of the perspectives on 360 degrees images in the Netherlands

Netherlands: *Aerial images*	Personal data	Argumentation
Data source	Not available	Not available
Legislator	Not available	Not available
Data protection authority	Not available	Not available
Jurisprudence	Yes	Personal data, because it shows the backyard of the defendant, but only a limited infringement of the right of privacy

Table 4: Overview of the perspectives on aerial images in the Netherlands.

5.3 *INSPIRE*

The implementation of the INSPIRE Directive in the Netherlands lead to some new datasets and different perspectives on the datasets and the way of dissemination. The perspective of the legislator is discussed first, second the Personal Data Protection Authority and third jurisprudence on the subject.

5.3.1 *Legislator*

In the Dutch situation there is no extra attention to the protection of personal data within the INSPIRE law. The WBP has little to no consequences for the implementation of the INSPIRE Directive in the Netherlands, because the INSPIRE legislation is aimed at already existing spatial data, there is no separate processing of data and the thematic categories are outside of the WBP scope, even if the categories contain personal data (Kamerstukken, 2008, p.10). The supply of the data is the responsibility of separate source holders. The legislation is only aimed at the access to the data, the legal compliance is the responsibility of the source holders. The holder of the data source should consider if access to their geographic data possibly leads to identification of a natural person. If the supplier of the data understands that the processor can combine the data and it is possible to identify a natural person, the data ´shifts in colour´ and is considered personal data, according to the WBP. The supplier becomes the responsible, because supplying is a form of processing, and has to operate in accordance to the WBP (Kamerstukken, 2008, p.10).

The citizen or governmental organization can request the responsible holder of the source data to remove or update the data. The Dutch Data Protection Authority has no further remarks on the decision about the implementation of this European Directive (Kamerstukken, 2008, p.10).

The Dutch Government proposed a law to create a key register containing addresses and information about buildings and associated objects (BAG). In the Explanatory Memorandum of the Key Register of Buildings and Addresses, the legislation states that in principle the Key Register does not contain personal data, because with these data itself it is not possible to identify natural persons. In a lot of cases, use of data will lead to a link with other data, resulting in BAG data being considered personal data. The supplier of this data should consider if the data is traceable to an identified or identifiable natural person, when processed by the processor. In this case the data source holder is responsible for the compliance with the WBP (Kamerstukken, 2007, p.17).

The supplier has to notify the processor of the data, that when the BAG data is processed in combination with other data and, this leads to identification of a natural person, this is considered personal data and is subject to the WBP (Kamerstukken, 2007, p.18).

Another example in line with the INSPIRE Directive is the use of large scale topographic maps (BGT). In the Netherlands there was already a map with topographic data, with a scale of 1:10.000(BRT). Next to this map the BGT was developed, with a larger scale of 1:5000 till 1:500, for more precise planning (Kamerstukken, 2013, p.2).

The BGT does not contain personal data, according to the minister of VROM. Because it does not contain personal data in itself, it is not proposed for an advice at the CBP (Kamerstukken, 2013, p.21). The BGT and BAG are disseminated online as open data.

5.3.2 *Data protection authority*

The Dutch Data Protection Authority states that the BAG itself does not contain personal data, because it only contains addresses and building and those are not traceable to identifiable natural persons. In case the supplier assumes that the data in combination with other data will be used for identification the data is considered personal data. CBP recognizes

the importance of the goal of the legislation, the legislation is careful enough about the possible processing of personal data (CBP, 2006).

The BGT is not researched by the Dutch Data Protection Authority, because it does not contain personal data according to the legislator.

5.3.3 Jurisprudence

To search jurisprudence in the Netherlands the search engine Rechtspraak (Rechtspraak, 2015) is used (Table 5).

INSPIRE
INSPIRE
Persoonsgegeven Basisadministratie Adressen en Gebouwen (BAG)
Persoonsgegeven Basiskaart Grootschalige Topografie (BGT)
Persoonsgegeven Topografische kaart
Persoonsgegeven INSPIRE

Table 5: Search queries on Rechtspraak

Netherlands: *INSPIRE topographic data*	Personal data	Argumentation
Legislator	BGT:No	BGT does not contain personal data.
	BAG: Yes	BAG does not contain personal data, but in combination with other datasets it is possible, to become personal data.
Data protection authority	BGT: No advice available	Not available
	BAG: Yes	BAG itself does not contain personal data, but it can contain personal data when linked to other data. The legislation is careful enough about possible processing.
Jurisprudence	Not available	Not available

Table 6: Overview of the perspectives on INSPIRE topographic data in the Netherlands.

Concluding, the extent to which geographic data is considered personal data differs in the Netherlands. The Data Protection Authority judges Street View images are considered personal data if it has consequences, this places responsibility at the data processor. With the dissemination of INSPIRE datasets the responsibility is placed at the data source holder. The BAG is considered personal data, because it can be combined with other datasets. With the

BGT does not contain personal data according to the legislation and there is no advice on the dataset by the Data protection Authority. Some topographic maps are disseminated online in the Netherlands without much discussion. In the next chapter the discussions in other Member States are considered.

6 *Case Belgium*

For the Belgian case, the legal context is discussed first. The implementation of the Directive 95/46/EC and other legislation is discussed. The mobile mapping applications are examined second, third the different geographic data in the INSPIRE context and access to these INSPIRE data is considered.

6.1 *Legal context*

The privacy law of Belgium was created on 8 October 1992. It is called the Wet ter bescherming van de Persoonlijke Levenssfeer ten opzichte van de Verwerking van Persoonsgegevens (WVP). The legislation guarantees the privacy protection of Belgian citizens, because it protects the citizens against misuse of their personal data. The law fixes the rights and duties of the data subject and also the rights and duties of the data processor (Senaat, 1992). It has been amended two times. The first in 1998, to translate the Directive 95/46/EC into Belgian law and in 2003 to amend the law for the computerized society (CBPL, 2015). The law defines personal data as:

"iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon verstaan, hierna "betrokkene" genoemd; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit" (Senaat, 1992, article 1.1).

This definition translates to all information, concerning an identified, or identifiable natural person. It also defines identifiable, by direct or indirect identifiable, with use of an identification number, or one or more specific elements that characterise the physical physiological, psychological, economic, cultural or social identity. The legislation definition is more or less the same as the Directive, the Directive was a proposal at the time of the Belgian legislation. The type of media containing the information does not matter for the legislation. Photos and video images, can also be considered personal data (Senaat, 1992).

The WVP defines processing as every operation or group of operations with personal data. For example the collection, fixing, sorting, storing, update, retrieving, consulting, and disseminating or making available in any other way, shield of, erase, or delete personal data (WVP article 2, 2014).

Along with the new Law the Belgian Data Protection Authority was founded, the Commissie voor Bescherming van de Persoonlijke Levensfeer (CBPL). The CBPL is an independent body and checks if the data processing is handled carefully. An adaptation of the law was made in 1998 to implement the privacy Directive 95/46/EC. The Directive was adopted with a clarification of the personal data definition. The identifiable definition was clarified, by means to identify a person. A person is identifiable when the person can be identified with use of proportionate means (De Kamer, 1998).

6.2 *Mobile mapping*

In Belgium there are different perspectives on the processing of mobile mapping data. The legislation on mobile mapping is discussed first. Second, is the view of the Belgian Data Protection Authority and third, jurisprudence is discussed.

6.2.1 *Legislator*

In the Belgian Senate, the Street View service has been discussed. A resolution is proposed to give a legislative frame to the processing of Street View images. First the developments in Belgium and the European Union are mentioned. The legislator gives different propositions for the resolution (Senaat, 2011):

1. The Belgian Senate needs to mediate a debate between different actors and Google.
2. In sub-areas there needs to be vigilance and prevention to protect the private life and interest of third parties.
3. Citizens need to be informed about the Google Street View project and the personal data that is being processed by Google (Senaat, 2011).

The photographs of a house are not mentioned, only faces and license plates are considered personal data (Senaat, 2011).

6.2.2 *Data Protection Authority*

The Belgian Data Protection Authority distinguishes four possible applications of mobile mapping data. Firstly, the government using mobile mapping to check the current state of an area. For example to check complaints of illegal dumping in an area. Secondly, to check the state of property in a municipality. For example estimates of property, or the location of property. Thirdly, tourism using mobile mapping to explore an area or neighbourhood. Fourthly in association with the third function is navigation (CBPL Advies 05, 2010). Use of mobile mapping could lead to privacy implications. The images contain persons, houses and vehicles. When the persons, houses and vehicles are recognizable the images are considered personal data by the CBPL (CBPL Advies 05, 2010).

In the context of WVP mobile mapping applications process data, and when data about an identified or identifiable person or their belongings is processed it is considered personal data. The collected images can be considered sensitive data, for example a queue at a prison entrance, or the entrance of a General Practitioner (CBPL Advies 05, 2010).

The processing of personal data in a mobile mapping application is possible, when the data subjects give permission for the processing, this permission is impossible to obtain because of the nature of the processing of the data. Other possibilities are permission by law or show a legitimate interest that outweighs the fundamental rights and interests of the data subjects. The goals of the data processers should be accurate, justified and registered at the CBPL. This gives context to the data processing, and it is possible to judge if the mobile mapping application contains personal data. A map without cars and person needs less protection than an online system to consult the images (CBPL Advies 05, 2010).

Protective options are privacy by design, by blurring at least the faces and license plates of the data subjects. Another option is to use a camera viewpoint on another height without recognizable people on the pictures and photograph places with a lot of traffic on a quiet hour (CBPL Advies 05, 2010).

Also information about the data processor should be available online and offline. This should consist of who is responsible for the data processing, the goal of the processing, which personal data is processed, and an assessment about the influence on the privacy and

personal data protection of the data subject. Possible actions for the data subject to restore their privacy and personal data protection (CBPL Advies 05, 2010).

The CBPL has also given advice on the use of satellite images for the detection of construction violations. The spatial planning ministry requested an advice, if a justified and specific processing of personal data was lawful. At the moment of the advice, there was no pro-active detection of construction violations with use of satellite images. But a private company offered to compare different satellite images, to detect construction violations. The urban-planning inspector is currently only using openly available satellite image sources. The CBPL considers the use of satellite images as personal data with respect to the definition in the WVP. The images show parcels (all information) belonging to (concerning) a natural person, the urban planning division is able to identify the owners of the building (identified or identifiable) (CBPL Advies 26, 2006).

6.2.3 *Jurisprudence*

To search for case law different search queries were used (Table 7) on the Juridat search engine (Juridat, 2015). There is no case law available on the topic of mobile mapping data and personal data protection.

Mobile Mapping
Mobile Mapping
Persoonsgegeven Google Street View
Persoonsgegeven satellietafbeelding
Persoonsgegeven luchtfoto
Persoonsgegeven afbeelding van huis
Cyclomedia
Google Street View

Table 7: Search queries on Juridat

Belgium Mobile mapping	Personal data	Argumentation
Data source	Yes	Image from the public road is sensitive data.
Legislator	No	Digital images of a house are not mentioned. Only faces and licence plates.
Data protection authority.	Street View: Yes	Street View: An image of a house could lead to identification.
	Aerial images: Yes	Aerial images: The images show parcels (all information) belonging to (concerning) to a natural person, the urban planning division is able to identify the owners of the building (identified or identifiable).
Jurisprudence	Not available	Not available

Table 8: Overview of the perspectives on mobile mapping data in Belgium.

6.3 *INSPIRE*

On the implementation of the INSPIRE Directive in Belgian legislation are different perspectives. The perspective of the legislator is discussed first, second the Personal Data Protection Authority and third jurisprudence on the subject.

6.3.1 *Legislator*

To guide the dissemination of geographic data in Belgium the Geographic Data Infrastructure (GDI) is translated in to law in a decree. A decree is an act passed by the Flemish parliament. The Flemish GDI Decree describes the definition of geographic data as: “elektronische gegevens die direct of indirect verwijzen naar een specifieke locatie of een specifiek geografisch gebied;” (Vlaams Parlement, article 3.3, 2009). This means that geographic data is electronic data, directly or indirectly related to a specific location or a specific geographic area (Vlaams Parlement, article 3.3, 2009). The geographic data infrastructure with INSPIRE topographic maps are disseminated via the internet. It shows lots with information (Figure 5). With concern to the processing of personal data, the Flemish government states that the geographic data in most cases does not contain personal data, but some data does contain personal data. This is the case with the dissemination of data on permits via a register and when data can be linked using other databases (Vlaams Parlement, 2009).

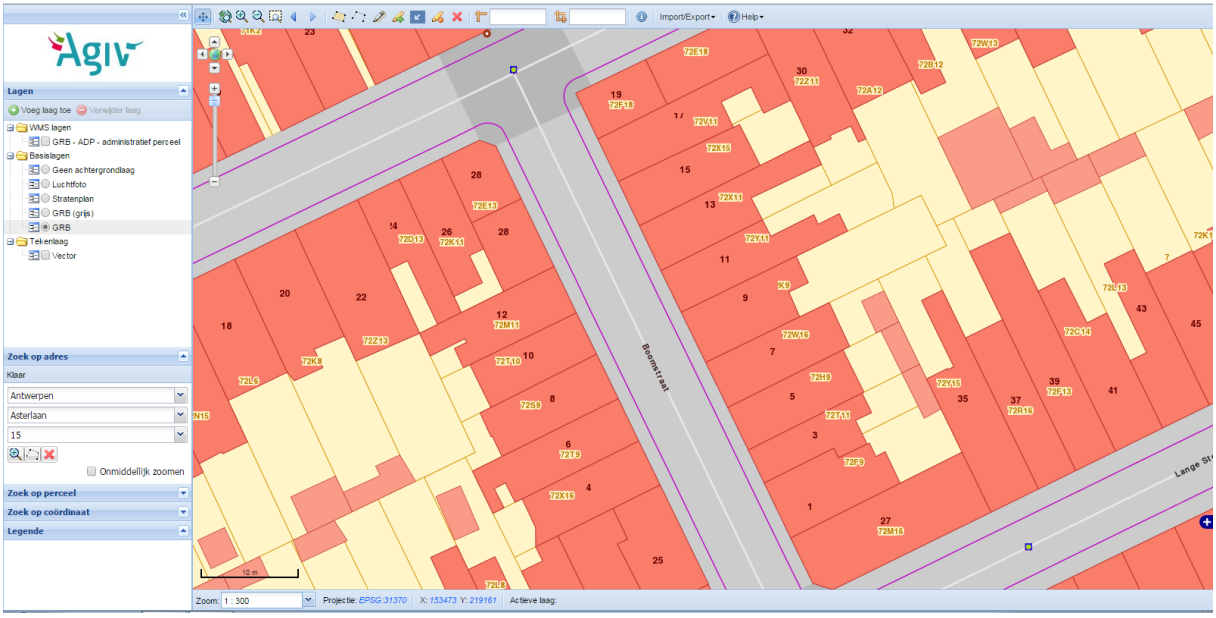

Figure 5: Lots with house numbers. Source: AGIV Viewer (2015).

6.3.2 *Data protection authority*

The CBPL has ruled that the GDI/INSPIRE Directive does not match the purpose specification principle, the principle of proportionality and data retention period. It has given a negative advice, on the design of the decree (Vlaams Parlement, 2009, p.16). It did not meet the requirements of: purpose specification, proportionality and retention period of data (CBPL Advies 32, 2008)

Geographic data is data that has a link to a specific geographic place on the earth, or a specific geographic region. When this data contains an identified or identifiable natural person this data is considered personal data. Geographic data can contain personal data, for example when a land lot is linked to an address, information about the owner can be derived from cadastral information. Via the Flemish Geographic Data Infrastructure it is possible to check granted building permits for land lots, when these land lots are recognized by position

described in the permit and the land lots are linked to an address, information about a natural person can be retrieved from a cadastral registry (CBPL Advies 32, 2008).

The CBPL advised the Belgian Ministry of Spatial planning on a geoportal with vacant lots. On this geoportal only the vacant lots will be available without the owner of the lot and cadastral registry number. The commission gives advice to totally anonymize the register, otherwise the reuse of public sector information via internet is not possible (CBPL Advies 40, 2006). Images of a scale greater than 1:50.000 are considered personal data. When photos of parcels and plans are disseminated on the internet, this will lead undoubted to the identification of the owners, according to the CBPL. The Data Protection Authority also judges that the parcels can be selected by surface size, this can lead to identification of the parcel, and it is considered personal data (CBPL Advies 40, 2006).

The geographic data added to the GDI is considered personal data, and also the access to this data via the geoportal is considered personal and falls under the WVP.

6.3.3 *Jurisprudence*

To search for case law different search queries were used on the Juridat search engine (Table 9) (Juridat, 2015). There was no case law found on the personal data and geographic information, or topographic maps.

INSPIRE
INSPIRE
Persoonsgegeven INSPIRE
Persoonsgegeven Geografische informatie
Persoonsgegeven Topografische kaart

Table 9: Search queries on Juridat

Belgium: INSPIRE topographic data	Personal data	Argumentation
Data source	Not available	Not available
Legislator	Yes, in some cases	Yes data that can be linked with other databases and data on granted permits resulting in the identification of individuals.
Data protection authority	Yes	Maps with information on land lots and vacant lots can lead to identification of a natural person. When land lots can be selected on surface size, the land lots become identifiable.
Jurisprudence	Not available	Not available

Table 10: Overview of the perspectives on INSPIRE topographic data in Belgium.

Concluding, in Belgium mobile mapping is discussed by the government and Data Protection Authority, but there is no jurisprudence available on the way geographic data can be considered personal data. The reasons for considering geographic data as personal data lie in the fact that it can possibly lead to identification of a natural person. If the reasons and cases differ in Germany is discussed in the next chapter.

7 *Germany*

For the German case, firstly the legal context is discussed. The implementation of the Directive 95/46/EC and other legislation is discussed. Secondly the mobile mapping applications are examined and thirdly the different geographic data in the INSPIRE context and access to these INSPIRE data is considered.

7.1 *Legal context*

The Bundesdatenschutzgesetz (BDSG) is the legislation that protects personal data in Germany, personal data is defined in the law by 1991, and there has been some changes in the legislation due to the Directive 95/46/EC. Personal data is defined as: “Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)” (BMJV, 2003, paragraph 3.1).

This means that personal data are particulars about personal or factual relationships of an identified or identifiable natural person (person concerned). This definition stems from the European Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. The amendments of the BDSG to comply with Directive 95/46/EC are concerning the subjects of media, press and video surveillance (BT-Drs, 1997).

In 2006 the Federal Constitutional Court of Germany defined the right to be let alone in your own home and have a right to privacy in your own home without being disturbed as: “In seinen Wohnräumen hat er das Recht, in Ruhe gelassen zu werden. Art. 13 Abs. 1 GG gewährt ein Abwehrrecht zum Schutz der räumlichen Privatsphäre und soll Störungen vom privaten Leben fernhalten” (BVerfG, 2006).

This leads to: “Die bedingt auch, dass kein beliebiger, weltweiter Bezug zwischen einem Betroffenen und seiner Wohnsituation hergestellt werden darf bzw. hier die Betroffenenrechte überwiegen[...]Zumindest bei Einfamilien- oder kleineren Mehrfamilienhäusern oder bei Gehöften wird man von einer Bestimmbarkeit einzelner Personen, bei denen ihr schutzwürdiges Interesse überwiegt, ausgehen müssen” (Bergmann, Möhrle & Herb, 2009).

This means that no worldwide relation between a data subject and his living situation can be made and outweigh the data subjects right. For at least single family and small flat complexes and little rural towns the possible identification of persons is an interest worth of protection that must outweigh other interests. The right to be let alone is also applicable to the residential area (Van der Sloot, 2011, p.177).

The access to geographic data is granted by law in Germany. The Geodatenzugangsgesetz. The legislation defines geographic data as: “Geodaten sind alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet” (BMJV, 2008, article 2, par.3).

A note to the legal and parliament context in Germany is the different set-up. Because all the different States (*Ländern*) in Germany have different laws and perspectives, there is some difference. In the research the used perspective is that of the federal government when it comes to jurisprudence and legislation, and some more local perspectives, to give some different arguments and local insight perspective.

7.2 *Mobile mapping*

In the part about Mobile mapping different perspectives on mobile mapping are described. The legislation for processing of images is discussed, secondly the data protection authority's opinion is displayed and thirdly, jurisprudence about a case with satellite images of homes is reviewed.

From the interview with the data source holder the conclusion can be drawn that in Germany there are more restrictions for the data source holder. The interpretation of personal data is much stricter. The use of panorama images are restricted and there must be anonymization.

7.2.1 *Legislator*

Because of the development in the use of internet the German legislator proposed amendments to the 'Bundesdatenschutzgesetz'. Internet can also be used to gain personal information about a person. A possible way is via the use of Google Street View. It was legally uncertain if photographs and films of entire streets are permitted. The draft law proposed a specification of the concept "allgemeinen Zugänglichkeit" (general accessibility) of data (BR-Drs, 2010, p.2). The data processor needs to blur the faces of persons and license plates of cars. It gives people and homeowners the right to object to dissemination of the image of their home without restrictions. People are able to request that images of their body and face to be made totally unrecognizable. The data processor needs to publicly announce the project and be registered at the data protection authority. It is punishable by a fine if the service does not meet the requirements (BR-Drs, 2010, p.2). The legislator considers Google Street View images of a home personal data.

7.2.2 *Data Protection Authority*

The Data Protection Authority of Düsseldorf judged that is was not possible to legally prohibit Google Street View, because Google blurred license plates, faces of people and house numbers (Van der Sloot, 2011, p.177). Based on jurisprudence of the City Server case (mentioned in 7.2.3.), the Data Protection Authority states that digital images of a home are not in conflict with the BDSG. When the images of a home are in the hands of a municipality, the images are personal data, because with use of the municipal databases it is possible to trace the owner of the building (Datenschutz Baden-Württemberg, 1999, p.138). The Datenschutz Schleswig-Holstein states that Google Street View is not in accordance to the BDSG. It shows the state and type of the building, exterior, furnishing and garden and can possibly lead to economic value assessment and theft. The Datenschutzzentrum also claims that the Data Protection Authorities in the other German States agree with this view (Datenschutzzentrum, 2008).

The Data Protection Authority adds, that with the use of internet the possibilities for identification of a natural person increased. With use of georeferenced images and images with house numbers or street names, images of homes are considered personal data as defined in the Bundesdatenschutzgesetz (Karg, 2008, p. 14). For satellite images, the general rule is by 40cm per pixel the images are considered personal data, because with a higher resolution it is possible to link a person and an object. It refers to the judgement of the constitutional court in 2006 (BVerfG, 2006a).

7.2.3 *Jurisprudence*

In 1999 a plaintiff started a case against a defendant that wanted to build a digital image database, including pictures of plaintiff's house. To create this database, the defendant had different cars taking pictures and these pictures were linked to coordinates (longitude, latitude and altitude). The defendant wants to sell the database under the name 'City Server'. The plaintiff claimed that the defendant in this way had photographed his private home and linked that picture to address data (zip code, street name and city). The plaintiff thinks this is

an infringement of his constitutionally protected ownerships right and personal privacy right and the defendant should refrain from publishing the recorded pictures. The photos from the public space cannot be prohibited, but it could lead to use by commercial enterprises, and even burglaries (LG Waldshut-Tiengen, 1999).

The Chamber does not see the right for the plaintiff to restrain the defendant from publishing the pictures. Because, when the database was used to find the dweller or homeowner of a house with a single address, this was not possible (LG Waldshut-Tiengen, 1999). The case against City Server is also been brought to the Court in Karlsruhe. The Chamber stated that when automatic linking to other data sources is not possible there is no invasion of the right to privacy and personal data (VG Karlsruhe, 2000).

In another case a homeowner feared that the private areas of her front yard and her family could be identified by use of Google Street View. She tried to sue Google for the possible invasion of privacy and property. The Court of Appeal in Berlin stated that Google Street View could photograph a home as long as it did not photograph behind the fence of the house. It is prohibited to photograph a fenced off home. Photographs of housing rows and houses without fences are not judicial relevant (KG Berlin, 2010).

In yet another case, in 2006, the owner of a news agency wanted to publish aerial photos of homes of famous Germans living in Mallorca. With the use of a helicopter the defendant took pictures and accompanies these pictures with the location of the homes, in the form of directions, and the names of the home owners (BVerfG, 2006a). The court claims that the publication of the aerial images was an infringement of the right to privacy, because the homes and the land owned by the plaintiff are protected by the Data Protection Law. The court judges that the right to privacy not only ranges to people but also to pictures of spatial objects. The spatial object are likely to reflect the personality of the owner, even more have a misjudged dangerous potential that the person concerned against his will should not be exposed to. Aerial images give a sight on property that is not visible from the street (BVerfG, 2006).

The applicant's right to freedom of press is outweighed by the right to privacy (BVerfG, 2006a). It is not about the interest of a large public to publish the images and information, moreover it is used to satisfy the curiosity towards celebrities personal lives of a large group of people. The images are seen as an invasion of the right to privacy and the right to a personality, because the pictures show the part of the personality of a person, and invades his right to a private life (BVerfG, 2006a).

This jurisprudence has led to the solution of considering digital imagery of a home with a minimum resolution of 40cm per pixel is considered personal data (Karg, 2008).

Germany: Mobile Mapping	Personal data	Argumentation
Data source	Yes	Image from the public road is sensitive data.
Legislator	Yes	The data subject has the right to blur face, body and house. Otherwise considered personal data.
Data Protection Authority	360 degrees images: Yes	Pictures of a home are considered personal data. It can be used for economic value assessment, and possibly theft.
	Aerial images: Yes	Aerial images with a higher resolution than 40cm per pixel satellite images are considered personal data, based on the jurisprudence.
Jurisprudence	Digital images of a home: no	Images of homes are not personal data, because it is not possible to lead to identification. The view from the street does not violate the privacy rights, as long as the house is not fenced off.
	Satellite images: yes	Aerial images of a home are an invasion of the right to privacy, because it shows a characteristic of a person and gives a view that is not possible from the street. Satellite images with a resolution higher than 40 cm are considered personal data.

Table 11: *Overview of the perspectives on mobile mapping data in Germany*

7.3 *INSPIRE*

7.3.1 *Legislation*

In Germany the discussion on restrictions to access of INSPIRE data is based on Article 13 in the INSPIRE Directive (European Union, 2007, Article 13). In the article is stated that access should be granted, but also in compliance with the Directive 95/46/EC. The INSPIRE Directive shows that there are some options open to Member States to control the access to INSPIRE data. The protection of personal data is mainly the responsibility of the data source holders. But with respect to the actual functionality and embodiment of the spatial service the operators can also have the responsibility for the protection of personal data. In this way not only data processors can add to it. The start of the implementation of the INSPIRE Directive leads to a possibility to normalize the unsatisfactory shift between collection, processing and use of geographic data and personal data protection. The INSPIRE Directive gives legislative scope for the Member States to protect personal data under the access and implementation of the Directive 95/46/EC. The Member States have the responsibility to protect the processing of personal data with the creation of a national Spatial Data Infrastructure (Karg, 2008).

The decision on access to geographic information depends from case to case. There must be an assessment of the interest of the stakeholders and the interest of the access and freedom of information. It affects the potential of the INSPIRE data. The legal framework must be known, before the collection, processing and use of geographical data is beneficial.

A solution would be if the spatial access law grants the public interest an overriding order. This is a very common problem with the access to geographical data, the personal data protection is a hurdle to be taken. In these cases there are strict access rules to geographic data which contain personal data. This does not answer the question if personal data is present, the gain in privacy protection is realized by the public body assessment. The assessment places the responsibility of personal data protection at the authority providing the data.

The advice is to categorize based on the risk potential, the categories of the geographic data in the annex of INSPIRE, in that way the access can be regulated. For every category the freedom of information and personal data protection are assessed.

In Germany there is also discussion about the national SDI and the access to the SDI. Germany has a right to access of geographic data. The ‘Geodatenzugangsgesetz’, it is different from the INSPIRE Directive because it contains access to all geographic data, while this is not the case in the INSPIRE Directive. Some parties argue that the right to personality, the right to privacy is neglected. It is possible that personal data is processed. And this has consequences for people. For example when certain households don’t get access to credit anymore (Bundestag 16, 2008).

The access to geographic information is important under the Freedom of Information Act But, the possible freedom to information and the invasion of personal data protection should be weighed when geographic data is accessed. Geographic data is in the first place information about object, but the objects lead to information about the identity, characteristics or behaviour of a person. There are no clear criteria that mark a distinction between personal data and data about objects. The INSPIRE directive makes access to geographic data not only a responsibility of the administration, but also of the legislator (Bundestag 16, 2008).

The design for the law now has only one part about the difference between personal data and geographic data, and is therefore inadequate. In the debate the general rule based on research by the Data Protection Authority that geographic data with a scale of 1:10,000 does

not contain personal data, because with a more detailed scale it is possible to distinguish information about the state of the ground and use of the land (Bundestag 16, 2008).

7.3.2 *Data Protection Authority*

Geographic information is personal data when it tells something about a person. For example information about the location of a person. Geographic data is also personal data when it is possible to link a natural person to geographic data. The data processor needs to be able to link the natural person and geographic data. Geographic data is mainly data about an object and not about a person. The concept of a person, is a judicial concept, and this creates a stretch of the definition of personal data. Because with the increased use of internet, more and more data is interconnected. The data processor defines in which way the content of the data refers to the natural person. The content refers to a natural person, a goal that refers to a natural person and contains references to a natural person is considered personal data. The more intense the data intervenes on a person's life, and the more it decides on the relation with a person's environment the more it is considered personal data (Karg, 2008, pp.53-54). A traffic light model is proposed that is in line with the used systematics (Karg, 2008, p.55).

Green: Unproblematic data for the data protection, firstly factual data with no reference to a person and secondly publicly available data with no influence or neglect able influence on a person's privacy (Karg, 2008, p.55).

Yellow: This category, contains data with a personal link. The data has an influence on the privacy of the concerned persons. The information about a person differs from datum to datum. A risk potential analysis is only possible when processing of the data has a fixed objective (Karg, 2008, p.55).

Red: Sensitive data, as described in the Directive 95/46/EC are mainly in this category. Data has an influence on the life of a person. With the collection, storing and processing of this data there should be given explicit permission to process these data of the data subject, as mentioned in BDSG (art. 4 par.3) (Karg, 2008, p.55).

When the INSPIRE Directive is implemented in Germany, Datenschutz states that the legislation should protect the collection, processing and use of geographic data when the INSPIRE Directive is implemented.

INSPIRE polygon land use maps are not considered personal data, when the scale is smaller than 1:10.000. When the scale is more detailed it can be considered personal data because, information about the use of land shows the state of the user and the use. The presentation should show that the current of owner of the land is responsible for the current state of the ground (Karg, 2008, p.60).

The 1:10.000 rule is also used with topographic maps. Only maps with a scale of 1:5.000 or 1:2.500 show the reality without generalization with location, size and use of the property. These maps contain personal data (Karg, 2008, p. 68).

7.3.3 *Jurisprudence*

The queries used to search for case law on beck-online (Beck-Online, 2015), but no results were found (Table 12).

INSPIRE
INSPIRE
INSPIRE Personenbezogene daten
Topographische Karte personenbezogene daten
Personenbezogene daten AND Luftbild
Personenbezogene Daten AND Häuserbild
Cyclomedia
Google Street View

Table 12: Search queries on Beck-Online

Germany: INSPIRE topographic data	Personal data	Argumentation
Legislator	Yes for scale larger than 10.000	Based on advice of the data protection authority maps with a scale larger than 10.000 are considered personal data, because with a more detailed scale it is possible to distinguish information about the state of the ground and use of the land There needs to be a weight of the different interests.
Data protection authority	Yes for scale larger than 10.000	For topographic maps a scale larger than 10.000 can lead to identification of use, location and size of the property.
Jurisprudence	Not available	Not available

Table 13: Overview of the perspectives on INSPIRE topographic data in Germany

8 *United Kingdom*

8.1 *Legal context*

In the United Kingdom the Data Act from 1998 defines personal data. Personal data is defined as: ""personal data" means data which relate to a living individual who can be identified—

(a) From those data, or

(b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;" (Data protection Act, 1998, Part. 1.1).

In the United Kingdom the responsible data protection authority is the Information Commissioner Office (ICO). The ICO has given a recommendation to assess the privacy impact (PIA) of the Price Property Index (PPI). The assessment consist of an explanation which data is collected, approach, analysis, controls and mitigation to minimize the impact on privacy. The PIA has been conducted to research if the PPI is personal data or not (Land Registry, 2012).

PPI is information about the single residential sales at full value market at England and Wales. These sales are stored at the Land Registry. The data consists of full addresses, the price paid, date of transfer, property type, whether the property is new build or not and whether the property is freehold or leasehold (Land Registry, 2012).
To check if the PPI is property related, the analysis was re-examined. Since the first of April 2000 the PPI is available from the register of deed. The land registration act and rules need to have the register publicly available. When this is not publicly available, the law is broken.

The impact assessment concluded that the data was related to property and not to a person, and is not considered personal data. (Land Registry, 2012).

The re-examination in 2013 confirms that the PPI is not considered biographical in nature, this makes it information on property and not on the person selling or buying property. Following this reasoning, PPI is considered property information and not personal data (Land Registry, 2013).

Another part of the PPI privacy impact assessment is the privacy of the Historic Price Paid Data (HPPD). It contains the price paid for every single residential property sold between 1995 and 31 January 2012 in England and Wales. The price paid data was not open for public inspection before 2000, but this had minimal impact, because the public was able to request information under the Land Registration statutory regime. According to the ICO the HPPD was also property related and not considered personal data, because it doesn't identify the owners, nor gives information about the owners nor is it biographical (Land Registry, 2013).

8.2 *Mobile mapping*

8.2.1 *Legislator*

During the debates of the United Kingdom's parliament, there is no mention of mobile mapping, use of Google Street View, other mobile mapping applications, or aerial photographs.

8.2.2 *Data Protection Authority*

In the first weeks of the introduction of Street View on the UK market there were some complaints about the privacy of the Britons. Privacy watchdog Privacy International (PI) complained about images on Street View to the ICO. PI argued that Street View needed the consent of the communities before the images were taken. The inhabitants of Broughton barricaded the streets to prevent the Google Street View car from entering. The Street View car could facilitate the actions of burglars (BBC, 2009).

The ICO stated that in a response to the PI complaint that: "It is important to highlight that putting images of people on Google Street View is very unlikely to formally breach the Data Protection Act," (ICO, 2009, p.1). The ICO received complaints, and concluded that it was disproportionate to delete a service based on relatively small number of complaints. When Google blurred the faces of people and license plates the privacy of the UK citizens was guaranteed (ICO, 2009, p.1). In the editors notes of the press release the ICO states that "Data protection is about people's personal information; so an image of a house held on Street View is not a data protection matter" (ICO, 2009, p.2).

If the images are considered personal data, Rand Europe has given the ICO advice on the Directive 95/46/EC in a report. Rand Europe gives the explanation:

"Data such as those in Google Street View may come under the Directive if they include images of individuals" (Robinson et al., 2009, p.27).

It is stated that the EU Directive 95/46/EC misses focus on what personal data has a real privacy impact. And the question is raised if the impact a relevant criterion is for the protection of personal data (Robinson et al., 2009).

8.2.3 *Jurisprudence*

Westlaw UK (Westlaw UK, 2015) is used to search jurisprudence on mobile mapping cases in the United Kingdom (Table 14). No case law on mobile mapping and personal data protection was found.

Mobile Mapping
Mobile Mapping
Personal data Google Street View
Personal data satellite images
Personal data digital images of homes
Google Street View
Digital images of a home
Satellite images of a home

Table 14: Search queries on Westlaw UK

United Kingdom Mobile mapping	Personal data	Argumentation
Legislator	Not mentioned	
Data protection authority	No	Data protection is about protecting someone's personal information. An image of a house is not a data protection matter. So, an image of a house is not personal data
Jurisprudence	Not available	

Table 15: *Overview of the perspectives on mobile mapping data in the United Kingdom*

8.3 *INSPIRE*

8.3.1 *Legislator*

The INSPIRE Directive led to some debate in the United Kingdom on the role of the Ordnance Survey (OS). The National Mapping Agency argued that the INSPIRE Directive led to a loss of income, due to opening up of data (The Guardian, 2006).

The INSPIRE Legislation defines spatial information as: “spatial data” means any data with a direct or indirect reference to a specific location or geographical area;” (The INSPIRE Regulations, 2009, article 2.1.b). In the article about access to data, the public access to personal data by a public authority or a third party is prohibited. Personal data is defined as in the Data Protection Act of 1998 (The INSPIRE Regulations, 2009 article 9.2).

8.3.2 *Data Protection Authority*

The ICO published a document on how to deal with the INSPIRE data and how to make a complaint. It does not mention the privacy implications of disseminating spatial data on the internet (ICO, 2009a). The ICO stated in a request on information that it has not received any complaints about INSPIRE (ICO, 2014).

8.3.3 *Jurisprudence*

Westlaw UK (Westlaw UK, 2015) was used to search jurisprudence on mobile mapping cases in the United Kingdom(Table 16). No case law on personal data protection and topographic maps was found.

INSPIRE
INSPIRE
Personal data geographic information
Personal data INSPIRE
Personal data topographic data
Personal data building
Topographic maps

Table 16: Search queries on Westlaw UK

United Kingdom INSPIRE topographic data	Personal data	Argumentation
Legislator	Not mentioned	
Data protection authority	No	No complaints on the protection of personal data by Britons
Jurisprudence	Not mentioned	

Table 17: Overview of the perspectives on mobile mapping data in the United Kingdom

9 *Analysis*

The research question and sub-question are answered in this part.

What are personal data, open data and geographic data?

The concept of personal data is defined based on Convention 108 and Directive 95/46/EC as information relating to an identified or identifiable natural person. In Directive 95/46/EC the most comprehensive definition is used:

"'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (European Union, 1995, article 2a).

This definition gives room to a broad interpretation. In European legislation every datum that can lead to identification is considered personal data, even when data is not used for identification. The used definition of personal data in the Draft General Data Protection Regulation is the same definition as in Directive 95/46/EC.

Open data is defined as data that can be used freely, reused and distributed by anyone, without reuse restrictions (Open Definition, 2014). Directive 2013/37/EU creates an obligation for EU Member States to publish open data. "Directive 2003/98/EC should therefore be amended to lay down a clear obligation for Member States to make all documents reusable unless access is restricted or excluded under national rules on access to documents and subject to the other exceptions laid down in this Directive" (European Union, 2013, p.2).

Geographic data is defined as data with a link to a place on earth. The link can be factual or administrative. Another division between types of geographic data is in three categories: topographic data, cadastral data and aerial photography.

To what extent do the interpretations of the personal data definition of EU Directive 95/46/EC differ between the Article 29 Working Party, the European Court of Justice, European Court of Human Rights, and the Draft General Data Protection Regulation?

The interpretations of personal data between the Article 29 Working Group and ECJ differ. The Article 29 Working Group gives a broad definition of personal data. It divides the definition in three parts. The first part, any information leads to a wide definition of personal data, because it does not matter if the information is true, or false, and what medium carries the information (Article 29 Working Party, 2007). Relating to gives information about the relations and the importance of the relations. The third part, is the identified or identifiable person. This part describes 'identifiability' (Article 29 Working Party, 2007).

The ECJ considers data containing personal data not necessarily as personal data. An analysis based on personal data, is not considered personal data for example. The ECHR defines personal data as defined in article 8 in the Convention on Human Rights.

The Draft General Data Protection Regulation continues to use the definition of the Directive, while the broad definition of Directive 95/46/EC is one of the main problems in the processing of personal data. It creates a barrier because it leaves room for interpretation by the different EU Member States, and by the different organisations in Europe and the Member States. For example the ECHR and ECJ interpret the personal data definition in different ways. The ECJ has a narrower definition than the definition used in most Member

States. The definition in Directive 95/46/EC leads to a patchwork of privacy legislation in the different EU Member States (Korff, 2002 and 2010).

To what extent does the implementation of the Personal Data Protection Directive differ between and within EU Member States (perspective of data holder, legislator, data protection authority and jurisprudence)?

The implementation of the definition used in the Personal Data Protection Directive is sometimes based on previous legislation, and often the implementation differs between the perspectives in an EU Member State. In the Netherlands, the Directive is implemented in legislation, and the definition of personal data is based on the previously given definition. In Belgium the Directive is also implemented, with respect to the previous legislation (Korff, 2002).

Germany has a federal personal data protection law: The Bundesdatenschutzgesetz (BDSG). This legislation resulted from the constitutional principle of 'a right to a personality.' From this right the German Federal Court has derived the informational self-determination right. This is a right to decide on which and what parts of the private life are revealed (Korff, 2002). The informational self-determination right can be linked to the previous discussed informational privacy. When personal data is processed, this is often linked to the information self-determination right in Germany. In German jurisprudence there are often references to the different constitutional provisions.

In the United Kingdom, the Data Protection Act (DPA) of 1998 includes a personal data definition that does not match the definition used in Directive 95/46/EC. The Act refers to "data relating to a living individual who can be identified from those data, or ... from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller" (Data Protection Act, 1998, Part. 1.1), rather than the definition used in the Directive. The ICO states that the DPA repeats Directive 95/46/EC, but the order of the definition actually is reversed. It first considers if the information is data, by stating the way the information is processed (by automatic means or non-automatic processing), and second and last by checking if the data leads to identifiability of a person, and then it is considered personal data (ICO, 2012).

Where are mobile mapping data, and topographical maps considered personal data and why?

First, mobile mapping data is discussed. In the Netherlands there is no concern from the Data Protection Authority about the use of images of a property. Only if used with consequences for a natural person, for example taxation it is considered personal data. This is a result of research in 2001 by the Dutch DPA on the use of panoramic 360 degrees images of public roads in a database. It is remarkable to see that there are no further actions taken in case of Google Street View, because these images are free to use without any data protection restrictions. It is considered personal data according to CBP, because it can be used to identify and it can have consequences for the data subject, and it should be processed according to the WBP.

In Belgium Google Street View is also discussed in the Senate, but images of a home were not discussed. The CBPL considers photos of a belonging personal data, according to this definition pictures of a home are considered personal data. CBPL wants a precisely described goal for the processing of data, and also different levels of data protection for different goals and datasets. The Belgian Data Protection Authority makes a distinction between maps without persons or cars or maps with living natural persons and objects.

In Germany the Datenschutz judges that photos of a home cannot be prevented, and with use of internet different datasets can be linked together and this can lead to identification of an inhabitant. The Data Protection Authority (*Datenschutz)* Schlewig Holstein is opposed to Street View in the State, because it invades the right to privacy of the inhabitants. Google Street View is disseminated via internet and is able to show the state of the buildings. The Germany courts state that when automatic linking is not possible there is no threat of the right to privacy and personal data. The courts state that when it is possible to automatically link geographic data to other data sources, the geographic data becomes personal data and is in interference with the right to privacy.

Google Street View is in interference with the right to privacy, when it disseminates photos of a fenced off house. A fenced house gives Street View no sight on the house, only photos of objects behind a fence are considered personal data. The German Federal Court judged that a spatial object could reflect someone's personality.

In the United Kingdom the ICO states that Google Street View is not considered personal data, because it is not someone's personal information.

Three out of four case studies consider the Google Street View images personal data and aerial images are also personal data. It is interesting to see the contrast between the Member States, the ICO is the only Data Protection Authority that despite complaints of citizens does not see Google Street View as personal data. The ICO states that a picture of a home is not personal information. With this statement the ICO claims that it is not possible to use the images from Google Street View to identify a person. Between the EU Member States the reasons behind the panorama pictures of streets differ. The CBP in the Netherlands has a focus on the context of the collection, if the goal is to identify a person, or it has societal consequences this is considered personal data. In Belgium the possible identification is the most important reason and in Germany the possible consequences for an inhabitant are also the reason for considering the image of a home as personal data.

In the United Kingdom these reasons do not count. The ICO uses information on a house as an example to explain the definition of personal data. Data relating to an individual is for example data about the house of an individual. The data about the house is not personal data when it is about the house and not linked to a person. The context of the processing and the goal of the processing is of importance according to the ICO. This use of the personal data definition is in line with the more narrow definition by the ECJ, for example when an analysis contains personal data the analysis is not considered personal data, but only the personal data itself. The ICO states that when data is about an individual for example the address of the individual or when the data used in decisions or deliberations affecting the individual, for example data on the electricity bill of an individual it is considered personal data (ICO, 2012).

In the EU Member States, between different institutions are also differences. In the Netherlands and Germany the judges claimed that Google Street View is not an invasion of the right to privacy. The Dutch court judged that Street View that the data on Google Street View did not refer to an address and did not contain personal data. While the Dutch and German Data Protection Authorities state that Google Street View contains personal data. Also the difference between Street View and Google Earth is remarkable, because the Dutch court ruled that the use of Google Earth with the tracking of crimes was an invasion of the right to privacy.

Netherlands	Personal Data	Argumentation
Data Source	Yes	Pictures of the public road are considered sensitive privacy data.
Legislator	No	The processing of Google Street View images are not considered personal data when a person's face and license plate of a car is blurred.
Data Protection Authority	Yes	If the images, are used in the context of identifying, or the images have societal consequences for a person the images are considered personal data
Jurisprudence 360 degrees images	No	Images of a home are blurred and the images lack a link between the inhabitant and the property
Jurisprudence Aerial Images	Yes	Personal data, because it shows the backyard of the defendant, but only a limited infringement of the right of privacy
Belgium		
Data Source	Yes	Pictures of the public road are considered sensitive privacy data
Legislator	No	Digital images of a house are not mentioned. Only faces and licence plates.
Data Protection Authority	360 degrees images: Yes	An image of a house could lead to identification.
	Aerial Images: Yes	The images show parcels (all information) belonging to (concerning) to a natural person, the urban planning division is able to identify the owners of the building (identified or identifiable).

Jurisprudence	Not available	Not available
Germany		
Data Source	Yes	Pictures of the public road are considered sensitive privacy data
Legislator	No	The data subject has the right to blur face, body and house. Otherwise considered personal data.
Data Protection Authority	360 degrees images: Yes	Pictures of a home are considered personal data. It can be used for economic value assessment, and possibly theft.
	Aerial images: Yes	Aerial images with a higher resolution than 40cm per pixel satellite images are considered personal data, based on the jurisprudence.
Jurisprudence	360 degrees images: No	Images of homes are not personal data, because it is not possible to lead to identification. The view from the street does not violate the privacy rights, as long as the house is not fenced off
	Aerial images: Yes	Aerial images of a home are an invasion of the right to privacy, because it shows a characteristic of a person and gives a view that is not possible from the street. Satellite images with a resolution higher than 40 cm are considered personal data.
United Kingdom		
Data Source	Yes	Pictures of the public road are considered sensitive privacy data
Legislator	Not mentioned	
Data Protection Authority	No	Data protection is about protecting someone's personal

		information. An image of a house is not a data protection matter
Jurisprudence	Not Available	Not available

Table 18: Overview of the perspectives on mobile mapping data in EU Member States

For the implementation of the INSPIRE Directive the same perspectives are used. Between the Member States the way geographic data is considered personal data differs. In the Netherlands the Data Protection Authority judged that use of some INSPIRE themes led to implications for the personal data protection, because it was possible to link data to other datasets and lead to identification of a natural person. The Dutch Data Protection Authority agreed with the Dutch legislation on the absence of personal data in topographic maps. The Register of Addresses and Building contained personal data when linked to other datasets. This confirms the importance of the context of the processing.

The Belgian Data Protection Authority advised the Flemish government about the implementation of the INSIRE Directive and the opening up of INSPIRE data, the CBPL has given negative advice on both, but the Flemish government has still published the data. The Flemish government added data about identified or identifiable natural persons to the exemptions of the legislation.

In Germany the Data protection Authority advised the use of a scale of 1:10.000, because with a greater scale it was possible to trace the use of the land, and state and possible identification. The ICO claimed that there were no complaints on the processing of personal data.

The German and Belgian authorities differ on the use of a privacy safe scale. The Netherlands decided that topographic information did not contain personal data. This is an interesting judgement, because with linking it could lead to identification and the topographic maps that are freely disseminated show information about the use and state of land. The differences inside and between the Member States focus on the identifiable part of the personal data definition. The Member States differ on the opinion in what way topographic maps tell something about a person and should be considered personal data.

It is interesting to see that in the European Union there is no resistance against the Directives that obliges governments to open up data, when the national Data Protection Authorities and the European Data Protection Supervisor warn for the invasion of personal data protection rights (EDPS, 2012).

Netherlands	Personal Data	Argumentation
Data Source	Not available	Not available
Legislator	BGT: No	BGT: does not contain personal data.
	BAG: Yes	BAG: BAG does not contain personal data, but in combination with other datasets it is possible, to become personal data.
Data Protection Authority	BGT: No advice available	Not available.
	BAG: Yes	BAG itself does not contain personal data, but it can contain personal data when linked to other data. The legislation is careful enough about possible processing.
Jurisprudence	Not available	Not available
Belgium		
Data Source	Not available	Not available
Legislator	Yes, in some cases	Yes data that can be linked with other databases and data on granted permits.
Data Protection Authority	Yes	Maps with information on land lots and vacant lots can lead to identification of a natural person. When land lots can be selected on surface size, the land lots become identifiable.
Jurisprudence	Not available	Not available
Germany		
Data Source	Not available	Not available
Legislator	Yes for scale larger than 10.000	Based on advice of the Data Protection Authority maps with a scale larger than 1:10.000 are considered personal data. There needs to be and weigh of the different interests.

Data Protection Authority	Yes for scale larger than 10.000	For topographic maps a scale of greater than 10.000 can lead to identification of use, location and size of the property
Jurisprudence	Not available	Not available
United Kingdom		
Data Source	Not available	Not available
Legislator	No	
Data Protection Authority	No	No complaints on the protection of personal data by Britons
Jurisprudence	Not Available	Not available

Table 19: Overview of the perspectives on INSPIRE data in EU Member States

9.1 *Harmonising the patchwork of data protection*

To unify this patchwork of data protection legislation there are different options. First it is important to notice that the context of the data processing is the most important factor to decide on if the data is considered personal data. It is mentioned in most of the cases, but it does not lead to a harmonized consideration on personal data, because the Data Protection Authorities differ too much on the definition of personal data. The ICO considers Street View not personal data, while they use the same definitions as context as the other Data Protection Authorities. And the Netherlands does not consider the BGT (Topographic maps) as personal data, where Belgium is the strictest Member State and considers topographic maps with a scale of 1:50.000 personal data, and Germany maps with a scale of 1:10.000.

The definition of personal data has sparked some discussion in the literature, it is mentioned that the definition of personal data is stressed or is called a broad definition. Schwartz and Solove define personal data as Personally Identifiable Information (PII) and created a model with what they call PII 2.0, the model makes a distinction between identified, identifiable and non-identifiable information (Schwartz and Solove, 2011).

Data is placed on a continuum on one end there is no risk of identification and on the other end identified natural persons. The three features of the model are (Schwartz and Solove, 2011).

1. Identified: An identified natural person is a person whose identity is determined. This data has a high risk level.
2. Identifiable: There is an immediate chance on identification of a natural person. This data has a moderate to low risk level.
3. Non-identifiable: Data with only a remote risk of identification. With means reasonable likely to be used for identification this data cannot be related to a natural person.

Sometimes identifiable data should be considered identified data, this is the case when the data processor is able to link data and with this link identify a natural person. Schwartz and Solove (2011) advice to develop an assessment for this category of data. This assessment should take the lifetime of the stored information and development of relevant technology in consideration. The assessment is also mentioned by the EDPS, the rules for the assessment should be defined in the Draft Regulation (EDPS, 2012).

A possible solution is the previous proposed traffic light model by the German Data Protection Authority. The colours will be:

Red: Sensitive data as defined in Directive 95/46/EC, article 8.

“Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life” (Directive, 95/46/EC, article 8). This data is prohibited from dissemination on the internet, or only with explicit consent of the data subject.

Orange: Personal data. This is a definition partly based on Directive 95/46/EC. For dissemination on the internet, the data subject needs to give consent. Examples are your name, or address.

“'personal data ‘shall mean any information relating to an identified natural person ('data subject'); an identifiable person is one who can be identified, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (European Union, 1995, article 2a). This definition focuses on an identified person, and the data needs to identify the person directly. For example, an address, or social security number.

Yellow: Data that can possibly lead to identification (IP-addresses, buildings). This data leads to the identifiable person, and indirect identifiable. For this type of data it is important to create a risk assessment. For example to consider the context of the processing, and with that context in mind give a go to the dissemination or prohibit access to the data. The rules for the risk assessment should be defined in the Regulation. An important factor for this is the goal of the processing of open data, some rules on reuse of open data should be considered when the data is disseminated.

Green: No personal data, or anonymized data.

The traffic light model can be a solution, because it gives clear indications for risk assessment and it uses the context of the processing. It does not have the strict boundaries of the current assessment of personal data. This model is more focused on the context of processing instead of a strict divide between personal data or non-personal data.

Concluding to create a more harmonised data protection legislation it is important to create a clear and well defined risk assessment, which focuses on the context of the processing and the type of data. The traffic light model is in this perspective a step in the right direction. And could be used to create a clearer view on the types of personal data.

10 *Conclusion*

This research addressed the following research question:

To what extent should geographic data in the EU be considered personal data and how may the different interpretations of EU Member States be harmonised?

Concluding, to construct personal data protection in the European Union it is the most important to tackle the problems with the differences in definition on what is considered personal data. Geographic data is considered personal data in the Netherlands, Germany and Belgium, and it is not considered personal data in the United Kingdom. The perspectives of different stakeholders in the Member States also differ, leading to new difficulties in harmonization. With use of the personal data definition in the current Directive 95/46/EC and the Draft Regulation, geographic data should be considered personal data in the EU context, because it is data that could lead to identification of a person.

The analysis shows that opening up of geographic data and the interpretation of personal data protection legislation is still a blind spot for legislators in Europe. 360 degree images, and aerial images are considered personal data by the national Data Protection Authorities in the Netherlands, Germany and Belgium, because these images could lead to identification of individuals. This possible violation of the personal data protection legislation is not discussed in the Parliaments of the EU Member States. The Data Protection Authorities have a clearer view on the application of the data protection legislation on geographic data, but these views differ. Data Protection Authorities consider geographic data personal data, and give some guidelines on the use and dissemination of geographic data. This aspect is missing in legislation.

Jurisprudence also differs from the other perspectives, and among themselves. With jurisprudence there are often references to general privacy legislation, but not so much to specific personal data legislation, and often cases have a very specific context, for example using Google Street View in law enforcement.

Using the traffic light model, there is a clearer view on the types of personal data. With geographic data the context of the processing stays important, because the data can be linked and it is possible by using geographic data to get an insight on the state of a building or lot.

But other types of geographic data, for example factual data that does not reveal sensitive information about a person can be disseminated easier by using the traffic light model. This gives room to opening up data under the INSPIRE Directive and the PSI Directive.

The Draft Regulation could implement the traffic light model and clear rules on the risk assessment to harmonise the different interpretation between and inside EU Member States.

11 *Discussion*

In this part the methods, and results of the research are discussed and further research is discussed.

Some parts of this research are still interesting for further research. This research aims at providing suggestions for harmonizing the data protection legislation in the different EU Member States. This harmonization should create opportunities for businesses operating in the internal market. Two things that are open for further research are the cultural aspect of privacy and personal data protection in the different countries, because privacy legislation and opinions on privacy and personal data protection shift from strict to less strict in different times and different cultures. This research did not go into detail on the cultural aspect.

Also, the research is executed with a geographic data perspective, but it could be interesting to research more from a juridical perspective, when there is more case law available to research, this could lead to interesting comparisons between the perspectives in the Member States.

Because the opening up of geographic data is a recent topic, there has not been very much jurisprudence on the subject, when there is more case law and more political attention towards this topic of opening up geographic data and the interpretation of data protection legislation this could result in a more extensive research.

The research was conducted with a literature study on four case-studies, this has some advantages, it is an opportunity to research a part of the European Union in the same way, and it gives some interesting and useful examples to compare. But more interviews on the subject by different stakeholders would give a better insight on the motivation and future processes and the role of technology for example linking of data.

12 *References*

AGIV Viewer (2015). Generieke Viewer [online]. URL= http://geo-vlaanderen.agiv.be/gdiviewer/ [Accessed: 24-04-2015].

Article 29 Working Party (2007). Opinion 4/2007 on the concept of personal data.

Article 29 Working Party (2013). Opinion 06/2013 on open data and public sector information ('PSI') reuse. Pp.1-28.

Bagviewer (2014). Bagviewer, Kadaster [online]. URL= https://bagviewer.kadaster.nl/lvbag/bag-viewer/index.html#?searchQuery=heidelberglaan,%20utrecht&objectId=0344100000027739&geometry.x=140333.04847436&geometry.y=455247.02659103&zoomlevel=13&detailsObjectId= [Accessed:07-11-2014].

BBC (2009). Call to 'shut down' Street View. 24-03-2009

Beck-Online (2015). Die Datenbank [online]. URL= www.beck-online.de [Accessed:24-03-2015].

Bergmann, L., Möhrle, R., & Herb, A. (2011). Datenschutzrecht Kommentar. Loseblattsammlung in, 3.

BMJV (2003). Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist.

BMJV (2009). Geodatenzugangsgesetz vom 10. Februar 2009 (BGBl. I S. 278), das durch Artikel 1 des Gesetzes vom 7. November 2012 geändert worden ist.

BR-Drs (2010). Gesetzesantrag der Freien und Hansestadt Hamburg Entwurf eines Gesetzes zur Änderung des Bundesdatenschutz-gesetzes. Drucksache 259/10. 24-04-2010.

Bryman, A. (2012). Social Research Methods. Fourth edition. Oxford University Press.

BT-Drs (1997). Gesetzentwurfdes Abgeordneten Manfred Such und der Fraktion BÜNDNIS 90/DIE GRÜNEN Entwurf eines Bundesdatenschutzgesetzes (BDSG). Drucksache 13/9082, 14-11-1997.

BVerfG (2006). ECLI:DE:BVerfG:2006:rs20060302.2bvr209904. 02-03-2006.

BVerfG (2006a). ECLI:DE:BVerfG:2006:rk20060502.1bvr050701. 02-05-2006.

Cate, F.H. (1995). The EU Data Protection Directive, Information Privacy, and the Public Interest. Iowa Law Review, 431, pp. 431-443.

CBP (2001). Digitale beelden van openbare omgeving vallen soms onder privacywetgeving[online]. URL=https://cbpweb.nl/nl/nieuws/digitale-beelden-van-openbare-omgeving-vallen-soms-onder-privacywetgeving-[Published 16-02-2001] .

CBP (2006). Advies wetsontwerp BAG. 12th July 2006.

CBP (2014). Missie, visie en kernwaarden[online]. URL=https://cbpweb.nl/nl/over-het-cbp/missie-visie-en-kernwaarden [Accessed:16-12-2014].

CBP (2015). Wat zijn persoonsgegevens[online]. URL= https://cbpweb.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens?qa=persoonsgegeven [Accessed: 22-04-2015].

CBPL Advies 26 (2006). Adviesaanvraag inzake het gebruik van satellietbeelden bij de opsporing en de vaststelling van bouwovertredingen. SA2 / A / 2006 / 015.

CBPL Advies 40 (2006). Bijhouden van gemeentelijke registers van onbebouwde percelen waarvan sprake in artikel 62 van het Vlaams Decreet van 18 mei 1999 houdende de organisatie van de ruimtelijke ordening en hun bekendmaking op het Internet via het toekomstige geoloket. SA2 / A / 2006 / 030.

CBPL Advies 32 (2008). Advies inzake het voorontwerp van decreet betreffende de Geografische Data-Infrastructuur Vlaanderen. A/2008/032.

CBPL Advies 05 (2010). Aanbeveling uit eigen beweging inzake Mobile Mapping. CO-AR-2010-007.

CBPL (2015). De Privacywet[online]. URL=http://www.privacycommission.be/nl/de-privacywet [Accessed 08-01-2015].

Council of Europe(1951). European Convention of Human Rights. Rome.

Council of Europe(1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg.

Cuijpers, C., P.Marcelis (2012). Oprekking van het concept persoonsgegevens beperking van privacybescherming? Computerrecht, 6, pp. 397-409.

Curia (2015). General presentation [online].
URL=http://curia.europa.eu/jcms/jcms/Jo2_6999. [Accessed:17-04-2015]

Cyclomedia (2014) [online]
URL=http://www.cyclomedia.com/nl/producten/beeldmateriaal/ [Accessed 16-12-2014].

Data protection act (1998). Data Protection Act 1998. 1998 CHAPTER 29.

Datenschutzzentrum (2008). Keine Straßenerfassung in Schleswig-Holstein ULD hält Google Street View für rechtswidrig. 01-10-2008.

De Kamer (1998). WETSONTWERP tot omzetting van de Richtlijn 95/46/EGvan 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens. - 1566 /1 - 97 / 98

ECHR (2015). Court in Brief. Council of Europe.

ECJ (2014). ECLI:EU:C:2014:2081. 17-07-2014.

EDPS (2011). Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union". Pp.1-36.

EDPS (2012). Opinion of the European Data Protection Supervisor on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents. Pp. 1-13.

EDPS (2015). Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations. Pp. 1-520.

Eisenhardt, K.M. (1989). Building theories from case study research. Management Review 14 (4), pp. 532-550.

ePSI (2012). How is open data valuable for a more efficient government [online]. URL=http://www.scribd.com/doc/94534830/How-is-open-data-valuable-for-a-more-efficient-government. [Accessed 15-08-2014].

EUObserver (2008). Google map service could face EU lawsuits [online]. URL= https://euobserver.com/economic/26154 [Accessed 07-08-2015].

EU open data (2014).Digital Agenda for Europe: Open data [online]. URL= http://ec.europa.eu/digital-agenda/en/open-data-0 [Accessed 21-10-2014].

Europa (2015).Regulation, Directives and other acts [online]. URL= http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm [Accessed 31-03-2015].

European Commission (2011). Open data, an engine for innovation, growth and transparent governance. COM (2011) 882 final.

European Commission (2011a). Results of the online consultation of stakeholders"Review of the PSI Directive" [online]. URL= http://www.lapsi-project.eu/lapsifiles/Results%20of%20the%20online%20consultation%20of%20stakeholders%20final.doc [Accessed 01-12-2014].

European Commission (2012).Reform of data protection legislation [online]. URL=http://ec.europa.eu/justice/data-protection/[Accessed: 17-10-2014].

European Commission (2012a). COMMISSION STAFF WORKING PAPER Impact Assessment. SEC(2012) 72 final.

European Commission (2012b) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.

European Commission (2014). The EU Single market. An historical overview [Online]. URL= http://ec.europa.eu/internal_market/top_layer/historical_overview/index_en.html [Accessed: 27-03-2015].

European Commission (2014a). COMMISSION NOTICE Guidelines on recommended standard licences, datasets and charging for the reuse of documents. Official Journal C 240, pp. 1-10.

European Commission (2014b). Factsheet on the right to be forgotten ruling.

European Union (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, pp.31-50.

European Union (2003). Directive 2003/98/EC of the European parliament and of the council of 17 November 2003 on the reuse of public sector information. Official Journal L345, pp. 90-96.

European Union (2013). DIRECTIVE 2013/37/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 amending Directive 2003/98/EC on the reuse of public sector information. Official Journal L 175, pp. 1-8.

European Parliament (2014). European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

Focus Magazin (2009). "Street-View-Start noch dieses Jahr". 27th of April 2009, p. 20.

Fornefeld, M., G. Boele-keimer, S. Recher and M. Fanning (2008). Assessment of the Reuse of Public Sector Information (PSI) in the Geographical information, Meteorological Information and Legal Information Sectors. Dusseldorf: MICUS Management Consulting GmbH.

Fromholz, J.M. (2000). The European Union Data Privacy Directive. Berkely Technology Law Journal 15, pp.461-484.

Gellman, R.M. (1996). Can Privacy Be Regulated Effectively on a National Level - Thoughts on the Possible Need for International Privacy Rules. Villanova Law Review 41, pp.129-172.

Google Street View (2014). Street View [online] URL=https://www.google.com/maps/views/streetview?gl=nl [Accessed:07-11-2014].

HUDOC (2015). European Court of Human Rights[online] URL=http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#{"documentcollectionid2":["GRANDCHAMBER","CHAMBER"]} [Accessed: 17-04-2015].

Huijboom, N., T. van den Broek (2011). Open data: an international comparison of strategies. European Journal of ePractice 12, pp. 1-9.

ICO, (2009). Common sense on Street View must prevail, says the ICO. Press Release via the national Archives online [url= http://webarchive.nationalarchives.gov.uk/20090506234143/http://www.ico.gov.uk/upload/documents/pressreleases/2009/google_streetview_220409_v2.pdf] .

ICO (2009a). The INSPIRE Regulations 2009.

ICO (2012). Determining what information is 'data'for the purposes of the DPA. Version: 1.1, 12-12-2012.

ICO (2014). ICO Disclosure Log Response to Request. 21-11-2014, IRQ0559613.

INSPIRE (2014). About INSPIRE [online]. URL=http://INSPIRE.ec.europa.eu/index.cfm/pageid/48 [Accessed: 10-11-2014].

INSPIRE themes (2014). Data specifications[online]. URL= http://INSPIRE.ec.europa.eu/index.cfm/pageid/2/list/7 [Accessed: 10-11-2014].

Janssen, K. (2011). The influence of the PSI Directive on open government data: An overview of recent developments. Government Information Quarterly 28, pp. 446-456.

Janssen, K., S. Hugelier, (2013). Open data as the standard for Europe? A critical analysis of the European Commission's proposal to amend the PSI Directive. European Journal of Law and Technology, Vol. 4, 3.

Juridat (2015). Juridat Rechtrspraak opzoeking[online]. URL= http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=nl [Accessed: 24-03-2015].

Kamerstukken (1998). Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). 1997-1998, 25892, nr.3.

Kamerstukken(2007) Regels omtrent de basisregistraties adressen en gebouwen (Wet basisregistraties adressen en gebouwen). 2006-2007, 30 968, nr. 3.

Kamerstukken (2008). Implementatie van richtlijn nr. 2007/2/EG van het Europees Parlement en de Raad van de Europese Unie van 14 maart 2007 tot oprichting van een infrastructuur voor ruimtelijke informatie in de Gemeenschap (INSPIRE) (Implementatiewet EG-richtlijn infrastructuurruimtelijke informatie). 2008-2009, 31 771, nr.3.

Kamerstukken (2010). Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden. 2509, nr.2.

Kamerstukken (2013). Regels omtrent de basisregistratie grootschalige topografie (Wet basisregistratie grootschalige topografie). 2012-2013, 33 527, nr.3.

Karg, M. (2008). Datenschutzrechtliche Rahmenbedingungen für die Bereitstellung von Geodaten für die WirtschaftUnabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). pp. 1-75.

KG Berlin (2010). 10 W 127/10. 25-10-2010.

Korff, D. (2002). EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE comparative summary of national laws. Human Rights Centre, University of Essex, Colchester.

Korff. D. (2010). Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, study commissioned by the European Commission. Working Paper No.2.

Kulk, S., B. van Loenen (2012). Open data and beyond Exploring existing open data projects to prepare a successful open data strategy. Deelrapport privacy, 2012.

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. Computer law & security review 25, pp. 307-317.

Land Registry (2012). Privacy Impact Assessment Report Making price paid data available through publication in a machine readable and reusable format. March 2012.

Land Registry (2013). Privacy Impact Assessment Review. Price paid data, transaction data and historical price paid data. April 2013.

LG Waldshut-Tiengen. Erfassung und Verbreitung digitaler Gebäudeabbildungen. MMR 2000, 172, 175.

Loenen, B. van, J.A. Zevenbergen, and J. de Jong (2008). Geo-informatie: wat is het en wat is de juridische context?

Loenen, B. van and Y. Verdonk (2011). Open Data: van ideaal tot realiteit. NCG 55, pp. 1-33.

Mapbox (2014). 40 cm satellite imagery starts today [online]. URL=https://www.mapbox.com/blog/sharper-satellite-images/ [Accessed:07-11-2014].

Miles, M.B., A.M. Huberman (1994). Qualitiative data analysis. 2nd edition. Sage publications: London.

Ministry of economic affairs (2013). Routekaart doorbraakproject ‘Open geodata als de grondstof voor groei en innovatie’. HLO versie 28 oktober 2013.

Newman, A.L. (2008). Building Transnational Civil Liberties: Trans governmental Entrepreneurs and the European Data Privacy Directive. International Organization, 62, pp. 103-130.

Marschan-Piekkari,R., C. Welch (2004). Handbook of qualitative research methods for international business. Cheltenham: Edward Elger publishing.

Open Data Index (2014). Global Open Data Index.[online]. URL=http://global.census.okfn.org/[Accessed: 16-10-2014].

Open Definition (2014). The open definition [online]. URL=www.opendefinition.com [Accessed: 18-09-2014].

Open Government Data (2014). Why open government data[online] URL=www.opengovernmentdata.org [Accessed: 18-09-2014].

Open Government Partnership (2014). What is the Open Government Partnership? [online] URL=http://www.opengovpartnership.org/[Accessed: 18-09-2014].

Privacy International (2007). National Privacy Ranking 2007.

Rechtspraak (2013). ECLI:NL:GHAMS:2013:5224. 2nd of May 2014.

Rechtspraak (2015). Zoeken in uitspraken[online]. URL= http://uitspraken.rechtspraak.nl/. [Accessed: 24-03-2015].

Robinson, N., Graux, H., Botterman, M., & Valeri, L. Review of the European Data Protection Directive.

Rothenberg, J. (2012). Towards a better supply and distribution process for open data. Case study international benchmark on open data and use of standards. Forum Standaardisatie.

Senaat (1992). Ontwerp van wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. 445/2. 27-10-1992.

Senaat (2011). Voorstel van resolutie waarin wordt gevraagd de eerbiediging van het privéleven en de integriteit van de overheidsinfrastructuur te waarborgen in het licht van de opnames die google inc. maakt voor zijn « street view »-dienst. 1101/1, 01-06-2011.

Scassa, T. (2014). Privacy and Open Government. Future Internet, 6, pp. 397-413.

Schwartz P.M. and D. J. Solove (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L.Q.Rev. 1814.

Solove, D.J.(2008). Understanding Privacy. Cambridge, Massachusetts, etc. : Harvard U.P.

Standaard, de (2009). Google doet aangifte bij Privacycommissie voor straatfoto's. Published:09-04-2009.

Tan, D.R. (1999). Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulation in the United States and European Union. 21 Loy. L.A. Int'l & Comp. L. Rev. 661.

The Guardian (2006). UK fights against tide on data directive. 26-07-2006.

Trouw (2008). Privacy gewaarborgd, dus geen bezwaar tegen straatfoto's Google. Published: 06-06-2008.

Tweakers (2009). Google Street View schikt zich naar Belgische privacywetgeving [online]. URL= [Accessed 06-11-2014].

VG Karlsruhe (2000). Elektronische Häuser- und Gebäudekarte. MMR 2000, 181.

van der Sloot, B. (2011). De wegen van Google zijn ondoorgrondelijk: over Street View en dataprotectie. Privacy & Informatie, 14(4), 176-190.

Vlaams Parlement (2009). ONTWERP VAN DECREET betreffende de Geografische Data-Infrastructuur Vlaanderen. Stuk 2022 (2008-2009) – Nr. 2.

Warren, S.D. and L.D. Brandeis. The Right to Privacy. Harv. L. Rev. 1890, 4, pp.193–220.

WestLaw UK (2015). Search Westlaw UK [online]. URL=http://login.westlaw.co.uk/maf/wluk/app/tocectory?sttype=stdtemplate&stnew=true [Accessed: 24-03-2015].

Westin, A.F. (1970). Privacy and Freedom. 2nd edition, London: The bodley head.

13 *Annex A*

Interview met Ir. Martin (M.J.G.M.) te Dorsthorst van Cyclomedia .

Cyclomedia is een bedrijf dat foto's van de leefomgeving maakt voor de zakelijke markt. Ze zijn actief in Nederland, Duitsland, Noorwegen, Zweden en de Verenigde Staten en niet meer actief in België. We maken foto's van openbare wegen, dat is privacy gevoelige informatie.

Hoe vinden ze de initiatieven van Europese Unie om data te beschermen?

De initiatieven om data te beschermen hebben we geen problemen. Maar, dit moet wel realistisch gebeuren. Overtrokken reageren is belemmerend. Bijvoorbeeld in Duitsland wordt met veel paniek gereageerd. Omdat onze gegevensverwerking in het zicht plaatsvindt, tastbaar is wordt er met meer paniek op gereageerd dan bijvoorbeeld met Facebook, en andere sociale media. Als je praat over geo gegevens, ook al worden alle gegevens geanonimiseerd.

Merkt u van de regelgeving in Europa?

Van de regelgeving wel, vooral dat er geen eenduidig beleid is. Nederlands is wat liberaler. Wij verstrekken alleen aan de zakelijke markt. Het gebruiksdoel moet worden vastgelegd en kan niet algemeen gebruikt worden.

Hoe gaat dat met de verschillen tussen landen? En heeft u hier voorbeelden van?

Het verschil zit vooral in de implementatie tussen lidstaten. Brussel wordt steeds strenger, en dat leidt tot verkeerde situaties.

In Duitsland wordt meer vanuit paniek gereageerd, de politiek begrijpt het niet en de regel zijn niet duidelijk te interpreteren. In Nederland is het zakelijker. In België is het ook strikter, alles moet bijgehouden worden, daar moet alles bewijsbaar en aantoonbaar zijn. Als een ambtenaar een bepaalde beeld bekijkt dan moet gelogd worden waarom hij dat heeft gedaan. Daarin zie je de verschillen tussen Europese landen. Als je kijkt naar Zweden dat ligt dichterbij Nederland en Noorwegen dichterbij de Duitse interpretatie.

In Duitsland gaan we het verst, daar moeten we kentekens, en gezicht blurren, en op verzoek van de bewoners ook hun huizen. Dan ga je al een stap verder. Om problemen te voorkomen plaatsen we ook advertenties in een lokaal weekblad waar we aangeven, wat we gaan doen en waar voor de gegevens gebruikt worden. Als iemand wil dat we op voorhand zijn huis blurren, dan doen we dat. We zetten er een telefoonnummer bij en als mensen een auto van ons zien rijden en foto's maken kunnen ze ook contact opnemen. We respecteren de gevoeligheid die daar is, die gevoeligheid is veroorzaakt door Google.

Google heeft de zaak opgeblazen, door ook onzichtbare gegevens op te nemen. Door bijvoorbeeld sensoren op de auto's te plaatsen om Wi-Fi signalen op te nemen. Dan vertrouwt niemand je meer, dat soort escalaties. Maar, we merken wel dat door bijvoorbeeld Google dat met de Street View auto's MAC adressen heeft verzameld .

Dit soort verschillen kun je voorkomen door eenduidige wetgeving, dan weet iedereen wat er gebeurt en wat er met de data gaat gebeuren.

Wat verstaat u onder eenduidige wetgeving? Wat vinden ze van de verantwoordelijkheid van Nederlands als bronhouder van de gegevens?

Verantwoording mag best bij de bronhouder, maar wel op eenduidige wijze. Wat je bij bronhouders wel hebt is een ander aspect, dat van concurrentie. Zorgvuldiger omgaan met privacy gevoelige informatie, dus bijvoorbeeld het blurren, kost geld. Niks voor niks dus dan

krijg je concurrentie vervalsing. Dus als je een gemeenschappelijke basis maakt voor iedereen, en je zorgt dat die basis wordt gehandhaafd. Dan is dat goed.

Merkt u een verschil in argumentatie tussen de lidstaten?

In Nederland is er een zakelijke argumentatie, er wordt gekeken naar wat voor nut het heeft. In Duitsland wordt veel meer vanuit paniek gereageerd. Dat is veroorzaakt door Google, door dingen te doen waarvan mensen zeggen, dat is niet recht en misschien gebeurt er wel meer wat wij niet weten. Wij werken op basis van vertrouwen, in Duitsland op basis van wantrouwen. Het geldt hier vertrouwen komt te voet en gaat te paard. Een keer iets fout, zoals Google heeft gedaan en dat duurt lang voordat dat weer hersteld is. Eenduidige wetgeving, als die handhaafbaar is, als je de middelen daarvoor hebt dan ben je op de goede weg.

Kent u nog meer cases op geo-gebied? Heeft u verder nog input?

Wij maken naast panorama beelden ook obliek fotos. Met panoramabeelden kijk je recht tegen het huis aan, met luchtfoto's kijken je van boven naar beneden. Met obliek fotos kijk je in alle windrichtingen, hoge resolutie je kunt veel details zien. Wij zullen ook nooit foto's in het kader van een proces. Als een advocaat vraagt om foto's van dit jaar of vorig jaar om te kijken of die auto daar nog steeds staat met dat kenteken. Wel als we bevel krijgen van OVJ werken we daar aan mee. Geen open data, heel beschermde data.

- Open data. Ik denk dat, open data is politiek een dankbaar onderwerp. Met openbaar geld verzamelen we informatie, dat geven we terug aan de maatschappij, dat klinkt genereus. Niet van de details, klinkt dat aardig. Niet gekeken naar privacy, afschermen als ze iets niet willen, privacy argument maar dat is niet het echte argument. Open data is prima, maar in bepaalde mate. Open data is die data die door de overheid is gecreëerd en benodigd is voor haar publieke taak en daar moet het bij blijven. Als het over die grens heen gaat wordt het gevaarlijk. Waar die grens moet liggen, gebruik ik een metafoor. Een ambtenaar heeft voor z'n taak informatie nodig, ook nieuws hoort daar bij. Dus de ambtenaren krijgen een landelijk dagblad. De Telegraaf wint die tender. Dus de overheid zegt dan gaan we die informatie openbaar weergeven. Dat zorgt voor verstoring van de open data markt. Er wordt niet naar privacy, marktverstoring en innovatie gekeken. Dat besef begint een beetje te komen. Dus privacy en privacy gevoeligheid komen bij open data om de hoek kijken.

- Internet of things en wearables. Het aantal devices dat informatie verzamelt vertienvoudigt in de komende jaren en in 2020 is dat aantal 15 keer zoveel. Al die info heeft een geo-component in zich. Al die sensoren, dus al die informatie over plaatsen komt beschikbaar. Dus als je gaat hardlopen en je neemt je hartslag op en informatie over je hartslag komt als big data beschikbaar, de verzekering kan dan kijken wat is de conditie van de jongeman. Zoals het nu gehanteerd wordt, om angsten tegen te gaan. Mensen delen op Facebook alles, bijvoorbeeld trainingsschema's. Dat is eigenlijk veel gevaarlijker dan een foto van je huis. Het tastbare en zichtbare wordt geprotesteerd, en het ontastbare en onzichtbare, daar doet iedereen aan mee en denkt dat het goed afloopt.

Bedankt voor het interview.