

Can the European Data Retention Directive Settle in the United States of America?

June 27, 2008

David Riphagen: 1102303

EPA1431: Cross-cultural management

Delft University of Technology



Summary

The European Union has a Data Retention Directive, which obliges Member States to implement a mandatory data retention act for telecommunication providers. Implementations amongst European countries varied with respect to which data to retain, the retention period, how to get access to the data and the legality of national acts. These differences are the outcomes of differences in cultural norms and values. The United States have hinted multiple times on implementing a similar data retention act, as a transplant from the EU. By examination of the cultural differences between the EU Member States, I can predict how data retention would be implemented in the USA. If the United States would implement data retention, the nature of the data to be retained would be detailed in the act, the retention period would be average (which is 12 months in Europe), access would be restricted by means of a court order and the legality of the act would be questioned on different levels of the government.

Keywords: policy transplantation, data retention directive, European Union, United States of America

Table of Contents

1. Data Retention in Europe: Transplantation to the USA?	4
2. European Data Retention Directive	7
2.1 What is the European Data Retention Directive?.....	7
2.2 Adoption and implementation by Member States.....	7
3. Which Cultural Differences Explain the Varying Implementations?	10
3.1 Families of nations.....	10
3.2 Cultural families.....	12
3.3 Follow-up.....	14
4. Cultural Differences Between the USA and the EU	15
4.1 How do the Americans score on key cultural factors?.....	15
4.2 Predicting a potential implementation of data retention in the United States.....	16
5. United States Law Concerning Data Retention	17
5.1 Period of data retention by private parties and access to this data.....	17
5.2 Data retention acts and legality of a new act.....	18
5.3 Detailing of data to be retained.....	18
5.4 Conclusion.....	19
6. Conclusions	20
6.1 Various European implementations of the Directive.....	20
6.2 Cultural factors explaining differences in implementation.....	20
6.3 Cultural differences and similarities concerning data retention between the United States of America and the European Union.....	21
6.4 United States law regarding data retention.....	21
6.5 Synthesis.....	21
6.6 Recommendations for further research.....	22
References	23
Appendix A – Implementation per Member State	28

1. Data Retention in Europe: Transplantation to the USA?

The European Union has a Data Retention Directive, 2006/24/EC (Kuner 2007; Article 29 Data Protection Working Party 2006; Article 29 Data Protection Working Party 2007). This Directive was implemented in March 2006 to harmonize rules on data retention across the Member States. The Directive sets guidelines for the retention of data by publicly available communication providers in the Member States for at least 6 and at most 24 months (EPIC 2007).

Adoption and implementation of the Directive in the European Union has been in flux and varies significantly per country (Hermida 2006). The Article 29 Data Protection Working Party notes that “[T]he Directive ... leaves room for diverging interpretation and implementation by the Member States” (Article 29 Data Protection Working Party 2007). Cultural differences between countries and differences in countries' histories play an important role in the diffusion of the implementations (Kuner 2007). This is most noticeable by the amount of time it takes Member States and the path they choose to implement the Directive, as Kuner (2007) predicted. As of the end of 2007, Slovenia has already implemented the Data Retention Directive as amendments to their Electronic Communications Act, while the Swedish Minister of Justice assigned a Commission of Inquiry with the task of reviewing the national legislation to propose the amendments required (Article 29 Data Protection Working Party 2007).

The American general attorney, US Congress and the FBI have, on multiple occasions, hinted at implementing a data retention act like the European Directive in the United States (Broache 2006; McCullagh 2006; McCullagh 2008). The proponents are looking at Europe as an example for data retention in the USA.

This paper is a part of the course EPA1431(Cross-cultural Management). Therefore I will focus on the cultural aspects of transplanting this directive to another country. The field of cross-cultural management provides guidelines to evaluate to what extent transplanting the European Data Retention Directive will succeed in the United States. In this paper I draw both from literature on culture (Hofstede 2005; F. Trompenaars, A. Trompenaars & Hampden-Turner 1998), institutional transplantation (De Jong, Lalenis & Mamadouh 2002) and international privacy laws (Solove & Rotenberg 2003; Allen 2007).

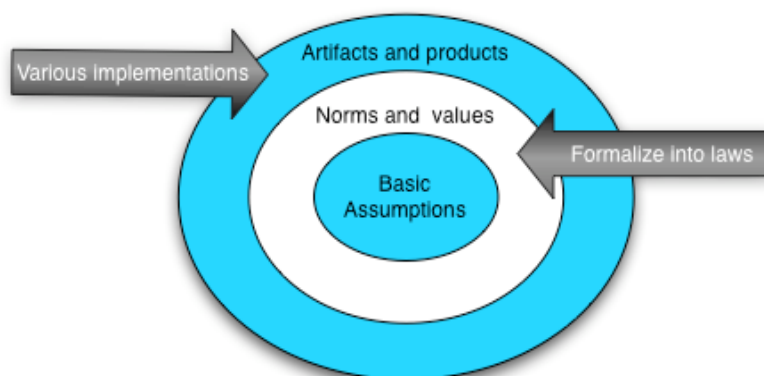


Illustration 1: Trompenaars' (1998) model of cultural layers and the implementation of the Directive

Hofstede and Trompenaars will provide the criteria to identify and assess cultural differences between the USA and Europe. The work of De Jong et al. serves as the main framework for assessing the transplantation of the European Data Retention Directive to the United States. Solove's and Rotenberg's extensive summary of (international) privacy law will be the main frame of reference for understanding the EU Data Retention Directive, comparing European and American privacy laws and identifying potential

problems with the transplantation of the EU Data Retention Directive to the USA.

In this paper I look at the transplantation of the EU data directive from a 'goodness of fit' perspective (De Jong, Lalenis & Mamadouh 2002), which is based on the idea that institutional structures have evolved historically and reveal certain legal, political and cultural values per country. The goodness of fit for an institutional transplant can be assessed by looking at similar and differing characteristics for the involved countries. Can this perspective provide more insight in how a transplantation of the EU Data Retention Directive would take place?

This paper answers the following question:

Which cultural values and legal differences influence the success of the transplantation of the EU Data Retention Directive to the United States?

To answer this question, I will answer the following sub-questions:

1. In what way do the various implementations of the EU Data Retention Directive in European Member States differ?
2. How can the differences in implementation be explained by cultural differences between Member States?
3. How do these cultural differences relate to the cultural differences between the European Union and the United States of America?
4. What legal differences between the European Union and the United States of America influence the institutional transplantation of the European Data Retention Directive to the United States?

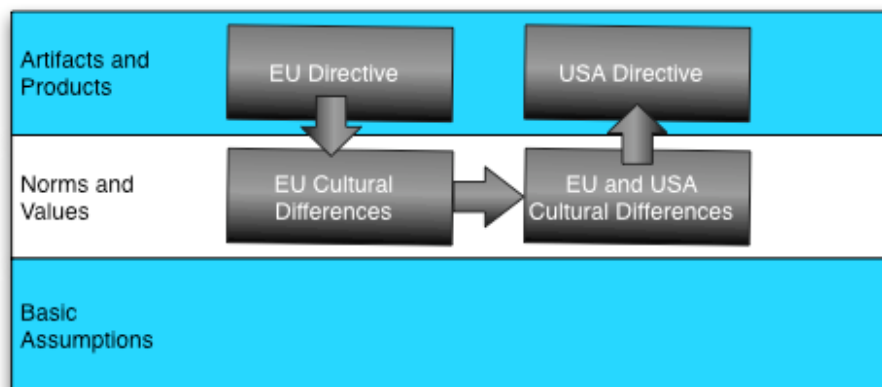


Illustration 2: Process of reconciling cultural differences in the implementation of data retention in the EU and the USA

These questions deal with policy transplantation on the different layers of culture. Trompenaars defines three layers of culture (1998):

- Artifacts and products,
- Norms and values,
- Basic assumptions.

The implementations, which vary amongst the Member States (sub-question 1) are an outcome of their different cultural norms and values (sub-question 2). Norms and values formalize into laws. Differences in cultural norms and values underlie an implementation of the EU Data Retention Directive in the USA. Sub-question three tends to clarify the differences in these norms and values between the EU and the USA. The last sub-question deals with another outcome of the differences in cultural values and

norms: the legal differences between the European Union and the United States. I will focus on legal differences that influence the data retention directive's transplantation to the USA. The relationships between Trompenaars' model and the implementation of the Directive are depicted in illustration one.

A plethora of literature is dedicated to the differences between the Common Law practiced in the United States and the Statutory or Civil Law practiced in Europe. Books about legal traditions compare both systems on their merits (Merryman & Perez-Perdomo 2007). I decided not to include these differences in my analysis for the following reasons:

- It diverts the focus from the cultural norms and values that form the basis of the cultural differences, which materialize in the differing implementations.
- The legal tradition is not relevant for the thoughts and motives supporting the Directive, which are shaped by cultural norms and values.
- Solove and Rotenberg (2003) argue that a comparative analysis on the US and European privacy regimes is viable.

In chapter two I will provide a closer look at the European Data Retention Directive and how adoption and implementation differed per Member State. The chapter concludes with a list of key differing factors for the implementation. These are the artifacts and products of the cultural differences, as depicted in illustration 2. Chapter three investigates the cultural differences between European Member States regarding these key differing factors, or the cultural norms and values underlying the differences in implementation. This chapter concludes with the cultural differences that affected the differences in implementations the most. In chapter four I look at how these cultural factors vary between the European Union and the United States, as can be seen in the lower right of illustration two. In paragraph 4.2 I describe how a data retention act in the United States would look like, based on the USA's cultural characteristics. Chapter five goes more in-depth with the implementation of a data retention act in the USA by looking at the appropriate laws concerning the implementation. In chapter six I will present the cultural and legal differences that influence the success of the transplantation. I will present additional conclusions and suggestions for further research.

2. European Data Retention Directive

2.1 What is the European Data Retention Directive?

The European Data Retention Directive was adopted to ensure the availability of traffic data for antiterrorism purposes. It states that communication service providers, such as Internet Service Providers (ISPs) and telecom operators (telcos), should routinely capture communications data and retain this for a minimum period of six months and a maximum of two years (EPIC 2007; Kuner 2007). Communications data is defined as traffic data and location data. Traffic data is all data that is generated to ensure the transportation of data over the network, such as destination address, origin address and routing information. Location data indicates the geographic position of the users. The Directive does not cover the content of electronic communications.

Kuner (2007) summarizes the types of data to be retained according to the Directive as follows:

- Data necessary to trace and identify *the source of a communication*.
- Data necessary to identify *the destination of a communication*.
- Data necessary to identify *the date, time and duration of a communication*.
- Data necessary to identify *the type of communication*.
- Data necessary to identify *a user's communication equipment or what purports to be their equipment*.
- Data necessary to identify *the location of mobile communication equipment*.

The data should become available to competent national authorities in specific cases, "[F]or the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law" (EPIC 2007). These authorities should be able to access the data without undue delay.

The data should be retained for between 6 and 24 months from the date of communication. It must be erased following expiration of the retention period.

2.2 Adoption and implementation by Member States

The Member States of the EU initially had until September 15, 2007, to implement the laws complying with the Data Retention Directive. However, a delay until March of 2009 was foreseen (EPIC 2007). This is the most visible difference between the implementations of the various Member States. Sixteen of the twenty-five Member States have said to make use of this extension period. These are: Austria, Belgium, Cyprus, Czech Republic, Estonia, Finland, Germany, Hellenic Republic, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Slovenia, Sweden, UK (Article 29 Data Protection Working Party 2007).

The Czech Republic, Estonia, Ireland and Italy already had mandatory data retention acts. Except for Ireland, those implemented the EU Directive faster as an amendment to their current laws (2005; 2005b; Pospipil 2006; 2007c). The UK had a voluntary data retention agreement with several ISPs (2007h).

The Member States also have the freedom of setting the period that telcos and ISPs should retain the data. The general agreement in the Directive says that the data should be retained between six and twenty-four months. Austria and Germany require retention for six months. Poland and Slovenia require telcos and ISPs to retain the data for twenty-four months. Other Member States, including Bulgaria, the Czech Republic, Denmark, France, the Netherlands, Romania, Spain and the United Kingdom have proposed or installed a retention period of twelve months (Joergensen 2006; Pospipil

2006; Article 29 Data Protection Working Party 2007; 2007; 2007b, 2007d, 2007e, 2007g; Grancharova 2008; Van Hoboken 2008; 2008).

The German working group on data retention challenged the law at the Federal German Constitutional Court on January 6, 2008 (2008). In Hungary (Foldes 2008), Ireland (McIntyre 2008) and Lithuania (2004) different organizations have brought the data retention act before their respective constitutional courts.

I have explored the varying implementations per Member State. The results are described in appendix A and I deal with specific references in that appendix. Below I provide a summary of the most important differences in implementation. The key differences in implementation of the Directive by the Member States are:

1. **Speed of implementation.** Sixteen of the twenty-five Member States announced to use the extension period for implementation of the Directive (Article 29 Data Protection Working Party 2007). In Bulgaria, Denmark, Germany, Romania and the United Kingdom the law went into effect respectively on February 2, 2008 (Grancharova 2008), August 10, 2008 (Joergensen 2008), January 1, 2008 (2008), February 20, 2008 (2008a) and July 24, 2007 (2007).
2. **Presence of a data retention act.** The Czech Republic, Estonia, Ireland, Italy, Lithuania and Poland already had a data retention act, anticipating on EU Directive (2004; 2005; 2005b; Pospipil 2006; Article 29 Data Protection Working Party 2007; 2007c). The United Kingdom had a voluntary code by which ISPs guaranteed to retain data (2007h).
3. **Period of data retention.** The period that telcos and ISPs should retain data varies per Member State from 6 months (Germany, Austria) to 12 months (such as The Netherlands) and 24 months (Poland, Slovenia) (Joergensen 2006; Pospipil 2006; Article 29 Data Protection Working Party 2007; 2007; 2007b, 2007d, 2007e, 2007g; Grancharova 2008; Van Hoboken 2008; 2008).
4. **Compliance with national constitutional law.** In the Member States Ireland (McIntyre 2008), Lithuania (2004), Hungary (Foldes 2008) and Germany (2008) the Constitutional Court was asked to decide on the compliance of the implementation of the Directive with the respective constitutions.
5. **Access privileges.** Some Member States allow all their government agencies access to the data, other restrain access to the police. The latter is the case in the Czech Republic (Svatosova 2008). France (2007b) and Belgium (Article 29 Data Protection Working Party 2007) both have specific government agencies that retain and regulate access to the data. Most countries, such as Italy (2005b), Germany (2007d) and Romania (2008) ask for court orders before access to the data is granted. The UK Regulation and Investigatory Powers Act enables public officials of 702 agencies to obtain traffic data from service providers (Anderson 2008). In the Netherlands, government agencies can claim complete parts of the collected data to be retained (Van Hoboken 2008).
6. **Amount of detail in the law about the type of data that should be retained.** A few Member States, such as the Czech Republic (Svatosova 2008) don't describe the type of data that should be retained by ISPs and telcos at all. Other Member States, such as Denmark (Joergensen 2006), France (Marzouki 2006), Italy (2005b), Lithuania (2004), The Netherlands (Van Hoboken 2007) and the United Kingdom (2007) provide an (exhaustive) list of what information should be retained. In Germany, providers of "anonymization" services are also obliged to retain data (2007d). The Lithuanian Constitutional Court ruled that the retention of data by telcos and ISPs should be strictly limited to data that is already retained for ISPs ordinary business activities. (2004).
7. Ireland and Slovakia doubt **the legality of the European Data Retention**

Directive, arguing that it should be a European Framework Directive under the third pillar. They challenged the law in front of the European Court of Justice (Bendrath 2006). The German parliament didn't pass a motion to join Ireland and Slovakia in these efforts (Bendrath 2006).

In the next chapter I will discuss the differences in cultures between the European Member States and will come up with hypotheses about how these cultural differences influence the varying implementations of the Directive.

3. Which Cultural Differences Explain the Varying Implementations?

The differences in cultural artifacts and products between the Member States are a result of the underlying differences in cultural norms and values (Trompenaars 1998). Similarities on cultural norms and values between countries influence the success or goodness of fit of the transplant, the European Data Retention Directive (De Jong, Lalenis & Mamadouh 2002).

The goodness of fit between the transplant and the hosts (Member States) can be assessed by characterizing the involved countries as families of nations (De Jong, Lalenis & Mamadouh 2002). I agree with De Jong et al. (2002) that this perspective relies on how we distinguish families of nations and how influential the characteristics of each of these families are to the suitability of the transplant. In paragraph 3.1 I look at the how the differences in implementation of the Directive can be explained by the families of nations concept and provide a list of key factors. In paragraph 3.2 I assess how cultural families influence these differences and again provide a list of key factors. In paragraph 3.3 I will provide a follow-up to determine how these differences in cultures help determine the success of the data retention transplant.

3.1 Families of nations

Families of nations can be distinguished by looking at countries' lineage, their (separated) siblings, affinity groups (countries sharing an affinity for the same cause or ideas) or partnerships (Therborn 1993). De Jong et al. (2002) add legal similarities as an extra characteristic to determine a family of nations.

The lineage of the Member States correlates with the following similarities between the implementation in the different Member States:

- The neighboring countries of Bulgaria and Romania have already implemented the Directive. Their **speed of implementation** is considerably higher. Bulgaria and Romania were both part of the Soviet Union and share therein a common lineage. I argue that the influence of the Soviet Union, and particularly the KGB, as surveillance state has an important role on the speed of implementation of the Directive.
- The geographically concentrated countries of Estonia, the Czech Republic, Lithuania and Poland already **have a data retention act present**. The common factor of lineage with these countries is their descent from the former Soviet Union.
- The United Kingdom and Ireland, countries that share the same Atlantic-oriented lineage, also already **had a data retention act in place**. The UK pressed for data retention during its presidency of the EU (EPIC 2007). The strong bond between the UK and the USA and the frequently expressed American wish for data retention in Europe (Richard: 2007) are explanations for this emphasis on data retention.
- Neighboring Germany and Austria both have a **data retention period of 6 months**. This is the minimum period allowed by the Directive. The reason for this, I argue, is because of the horrors the Nazis committed by using the information stored in the public administration. This calls for the retention of sensitive data for as short amount of time as permitted.
- The **longest data retention periods**, of 24 months, are found in Slovenia and Poland. Both countries shared an affinity for the socialist or communist system and were part of a communist regime, respectively the Socialist Federal Republic of Yugoslavia and the USSR. The role of the state in communist regimes influenced the view of state-commanded data retention and the longevity of the retention period.
- France and Belgium, both from the same lineage and separated siblings, have specific

government agencies that retain the data and control access to the retained data, thereby **centralizing the access privileges**. This is reinforced by their inheritance from the Napoleonic State, which centralized the public administration and the way the French legal system has developed.

- The countries that are situated centrally in the European Union all have a **detailed description of the type of data that should be retained**. This group includes Denmark, Germany, The Netherlands, France and Italy. The United Kingdom also has an exhaustive list of what data should be retained. These countries all have in common that they were part of the early European Union agreements in 1973, which could explain their experience with translating European Directives into detailed acts.

Regarding separated siblings, I mentioned above that the countries that were part of the Soviet regime already had a data retention act before the Directive was accepted or were among the first countries to implement the Directive. The Czech Republic, as a former Soviet Union state, is an outlier in this increased surveillance: it restricts access to the retained data to the police.

The data about the implementation of the directive didn't show any direct correlations between affinity groups of Member States and the implementation process.

Within the European Union, there are different partnerships. An important partnership is the Benelux, between The Netherlands, Belgium and Luxembourg. There is however no evidence that this partnership influences the implementation of the data retention act. As mentioned above, it seems that Belgium is legally more aligned with France than with The Netherlands.

Loughlin (1994) and Loughlin and Peters (1997) base the idea of families of states on the legal systems and public law in the countries. They distinguish between the Anglo-Saxon, the Germanic, the French and the Scandinavian families of states. This classification clarifies the following similarities between the Member States:

- The UK and Ireland, which both belong to the Anglo-Saxon family, already had a data retention act in place.
- The Germanic states of Austria and Germany both have the minimum retention period.
- The Napoleonic states of Belgium and France both have a centralized government agency to coordinate the data retention, in Belgium a coordinating body of threats (OCAM) and in France a coordinating center for antiterrorism (Uclat).

I conclude that the following cultural factors had an impact on the implementation of the Directive:

1. **Descent from a communist regime** has influenced the speed of implementation, the presence of a data retention act and increased of the length of data retention.
2. **Atlantic orientation and the presence of an Anglo-Saxon public law system** correlate with already having a data retention act in place.
3. **Involvement in prior atrocities made possible by accurate public administration**. This influenced the period of data retention, which is set to the minimum provided by the directive. Both countries that have the minimum data retention period also have a Germanic public law system.
4. **Inheritance from the French legal system** has influence on the centralization of retaining the data and controlling access to the retained data.
5. The countries that **adopted the European Union in an early stage** have detailed descriptions in their national laws about which data should be retained. This, I argue, is a consequence of their experience with implementing European

Directives in their countries.

3.2 Cultural families

Hofstede (Hofstede 2005) and Trompenaars (F. Trompenaars, A. Trompenaars & Hampden-Turner 1998) define several dimensions of cultural differences. These dimensions provide the basis for the division of the Member States in cultural families and gain additional insight in why implementation of the EU data retention act differs per country.

One of Hofstede's dimensions (2005) is the Power Distance Index (PDI), defined as the dependence that people in lower ranks have on people in higher ranks. Member States that have a low PDI (like Germany and Austria) have the shortest data retention period. This is explained by the fact that their citizens are not as dependent on their government and thus are not willing to let the government retain data longer than necessary. Countries with a high PDI, such as Poland and Slovakia, implemented the maximum retention period. It is striking that the UK and Ireland, both countries with a low PDI, already had a data retention act.

The Individualism Index (IDV) is the dimension that measures the amount of individualism in a culture. The right to privacy is a central theme in many individualist societies, and it doesn't find the same sympathy in collectivist societies (Hofstede 2005). It is therefore not surprising that the countries where the Data Retention Directive was considered unconstitutional (Ireland, Germany, Hungary) all have a high score on the IDV. Data for Lithuania was unavailable. The countries where the Directive was challenged at the constitutional court also have a low PDI and reside in the quadrant low IDV / low PDI (Hofstede 2005).

Hofstede's Masculinity Index (MAS) measures the equality of roles between the different genders. The more divergent the roles between the genders are, the higher the score on this index. This attitude towards gender replicates in attitudes towards immigrants and lawbreakers (Hofstede 2005). That would explain the questioning of the legality of the Directive at the European Court of Justice by Ireland and Slovakia (both high MAS) and the questioning of the specific law at the national constitutional courts in Ireland, Germany, Hungary and Lithuania (all high MAS, except Lithuania: no data available). The presence of a data retention act in Ireland and the UK might be explained by their intolerance for lawbreakers (high MAS) and the attention for tracing lawbreakers. The same goes of the maximum retention period for Slovakia and Poland, 24 months.

The Uncertainty Avoidance Index (UAI) measures the level of anxiety that exists in a particular society in the face of an uncertain future. In this respect it is very surprising that Ireland and the UK, two countries with a low UAI, already had a data retention act in place to combat this anxiety. Specifically, Hofstede (2005) mentions that the burden of proof in a country with a low UAI for identifying a citizen is with the authorities. In countries with a higher UAI citizens have to identify themselves all the time, as happens in countries with a strong uncertainty avoidance score. This contrasts the implementation of data retention acts in Ireland and the UK before the EU Directive was adopted. The terrorist attacks on 9/11 and the London and Madrid bombings could explain the presence of these data retention acts. I argue that the level of anxiety that people experience in the face of an uncertain future rises with the threat of terrorist attacks. This is exactly the goal of terrorists: to spread terror or anxiety. The terrorist attacks in the USA and Europe were followed by a plethora of proposals for data retention in the UK (2002; 2005c), Ireland (Hunter 2006) and other European countries (EPIC 2007). The proposals aimed at providing a less uncertain future by diminishing the probability of terrorist attacks.

Long-Term Orientation (LTO) measures a culture's fostering of virtues toward future rewards. Short-term orientation could explain the short periods of data retention in

Austria and Germany (both low LTO). However, the history of the countries might be a better explanation. Although The Netherlands has a medium data retention period and a medium LTO, both Slovakia and Poland have a low LTO and a long retention period. I conclude that the findings from the LTO are not univocal.

Trompenaars states that culture is like gravity: you don't experience it until you jump six feet in the air (F. Trompenaars, A. Trompenaars & Hampden-Turner 1998). Culture, according to Trompenaars, is the way a group of people solves problems or reconciles dilemmas. In his book, Trompenaars describes the factors that underly the various cultures and their ways of solving problems.

The first dimension that Trompenaars (1998) distinguishes is universalism versus particularism, where universalists believe that the same rules apply to everyone. The data underlying this dimension is however far from complete or consistent. The Member States where the national law is challenged at the constitutional court and where a court order is a requirement to access the retained data have a more universal outlook. The universalist countries also detail the data to be retained in their national law.

Trompenaars' second dimension distinguishes individualist from communitarian countries: do people strive for their own interests or those of a group? The data that Trompenaars presents here doesn't include the implementation of the Directive in key countries such as Germany, Austria, Slovakia, Lithuania and Romania. The Czech Republic scores very individualistic, which explains why they restrain access to the retained data to the police. Their cultural outlook is that the individual right goes before the collective right. This does not explain why the Czech didn't detail the data to be retained by the ISPs and telcos.

The range of feelings expressed by people in certain countries is measured by Trompenaars on the dimension of affective versus neutral cultures. This data didn't reveal any patterns in the implementation differences between Member States. This dimension has more to do with communication between people instead of interaction between the state and its citizens.

The Czech Republic scores diffuse on the specific-diffuse dimension. This means that the Czechs prescribe the same role to the same people for specific life spaces as work, family and public life. Your boss is not only senior in the office, but also in the supermarket and that's why you let him pass through at the cashier. That is in stark contrast with the fact that The Czech Republic limits access to the retained data to the police, a recognized authority for this purpose. The short retention period in Germany and Austria can be explained by their specific look at life spaces: the government should not intrude upon its citizens. This, however, does not explain the higher retention period and higher score on specificity for The Netherlands.

In some countries Trompenaars (1998) found that people accord status based on ascription and in others based on performance. This dimension splits the EU in eastern countries (Czech Republic, Bulgaria, Romania and Hungary) and western countries (UK, Norway, Netherlands, Ireland), but this doesn't correlate with differences found in the implementation of the Directive.

Trompenaars also distinguishes a dimension oriented to time. His data doesn't support the conclusion drawn from Hofstede's data that the short-term orientation of Germany and Austria are an important factor in setting their short retention period.

Finally, I couldn't find any proof linking the differences in implementation of the Directive to the amount of control the citizens of the different countries want to impose on nature, a cultural dimension identified by Trompenaars (1998)

In conclusion, the following cultural factors had an impact on the implementation of the Directive:

1. A low score on the **Power Distance Index (PDI)** translates into a shorter data retention period.
2. A high score on the **PDI** correlates with a longer data retention period.
3. A low score on the **PDI** and a high score on the **Individualism Index (IDV)** correlates with the national law being litigated at the constitutional court.
4. A high score on the **Masculinity Index (MAS)** correlates with litigation of the national law at the constitutional court, questioning the legality of the Directive and already having a data retention act in place.
5. A low score on the **Uncertainty Avoidance Index (UAI)** also correlates with already having a data retention act in place.
6. A low score on the **Long-Term Orientation Index (LTO)** translates in a lower data retention period.
7. A **universal regard** regarding laws translates into challenging the national law at the constitutional court, restricting access to the retained data with a court order and detailing which information to retain in the national act.
8. A country that scores very high on **individualism**, as defined by Trompenaars (1998) is likely to restrain access to the retained data to one or a few agencies.
9. Countries in which citizens have a more **specific view of life spaces** tend to have a shorter data retention period.

3.3 Follow-up

In this chapter I have looked at families of nations and cultural families to define the underlying cultural norms and values that explain the variance in the implementation of the European Data Retention Directive among the European Member States of the EU.

In the next chapter I will explore to what extent these cultural aspects differ between the European Union and the United States. This is a good prediction for how the implementation of a similar data retention directive would fare in the United States of America.

4. Cultural Differences Between the USA and the EU

There are cultural norms and values that underlie the implementations of the Directive amongst the European Member States. In this chapter I will compare these European cultural norms and values to the American norms and values. This results in an indication of how a data retention act would be implemented in the USA.

4.1 How do the Americans score on key cultural factors?

In the last chapter I described which cultural factors influenced the implementation of the Data Retention Directive in what way. How does the United States score on these factors and what does that mean for the policy transplantation? Note that these predictions are all relative to implementations by the European countries and not at all absolute.

- The United States **did not descend from a communist regime**. Therefore the implementation will not be as speedy, there is a small chance of a data retention act being present before a nationwide implementation takes place and the period of retaining data will be small.
- The United States has an **Anglo-Saxon law system** and is oriented at the United Kingdom and Ireland. Both these countries had a data retention act in place before the EU Directive was adopted. Considering this resemblance, I expect the USA to already have a sort of data retention act or program.
- There is **no incentive, such as prior horrors committed by misuse of the public administration records**, to have a minimal retention period of the data. Also, the USA has an Anglo-Saxon and not a German law system, decreasing the probability of having a minimal retention period.
- The United States **didn't inherit the large centralized government organizations** from the French legal system. Considering this, I do not expect that there will be a general agency overseeing the retention of data and access to the retained data.
- The countries that were early adopters of the European Union all have detailed descriptions of the data to be retained. As the United States was **never part of the European Union, this does not apply to them**.
- The United States of America **score average on the Power Distance Index**, much like the Netherlands, which has a period of 12 months. Considering this, I expect an average data retention period.
- On **the Individualism Index, the United States scores the highest**. This predicts that a data retention law will be challenged in the constitutional court, the Supreme Court of the United States.
- The USA **scores high on the Masculinity Index**, but not as high as the European countries where:
 1. The Directive was challenged at the constitutional court.
 2. The legality of the Directive was challenged at the European Court of Justice.
 3. Which already anticipated on the Directive by having a data retention act.
- On **the Uncertainty Avoidance Index, the USA scores low**, implicating that a form of data retention will be in place before it is officially made into a nationwide act.
- The USA has a short-term outlook, **scoring low on the Long-Term Orientation Index**. This translates into a low data retention period.
- The Americans have a **universal look** at the way laws and norms should apply to people. This predicts challenging of a data retention act at the Supreme Court,

restriction of access to the retained data to a single or few authorities and a detailed description of what information to retain.

- On **Trompenaars' (1998) individualism dimension, the United States also score high**, pointing towards restraining access to the retained data to a few agencies.
- The citizens of the United States **have a specific look at the different life areas**, predicting a shorter data retention period.

4.2 Predicting a potential implementation of data retention in the United States

If the United States would implement a data retention act, according to the cultural norms and values that influence the implementation in the EU, it would have the following characteristics:

1. The **period of data retention is average** (in Europe the average is 12 months) or shorter. However, the USA doesn't have the same incentives as Germany and Austria have to keep the retention period to a minimum.
2. **Access to the retained data is restrained** to a few agencies.
3. The **data retention act would most likely be challenged at the Supreme Court** of the United States.
4. Introduction of the data retention act would be **preceded by another form of a data retention act**.

Furthermore, I expect a **detailed description of the retained data in the act**, although this is not as clear as the factors mentioned above. When the act has a federal starting point, I expect that separate states will **question the legality of the act**.

In the next chapter I will look briefly at the legal differences between the EU and the USA that would influence said transplantation.

5. United States Law Concerning Data Retention

This paper examines the transplantation of the EU Data Retention Directive to the United States from a cross-cultural perspective. There are, however, national factors that also influence the acceptance of this transplant. These national factors include legal systems and specific laws. In chapter one I mentioned I would not deal with the differences between Common Law and Statutory Law.

In this chapter I provide a quick glimpse of the American legal aspects that would affect the implementation of data retention in the United States. Most of the examples and aspects are based on the work from Solove and Rotenberg (2003). These aspects are grouped by the four aspects mentioned in the previous paragraph.

5.1 Period of data retention by private parties and access to this data

The EU Data Retention Directive requires private parties to retain data of their customers.

The period that this data is retained is relevant for qualification of the type of data referenced in US law and the access mechanisms to the retained data. Communications in transmission are covered by the Wiretap Act, while communications in storage are covered by the Stored Communications Acts (SCA) (Solove & Rotenberg 2003). The Wiretap Act regulates the interception of information that is being transferred. This would apply to locational information. To obtain information from a wiretap, the government needs a court wiretapping order, which must be made under oath and must contain a variety of information. More important, the interception of the communication should be minimized (Rotenberg 2005). This contradicts the ongoing surveillance present in the EU Directive. Under the SCA, if the government wants to request data that has been in storage for 180 days or less, it must obtain a warrant supported by a probable cause. If the information has been stored for more than 180 days, the government has to put in more effort to get the data. It has to provide notice to the subscriber *ex ante* and obtain an administrative subpoena, a grand jury subpoena, a trial subpoena or a court order (Rotenberg 2005).

Regarding ISP records, the Electronic Communications Privacy Act (ECPA) would apply to the request of this data by law enforcement (Solove & Rotenberg 2003). The ECPA states that “[T]he government may require that an ISP provide stored communications and transactional records only if:

1. [I]t obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or
2. [I]t gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question (Solove & Rotenberg 2003, p.327).”

This suggests a court order, warrant or subpoena to restrict access to the retained information. However, the conditions under which such an order would be necessary are debatable. Solove and Rotenberg (2003) mention that in *United States v. Hambrick* (Michael 1999) the court judged that a user does not have a subjective expression of privacy when surfing the Internet with a nickname that is registered in the ISPs database. The court mentioned that the Fourth Amendment, which protects people against unreasonable searches and seizures, only applies when:

1. The citizen has manifested a subjective expression of privacy, and
2. The expectation is one that society accepts as “objectively reasonable.”

Apparently, the court found surfing the Internet with the same ID as is registered with an ISP not an objectively reasonable expectation of privacy, as the user cannot act as a

completely anonymous actor.

Access to the retained data for private parties is not restricted by the Fourth Amendment (Solove & Rotenberg 2003). In *United States v. Kennedy* (Belot 2000), the court ruled that as long as this search for information does not become government action, the private party can request ISP records. These may later be turned over to the government.

Concluding, the US government should get a court order for wiretapping and minimize the interception to the purpose for which the court order was sought. Access by the government to the retained data is regulated by US law, however it is debatable when and where the restrictions specifically apply. When a user has an expectation of privacy that society accepts as “objectively reasonable and when private parties can act as government actors is still unclear. These laws would restrict the access to the retained data and press for a short data retention period.

5.2 Data retention acts and legality of a new act

In 1998, the FBI has rolled out a system to intercept people’s e-mail and instant messaging information from their ISPs. This system, called Carnivore, was designed to locate the e-mails of a suspect when an ISP did not have the capacity to do so (Solove & Rotenberg 2003). To single out a suspect, Carnivore had to filter all the traffic at an ISP, thereby resembling the retention of data in Europe. The Electronic Privacy Information Center obtained information that mentioned that FBI discontinued Carnivore, because the ISPs can readily produce the information the FBI requires.

Under the Communications Assistance for Law Enforcement Act (CALEA), providers of broadband Internet service and telcos are required to isolate and intercept electronic communications and deliver them to law enforcement personnel when requested. This should be executed in a manner that protects the privacy and security of communications and call-identifying information not being intercepted (Solove & Rotenberg 2003).

The Fourth and Fifth amendments protect US Citizens against unreasonable searches and seizures and protect citizens of being a witness against themselves (Solove & Rotenberg 2003). These amendments should decrease the scope of data retention by ISPs and telcos.

In Fourth Amendment Law, the question of whether domestic security surveillance should be under less stringent procedures than surveillance for ordinary crime has long been unresolved (Solove & Rotenberg 2003). The Foreign Intelligence Surveillance Act (FISA) applies when foreign intelligence gathering is “a significant purpose” of the investigation. The data obtained under FISA cannot be shared with investigators of an ordinary crime, this is called the FISA wall. It is unclear how hard this wall is. Furthermore, the President has inherent constitutional power to conduct warrant-less foreign intelligence surveillance (United States Foreign Intelligence Surveillance Court of Review 2002).

Concluding, both the Carnivore program and CALEA can be seen as preambles of a data retention act as implemented in Europe. Although the Fourth and Fifth Amendment provide protection against unreasonable seizures and searches and being a witness against oneself, their applicability to domestic security surveillance is still being debated. Domestic security has been used as an argument for the European Data Retention Directive.

5.3 Detailing of data to be retained

Under FISA, the FBI can require the production of any tangible things for an investigation to protect against international terrorism or clandestine intelligence activities. Examples of these tangible things are books, records, papers, documents, and

other items (Solove & Rotenberg 2003). Although this list is detailed, it is unclear if this applies to electronic records as well.

The ECPA distinguishes between “content” and “envelope” information (Solove & Rotenberg 2003). The envelope contains information that the networks use for addressing and routing. Content is the information that is being conveyed. In general, content information is given stronger privacy protection under ECPA than envelope information. However, with Internet communications it is very unclear what part of the packet is content and what part is envelope. Arguing that the envelope content is similar to the packet header, would understate the privacy impacts of disseminating IP addresses, which could provide the path of how someone surfs the Internet.

Concluding, FISA provides a list of tangible things that the FBI can request and the ECPA gives stronger privacy protection to content than envelope information. Based hereon, I expect a public discussion about which data to be retained and how detailed this should be incorporated in the law.

5.4 Conclusion

The legal system of the United States and its laws influence the implementation of a data retention act. The most important aspects of the laws in the United States for data retention by ISPs and telcos are:

- **Access privileges:** government needs a court order for wiretapping and the interception of the communication should be minimized.
- **Access privileges:** communication data stored less than 180 days can be obtained by the government by a warrant, while information stored longer takes more effort to obtain.
- **Access privileges:** government access to ISP records is restricted by a warrant.
- **Access privileges:** private parties do not need warrants or court orders to get access to ISP records.
- The Carnivore program, specific parts of FISA and CALEA are both **preambles of a data retention act as implemented in Europe.**
- Fourth and Fifth Amendment provide constitutional protection against unreasonable search and seizure and being a witness against oneself. This would be in contradiction with the **compliance with national constitutional law** of an American data retention act.
- The United States has **somewhat detailed descriptions of what information law enforcement can access**, both under FISA and ECPA.

In the next chapter I will provide conclusions on the potential transplantation of the European Data Retention Directive to the United States.

6. Conclusions

In the previous chapters I examined the cultural norms and values that underlie the differences in implementation of the European Data Retention Directive between the Member States. These cultural norms and values are the independent variables that predict the implementation of a data retention act in the United States.

In this chapter I present the key differences in implementation in Europe, the cultural factors underlying these differences, how these cultural factors differ in the United States and United States law regarding data retention. Furthermore, I provide a synthesis of my findings and recommendations for further research.

6.1 Various European implementations of the Directive

As of June 2008, five Member States have implemented the EU Directive, while two others are challenging the legality of the Directive at the European Court of Justice. The speed of implementation differs per Member State. Ireland and Slovakia have challenged the legality of the European Data Retention Directive. In other Member States, the national act is challenged at the national constitutional court. Some of the countries where the Directive is not found to be contrasting with the constitution already had data retention acts in place, such as the UK, Poland, Estonia and Ireland. The period of data retention varies per Member State (from 6 to 24 months) and some countries have restricted access to the retained data to specific agencies or by court orders. The last key difference in the implementation is the amount of detail in the law about the types of data that should be retained.

6.2 Cultural factors explaining differences in implementation

The differences in implementations can be explained by differences in cultural norms and values between countries.

Some of the Member States share a common lineage (De Jong et al. 2002), that explains their implementations. Descent from a communist regime correlates with a speedier implementation, the presence of an ex ante data retention act and a long data retention period. An Atlantic orientation and the presence of an Anglo-Saxon public law system account for a form of data retention before the EU Directive was adopted. A minimum data retention period is explained by countries' involvement in prior atrocities made possible by accurate public administration. Belgium and France have centralized their retention activities and the access to the retained data, something that can be explained as an inheritance from the French legal system. Most Member States that adopted the European Union in an early stage have a detailed description in their national law of what data to be retained.

Another way of explaining the cultural differences is by looking at how the different implementations correlate with the cultural dimensions that Hofstede (2005) found in his research. A low or high score on the Power Distance Index, which defines the dependence of people of lower rank on people of higher rank, correlates with respectively a shorter or longer data retention period. In an individualist culture, measured by a high score on the Individualism Index, citizens will more likely challenge the directive at the national court. This challenging also correlates with a high score on the Masculinity Index (MAS), which suggests big differences in gender roles. The high MAS score also predicts a questioning of the legality of the Directive and a data retention act ex ante. A low score on the Uncertainty Avoidance Index (UAI) means that citizens do not feel anxiety in the prospect of an uncertain future. This contradicts with the fact that countries with a low UAI have a data retention act dating from before the EU Directive. A low score on Long-Term Orientation Index, meaning that citizens have a short-term outlook on life, indicates a shorter data retention period.

Trompenaars (1998) defined different cultural dimensions separate from Hofstede. Applying his research to the directive, I conclude that cultures that consider laws as universally applicable challenge the law at their constitutional court, question the legality of the Directive and might have an ex ante data retention act. A country that scores very high score on Trompenaars' individualism index will constrain the access to the retained data to one or a few agencies. Countries in which citizens have a more specific view of life spaces tend to have a shorter data retention period.

6.3 Cultural differences and similarities concerning data retention between the United States of America and the European Union

Cultural norms and values underlie the differences between the United States and the European Union. By identifying these cultural differences, I can predict how a data retention act would look like according to cultural norms and values. The United States has an Anglo-Saxon law system and scores average on the Power Distance Index. However it scores highest on the Individualism Index, and very high on the Masculinity Index. The United States scores low on the Uncertainty Avoidance Index and its citizens have a short-term outlook, scoring low on the Long-Term Orientation Index. On Trompenaars' individualism dimension (1998), the USA also scores high. Furthermore, Americans have a very specific look at the different life spaces.

Considering these cultural differences between the USA and the EU, an American data retention act would have the following characteristics: the data should be retained for an average to short period and access to the data is restrained to a few agencies. I expect that a new data retention act will be based upon former data retention acts and activities. Also, I expect that the data retention act will be challenged at the Supreme Court of the USA. Cultural norms and values also point at a detailed description of the data to be retained and questioning of the legality of the act by the different states.

6.4 United States law regarding data retention

The differences in cultural norms and values predict how a data retention act in the USA would be formed. Next to that, cultural norms and values can be formalized in national laws. A review of American laws leads to the following conclusions about how the American legal system influences the data retention: it is most likely that access to the data, which would likely fall under the Stored Data Communications Act, is restricted by court order, warrant or subpoena. I expect that a new data retention act will be building on the earlier data collection program Carnivore, the data collection allowed by the Communications Assistance for Law Enforcement Act and the Foreign Intelligence Surveillance Act.

However, American laws provide protection against the collection and retention of data. The Fourth and Fifth amendment will place restrictions on the data retention act by protecting citizens against unreasonable search and seizure and being a witness against oneself. Furthermore, based on the detailing of other American laws, I expect that the data to be retained will be detailed in the data retention act.

I did not find any data in American laws concerning a data retention period and the questioning of federal laws by the different states. Based on the research I expect a data retention act in the USA to have a short to average data retention period. Furthermore, I expect that the different states question a federal law of this type.

6.5 Synthesis

Implementation of a data retention directive would follow the general outline sketched in paragraph 6.4. De Jong et al. (2002) provide guidelines to estimate the acceptance of a policy transplant. Although the framework that they provide is constructed for ex post evaluation, the hypotheses that they validated provide fruitful insight for the acceptance

of the Directive's transplant.

The most obvious guideline is that system upheaval or performance crisis makes the acceptance easier. In paragraph 3.2 I already concluded that the 9/11 attacks and the London and Madrid bombing have increased the acceptance of data retention in Europe. This also significantly increases the acceptance of data retention in Europe.

De Jong et al. (2002) find that Xeroxing (exactly copying) the transplant makes the acceptance less likely. This is consistent with the findings that USA law will influence the data retention act, as mentioned in paragraph 6.4. This process is called 'bricolage.'

Considering only one clear model will make success of the transplant less likely (De Jong et al. 2002). In this respect, the idea of data retention is the only means being considered for gathering intelligence on terrorists. This decreases the acceptability of the transplant.

A transplant with a generic character is easily accepted (De Jong et al. 2002). In that respect, the idea of data retention as mentioned in the EU Directive is very generic and can be implemented however Member States wish. This is the cause of the differences in implementation across Member States. The acceptance of the Directive amongst Member States might also be less than the acceptance of the US states to implement federal law, because the latter have been forming a country for a longer period. This will increase the acceptance of data retention in the USA.

To conclude, I expect that data retention as a European transplant will have a good probability of being accepted. The transplant does have to reside in the United States and therefore will be shaped by the American cultural norms and values.

6.6 Recommendations for further research

Because of time constraints, it was impossible to find relevant data on all European Member States. I recommend to make the data set complete, by including more information on the Republic of Cyprus, Finland, Greece, Latvia, Luxembourg, Malta, Portugal and Spain.

Furthermore, the survey of American laws presented in chapter five only touched slightly upon the most important legal aspects for data retention. I recommend to spend more time on the legal analysis of data retention in the USA and incorporate American issues surrounding data retention.

References

2002. British liberty, RIP. Government snoopers must be stopped. Available at: <http://www.guardian.co.uk/Archive/Article/0,4273,4431010,00.html> [Accessed June 24, 2008].
2007. Data retention for one year for UK telecom companies. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.15/data-retention-UK> [Accessed June 13, 2008].
2005. Data retention: Council barks but cannot bite. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number3.21/retention> [Accessed June 14, 2008].
- 2007a. First draft on data retention law in Romania. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.9/data-retention-romania> [Accessed June 13, 2008].
- 2007b. French Government Decree on data retention - another Big Brother act. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.8/france-data-retention> [Accessed June 13, 2008].
- 2007c. PHR2006 - Republic of Estonia. Available at: <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559541> [Accessed June 15, 2008].
2008. German data retention act challenged. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.1/germany-data-retention> [Accessed June 13, 2008].
- 2005a. German industry position paper against data retention. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number3.17/dataretention> [Accessed June 14, 2008].
- 2007d. German Parliament adopted the data retention law. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.22/german-retention-law> [Accessed June 13, 2008].
- 2005b. Italy decrees data retention until 31 December 2007. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number3.16/Italy> [Accessed June 14, 2008].
2004. PHR2004 - The Republic of Lithuania. Available at: <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83771>

[Accessed June 15, 2008].

- 2008a. Romanian Govt adopts Data retention law, but calls it inefficient. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.4/romania-data-retention> [Accessed June 12, 2008].
- 2007e. The Austrian government has postponed the law for data retention. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.13/austria-data-retention> [Accessed June 13, 2008].
- 2007f. The French Ministry of Interior has a new interception platform. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.11/french-interior-interception> [Accessed June 13, 2008].
- 2007g. Traffic data could be retained for one year in Spain. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.14/data-retention-spain> [Accessed June 13, 2008].
- 2007h. UK implements the Data Retention Directive. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.10/uk-data-retention> [Accessed June 13, 2008].
- 2005c. UK urging e-mail data retention. BBC. Available at: http://news.bbc.co.uk/2/hi/uk_news/politics/4668903.stm [Accessed June 24, 2008].
- Allen, A., 2007. *Privacy law and society*, [St. Paul Minn.]: Thomson/West.
- Anderson, R., 2008. UK Government will store all phone, Internet traffic data. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.10/uk-isp-traffic-data> [Accessed June 12, 2008].
- Article 29 Data Protection Working Party, 2007. *10th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2006.*, Available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm [Accessed May 9, 2008].
- Article 29 Data Protection Working Party, 2006. Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm [Accessed May 9, 2008].

Belot, J., 2000. United States v. Kennedy,

Bendrath, R., 2006. German Parliament rejects motion against data retention. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number4.12/germandataretention> [Accessed June 14, 2008].

Broache, A., 2006. U.S. attorney general calls for 'reasonable' data retention. *CNET News.com*. Available at: http://bellsouth.com.com/U.S.+attorney+general+calls+for+reasonable+data+retention/2100-1030_3-6063185.html [Accessed May 9, 2008].

De Jong, W.M., Lalenis, K. & Mamadouh, V., 2002. *The Theory and Practice of Institutional Transplantation: Experiences with the Transfer of Policy Institutions*, Kluwer Academic Publishers.

EPIC, 2007. International Data Retention Page. Available at: http://epic.org/privacy/intl/data_retention.html [Accessed May 9, 2008].

Foldes, A., 2008. Hungarian Data Retention Law - challenged at the Constitutional Court. European Digital Rights Initiative. Available at: <http://www.edri.org/edriagram/number6.11/hungary-data-retention-constitutional> [Accessed June 11, 2008].

Glorioso, A., 2006. New law proposal on data retention submitted in Italy. European Digital Rights Initiative. Available at: <http://www.edri.org/edriagram/number4.22/data-retention-it> [Accessed June 13, 2008].

Grancharova, E., 2008. Protests in Sofia against data retention directive - News news. *Sofia Echo.com*. Available at: http://www.sofiaecho.com/article/protests-in-sofia-against-data-retention-directive/id_27465/catid_66 [Accessed June 15, 2008].

Hermida, A., 2006. UK rapped on data retention law. *BBC*. Available at: <http://news.bbc.co.uk/1/hi/technology/4744304.stm> [Accessed May 9, 2008].

Hofstede, G.J., 2005. *Cultures and Organizations: Software of the Mind*, McGraw-Hill Professional.

Hunter, P., 2006. ISP data retention becomes a reality. *Computer Fraud & Security*, 2006(4), 17-18.

Joergensen, R.F., 2006. Draft Administrative Order on data retention in Denmark. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number4.14/denmark> [Accessed June 14, 2008].

- Joergensen, R.F., 2008. Key privacy concerns in Denmark 2007. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.2/privacy-denmark-2007> [Accessed June 13, 2008].
- Kuner, C., 2007. *European Data Protection Law: Corporate Regulation and Compliance* 2nd ed., Oxford University Press, USA.
- Loughlin, J., 1994. Nation, state and region in Western Europe. In L. Bekemans, ed. *Culture: Building stone for Europe 2002*. Brussels: European Interuniversity press, pp. 229-248.
- Loughlin, J. & Peters, B., 1997. State traditions, administrative reform and regionalization. In J. Loughlin & M. Keating, eds. *The Political Economy of Regionalism*. London: Frank Cass, pp. 41-62.
- Marzouki, M., 2006. Telecom data to be retained for one year in France | EDRI. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number4.6/franceretantion> [Accessed June 14, 2008].
- McCullagh, D., 2006. Congress may consider mandatory ISP snooping - CNET News.com. *CNET News.com*. Available at: http://www.news.com/Congress-may-consider-mandatory-ISP-snooping/2100-1028_3-6066608.html [Accessed May 9, 2008].
- McCullagh, D., 2008. FBI, politicians renew push for ISP data retention laws | The Iconoclast - politics, law, and technology - CNET News.com. *CNET News.com*. Available at: http://www.news.com/8301-13578_3-9926803-38.html [Accessed May 9, 2008].
- McIntyre, T., 2008. Key privacy concerns in Ireland 2007 . Available at: <http://www.edri.org/edriagram/number6.2/privacy-ireland-2007> [Accessed June 12, 2008].
- Merryman, J. & Perez-Perdomo, R., 2007. *The Civil Law Tradition: An Introduction to the Legal Systems of Europe and Latin America*, Stanford University Press.
- Michael, J., 1999. *U.S. v. Hambrick*,
- Pospipil, F., 2006. Dispute over data retention costs in Czech Republic. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number4.3/czechdataretention> [Accessed June 14, 2008].
- Pospipil, F. & Tichy, M., 2008. Key privacy concerns in Czech Republic 2007. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.2/privacy-czech-2007> [Accessed June 13, 2008].

Richard, M., 2001. Prepared statement of the United States of America. Presented at EU Forum on Cybercrime, Brussels.

Solove, D.J. & Rotenberg, M., 2003. *Information Privacy Law*, Aspen Publishers.

Svatosova, H., 2008. Czech Parliament - close in implementing data retention directive. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.11/czech-data-retention> [Accessed June 11, 2008].

Therborn, G., 1993. Beyond the lonely nation state. In: F.G. Castles (Ed.). *Family of nations. Patterns of public policy in Western Democracies* (pp. 329-340). Dartmouth: Aldershot.

Trompenaars, F., Trompenaars, A. & Hampden-Turner, C., 1998. *Riding the Waves of Culture: Understanding Cultural Diversity in Global Business*, McGraw-Hill Professional.

United States Foreign Intelligence Surveillance Court of Review., 2002. In re Sealed Case,

Van Hoboken, J., 2007. Dutch DPA advises negatively on Dutch draft data retention. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number5.2/dpa-dutch> [Accessed June 13, 2008].

Van Hoboken, J., 2008. Dutch Parliament lowers data retention term to 12 months. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number6.11/nl-data-retention-12-months> [Accessed June 11, 2008].

Waglowski, P.V. & Majewski, W., 2005. Polish plans for 15 years mandatory data retention. *European Digital Rights Initiative*. Available at: <http://www.edri.org/edriagram/number3.24/Poland> [Accessed June 14, 2008].

Appendix A – Implementation per Member State

This appendix describes the process of implementation of the European Data Retention Directive and related processes in the various Member States.

Austria

Announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

In July 2007, the Austrian government said that “[T]here is no way to have data retention ready before the deadline set by the directive.” The proposed retention period of the retained data is 6 months (2007e).

Belgium

Announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

The coordinating body of threats (OCAM) can collect and retain data for 30 years. The purpose of the collection of data by OCAM should be to evaluate terrorist and extremist threat (Article 29 Data Protection Working Party 2007).

Bulgaria

The directive for data retention in Bulgaria went in to effect on February 2, 2008. It requires Internet Service Providers and telecom companies to collect data from their clients and retain this data for 12 months (Grancharova 2008).

Czech Republic

The Czech Republic already adopted a data retention law in the middle of 2005, anticipating on the EU Directive for Data Retention. This declared a minimum retention period for 3 to 6 months and a maximum retention period of 12 months. There still is a discussion about the amount of the reimbursements for the ISPs. These would compensate for the extra costs that come with data retention (Pospipil 2006).

Announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

In 2006, the data retention act was updated. Anonymous sources mention that the police used the data routinely for investigation in 2007, but there are no statistics about this (Pospipil & Tichy 2008).

In 2008, the Minister of Industry and Trade proposed to enhance the access for secret service and military intelligence, but this has not been implemented yet (Pospipil & Tichy 2008).

The period for retaining the data is 1 year (Svatosova 2008).

The specific data that are subject to retention are not included in the bill. This bill was proposed by the Minister of Transportation. The bill didn't mention reimbursement of costs for ISPs and telcos (Svatosova 2008).

IuRe, the Czech privacy activist group, has proposed an amendment about access the retained data being constrained to the police only. The majority of the parliament voted for this amendment (Svatosova 2008).

Republic of Cyprus

The Republic of Cyprus announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

Denmark

Denmark has released a draft proposal on the August 10, 2006. This proposal also foresees in the collection of Internet session data. It includes a detailed description about which data to retain. The data to be collected is not limited to data that ISPs or telcos already generate for billing purposes. (Joergensen 2006).

The retention period is one year (Joergensen 2006).

The draft proposal was implemented on September 15, 2007 after being approved on September 28, 2007. It goes further than the EU directive in that it also includes session logging. However, it applies only to commercial ISPs. The act details the data to be retained (Joergensen 2008).

Estonia

The Republic of Cyprus announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

Estonia installed a new Telecommunication Act in 2005 and the implementation of the EU Data Retention Directive in this act is foreseen after the initial EU deadline (2007c).

Finland

Finland announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

France

France announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

The draft decree for telecommunication data retention was made public on March 26, 2006. Collected data should be retained for one year. The data to be retained is defined as: "[T]he user and its terminal equipment - the recipients of the communication - the date, time and duration of the communication - the additional services used and their suppliers - the origin and the location of the communication (for telephony services)." The decree foresees in reimbursement of the costs for law enforcement agencies, but not for ISPs. Everyone providing access to the Internet for others should retain data (Marzouki 2006).

In April 2007, the government issued a new draft decree for the retention of data by web masters, hosting companies, mobile and fixed telcos and Internet service providers to retain all data concerning communication of their customers. The data retention period is one year. It is unclear from the proposal what the nature of the data is the telcos should retain. After the police obtains the data, it can keep the records for another period of three years (2007b).

On May 2, 2007, the French Ministry of Interior operated a new system, designed to intercept communication data related to text messages, mobile or Internet. Uclat, the coordinating center for antiterrorism, operates it (2007f).

A new proposal for data retention, based on the Sarkozy law adopted on January 23, 2006, states that Internet providers, Internet cafes, hosting providers and operators must communicate traffic data the authorized government agencies (2007b).

The French Justice system is said to be working on an own system to monitor SMS and phone calls. (2007b)

Germany

In August 2005, the general German industry association (BDI) and the two telecommunication associations (BITKOM and VATM) published a paper with demands for data retention legislation. "The industry mentions 5 more specific demands on both Commission and Council:

1) Any period, if the necessity can be proven, must not exceed 6 months; 2) Any obligation to retain data must not include data types currently not centrally processed and recorded within the networks; 3) Any obligation can only address services provided directly by the provider of a customer; 4) Full cost reimbursement for both infrastructure and operational costs, in stead of the vague wording of 'additional costs'; 5) No additional obligation on the industry to collect statistics. " (2005a)

Germany also announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

German opposition filed a motion to join Slovakia and Ireland in the appeal at the European Court of Justice, but this was however not supported by parliament. (Bendrath 2006). This German motion stated that "[T]he data retention decision should have been made in the 'Third Pillar' of the European Union structure, as the sole purpose of retention of the data is law enforcement. Therefore, the proper legislative procedure should have been a framework directive, which gives more power to national Parliaments and requires an unanimous vote on the EU Council of Ministers." (Bendrath 2006).

The law concerning data retention was adopted on November 9, 2007, as amendment to the current wiretapping legislation. The data should be retained for 6 months. Providers of anonymization services are also obliged to retain. The police, court and state prosecutors need court orders to access the retained data, intelligence services have access without restriction. There is no mention of special requirements in the case of confidential relationships in professional contexts (2007d).

The German data retention law entered into force on January 1, 2008. The German working group on data retention challenged the law at the Federal German Constitutional Court on January 6. They claim it is unconstitutional, because it is treating every citizen as a potential delinquent. They also state that the law would severely disrupt free communication (2008).

The regional court of Darmstadt ruled that Internet access providers are in principle no longer allowed to store their flat-rate customers' IP addresses. The Federal German Constitutional Court in preliminary decision limited the use of the retained data. It can only be transferred to law enforcement authorities in cases of serious crimes and with a judicial warrant. Also, it asked for a government report on practical effects of data retention (Article 29 Data Protection Working Party 2007).

Greece

Greece also announced to make use of the option to postpone implementation of the Directive (Kuner 2007).

Hungary

The Hungarian data Retention Law is challenged at the constitutional court by the Hungarian Civil Liberties Union. Their case is based on the omission in the law of the legal purposes of data processing. The purpose for collecting the data is wider than just for serious crime. The Hungarian Constitutional Court in 1991 prohibited data processing without previously defined purposes (Foldes 2008).

Ireland

In 2005, Ireland already had a data retention law for telephone data with a retention period of 3 years (2005).

Ireland voted against the Directive in the final decision in February 2006. Furthermore, it challenged the Directive before the European Court of Justice. The Irish government challenged the validity of the law. They argue it should have been a Framework Directive under the third pillar, the 'Police and Judicial [Cooperation] in Criminal Matters' (Bendrath 2006).

Irish NGOs litigate against the act. They state the act breaches the right of privacy (Irish law and EU Convention), has chilling effect on freedom of expression, and interferes with the right to travel by retaining the mobile phone location of citizens (McIntyre 2008).

The implementation of the law is done by order of the Minister, not by legislation passed by Parliament (Article 29 Data Protection Working Party 2007).

Italy

On July 2005, the Italian government published a decree about the retention of data by mobile telecommunication providers for at least two years and for Internet providers for six months. It also contained compulsory identification for mobile phone buyers, users of Internet cafes and users of Wi-Fi spots. Deputy public prosecutor can request the data, but this has to be approved within 48 hours of the receipt of the data by an investigative judge (2005b).

Italy has a data retention law for telephone data with a period of 4 years (2005b).

In November 2006, a new law proposal on data retention was submitted by the Winston Smith Project, making deletion of data the rule. It also stated that automatically collected data shall no be longer retained than strictly necessary to achieve the goal for which the collection took place in the first place (Glorioso 2006).

Italy's privacy watchdog, Garante, wrote an opinion about collection and retention of data included in the national register of the entities authorized to apply medically assisted reproduction techniques (Article 29 Data Protection Working Party 2007).

The Italian Constitutional Court ruled that using traffic data for purposes other than the fight against Mafia-type crime and terrorism, upon expiry of the retention period, is not unconstitutional (Article 29 Data Protection Working Party 2007).

Garante also addressed the retention period of so-called positive information, data concerning positive financial information, such as regular payments and good financial behavior. They stated that the maximum retention period may not be more than 36 months in these cases (Article 29 Data Protection Working Party 2007).

Garante also proposed a limited retention period of 72 hours for storage of a users ID with e-ticketing (Article 29 Data Protection Working Party 2007).

Latvia

Latvia announced to make use of the option to postpone implementation of the Directive to 15 March 2009 (Kuner 2007).

Lithuania

The Lithuanian Constitutional Court ruled that the retaining of data by telcos and ISPs should be strictly limited to data that is already retained for ISPs ordinary business activities. The data retention measures that the Law on Telecommunications proposed therefore never came into effect. Resolution number 290 of March 5, 2003, requires hosting providers to retain data related to and the content of their hosting services. This is also limited to data already retained for regular business purposes, because of the ruling of the Constitutional Court (2004).

Lithuania announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

Luxembourg

Luxembourg announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

Malta

Malta announced to make use of the option to postpone implementation of the Directive

to March 15, 2009 (Kuner 2007).

Netherlands

The Netherlands also announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

A draft proposal for the law on data retention was made public on December 21, 2006. The Dutch Data Protection Agency (DPA) stated that this proposal disregards the requirements of article 8 of the European Convention on Human Rights, the fundamental right to respect of one's private life (Van Hoboken 2007). The Dutch Data Protection Authority advised negatively on this draft, because it requires location data of mobile phones to be collected during the call, while the EU Directive only mentions data to be collected during the initiation of the call. Also, the proposal doesn't contain the specific description of the data to be retained (Article 29 Data Protection Working Party 2007). The proposed retention period is 18 months. The proposal also mentions retaining mobile telephone location data during the call, which goes further than EU directive. The DPA proposed limitations on access to retained data and reports on the statistics about the usage of data by law enforcement (Van Hoboken 2007).

The retention period of the law to be implemented is 12 months. The law doesn't mention that for e-mail or telephone data only the destination has to be retained, as the EU Directive does. The general costs that ISPs and telcos make will not be reimbursed. The data should be stored by the providers. Government agencies can claim complete parts of the collection to be retained. From now on, the Senate still has to approve the law (Van Hoboken 2008).

Poland

Poland announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

In December 2005, the Polish leader of governing party called for a new data retention law, retaining data for 15 years (Waglowski & Majewski 2005).

Poland has amended their Telecommunications Law, extending the period of data retention for traffic data from one to two years (Article 29 Data Protection Working Party 2007).

Portugal

No information available.

Romania

A draft of the data retention law was presented in April 2007 by the Ministry of Communications and Information Technology. It mentions that the data should not be retained by operators. Only electronic communication operators that have notified the Regulatory Authority should retain data (2007a).

The retained data can be accessed by prosecutors only in the penal cases related to organized crimes and terrorism. In case of a threat for national security, specific bodies, as explained in the laws on national security, are also allowed to access the retained data. (2007a)

The government adopted the draft law on data retention on February 20, 2008. The proposed retention period in this law is one year. The law was not adopted as Emergency Ordinance, as proposed in December 2007. Access to the data is only for prosecutors in penal cases related to organized crime and terrorism. They should have a proper judge-approved access authorization. There is still public confusion regarding the access for the security services to the retained data. In criticism on the law, the responsible Minister says however that obtaining data for email will not increase the

chances of discovering the crimes. (2008a).

Slovakia

Slovakia voted, together with Ireland, against the directive in the final decision in February 2006. Both countries hold a case before the European Court of Justice. They argue it should have been a Framework Directive under the third pillar, the 'Police and Judicial [Cooperation] in Criminal Matters' (Bendrath 2006).

The Office for Personal Data Protection in Slovakia commented on the data retention period mentioned in the Act of Banks (Article 29 Data Protection Working Party 2007).

Slovenia

Slovenia also announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

Slovenia implemented the data retention act as an amendment to the Electronic Communications Act. This amendment required Slovenian providers of communication servers to retain all traffic data created through their customers' activities for two years (Article 29 Data Protection Working Party 2007).

Spain

The retention period of data in Spain is one year. The data can be accessed by law enforcement and secret service only under court order (2007g).

Sweden

Spain announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

The Swedish Minister of Justice assigned a Commission of Inquiry with the task of reviewing the national legislation to propose the amendments required (Article 29 Data Protection Working Party 2007).

United Kingdom

The United Kingdom announced to make use of the option to postpone implementation of the Directive to March 15, 2009 (Kuner 2007).

In the United Kingdom, the voluntary code in which ISPs guarantee to retain data, is transferred into a binding law. The retained data can be requested by government agencies and be used for any crime. The data can be obtained without existing court proceedings and can be available to anyone who can convince the court they have a right to access them. The government proposes to compensate for the compliance costs and litigants should pay for the disclosure of documents they request (2007h).

The law to retain telephone data is approved on July 24, 2007. It binds telcos to retention of phone call logs. The retention period of this data is one year. Access to this data is guaranteed for security services (2007).

In 2008, Gordon Brown has proposed to store all traffic, itemized phone bills, mobile phone records and Internet traffic logs. This data is to be collected and stored in a central government database. The UK Regulation and Investigatory Powers Act enables public officials of 702 to obtain traffic data from service providers (Anderson 2008).