Quantifying Key Characteristics of 71 Data Protection Laws

by **Bernold Nieuwesteeg***

Abstract: This paper presents a pioneering study that unlocks six characteristics in the literal text of 71 Data Protection Laws (DPLs). The characteristics are: the type of collection requirements; the presence of data protection authorities; data protection officers; data breach notification laws; monetary-; and criminal penalties. The quantification allows comparison of data protection laws with each other, such as a potential federal U.S. DPL with European DPLs. It can also be used for empirical legal research in information security by linking the data to other variables, for instance, deep packet inspection. There are some noteworthy initial results: only 5 out of 71 DPLs have penalties for non-compliance that exceed 1 million euro. Moreover, compared to the United States (US), few countries (21 out of 71) have data breach notification laws. Principal component analysis reveals that the six characteristics can be grouped in two unobserved factors, which explain 'basic characteristics' across laws and 'add-ons' to these characteristics. By combining these two factors a privacy index is constructed. Moreover, countries that are not known for their stringent privacy control such as Mauritius and Mexico occupy a top position in this index. Member States of the European Union have DPLs with a privacy control score above average but hold no absolute top position. It is hoped that these findings will open avenues for new research, such as adding more characteristics to the database and further quantification of (internet) law.

Keywords: Data Protection Laws; comparative law; privacy control; quantitative text analysis; empirical legal analysis

Recommended citation: Bernold Nieuwesteeg, Quantifying Key Characteristics of 71 Data Protection Laws, 7 (2016) JIPITEC 182 para 1.

A. Introduction

1 This paper codes six key characteristics of 71 Data Protection Laws (DPLs). The following six characteristics are selected from the perspective of privacy control: 1.) the type of collection requirements and the presence of 2.) data protection authorities, 3.) data protection officers and 4.) data breach notification laws and 5.) monetary- and 6.) criminal penalties. Hereafter a principal component analysis is performed and two underlying factors are distinguished: 'basic characteristics' in the law and 'add-ons'. Subsequently, by combining these two underlying factors, a privacy control index is created. This research is, to the best of my knowledge, the first analysis to look at six key elements of data protection laws in 71 countries. The dataset consists of all continents and 70% of the world population.

2 By quantifying elements of the law, it can be unlocked for statistical analysis. Quantification provides an overview of DPLs and coded characteristics across countries. This has benefits for economists, policy makers and legal scholars. Economists benefit because they can measure the effect of data protection legislation on information security by relating the index of underlying variables with proxies for privacy control. An example is the intensity of deep packet inspection (DPI), for which quantitative data is available. Policy makers could be

curious whether the perception of privacy control by individuals matches actual stringency in the law such as the height of penalties. Moreover, policy organizations that try to map different aspects of Internet governance and regulation are potentially assisted by an overview of privacy control in DPLs.[1] Legal scholars and practitioners can benefit because the privacy control index gives them a quick overview of privacy control in different countries. The following insights were obtained:

- Only 5 out of 71 countries have a maximum penalty for non-compliance above 1 million euro. Although the threshold of 1 million euro is obviously arbitrary, penalties (far) below this amount possibly have a limited deterrent effect on non-compliance with the law, especially when considering the low likelihood of detection. Hence, it seems that most DPLs have a limited deterrent effect.

- Only 21 out of 71 countries have an obligation to notify data breaches, while in the US, 47 out of 50 states have such a Data Breach Notification Law.

- Approximately half the DPLs I analyzed have criminalized non-compliance with the DPL.

- Two unobservable factors explain variance within two sets of characteristics; I call these 'basic characteristics' and 'add-ons'.

- There are some unusual suspects in the top of the privacy index (the sum of the individual characteristics), such as Mauritius, Mexico and South Africa.

3 This introduction first addresses developments of DPLs in the US and the rest of the world. Hereafter, the law and economics of DPLs are introduced briefly. Next, the limitations of this study are addressed.

I. Developments in Data Protection Laws in the U.S. and the world

4 Recently, there has been a significant amount of attention on US data protection standards by legislators, organizations and privacy advocates. On June 1 2015, the United States congress allowed crucial parts of the US Patriot act expire. One of the key elements of the Patriot act - the extensive powers of the National Security Agency to collect personal data on a large scale - was terminated. On June 8 2015, the G7 discussed the implementation of the Transatlantic Trade and Investment Partnership (TTIP) at their annual conference in Bavaria, Germany. The differences in data protection law between the European Union (EU) and US was a central topic at this conference. According to experts, the risk of infringement of EU data protection standards by US companies could hinder the entry into force of TTIP.[2] Companies in the US have different data protection standards because of differences in data protection regulation between the EU and U.S. For instance, on October 6 2015, the European Court of Justice declared the US safe harbor regulation, which enables free flow of data between the US and EU invalid because of the existence of different data protection standards.[3] Also outside the EU, DPLs are becoming ubiquitous. By September 2013, 101 countries had implemented a data protection law.[4] In addition to that, in 2013, more than 20 privacy regulations were under consideration by other governments.

5 In the US, data protection regulation is scattered over sectors and states. Therefore, on March 25 2015 the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade proposed a federal data breach notification law, the Data Security and Breach Notification Act of 2015. However, this federal law has been criticized for being "less stringent than many state laws".[5]

6 This paper argues that it is necessary to identify other DPLs outside of the US to foster the design of a federal law. US DPLs inherently interact with other DPLs in the world. Not only because of the borderless nature of the Internet, but also because major US companies such as Amazon, Google, Facebook and Microsoft have a large influence over the Internet. For instance, in 2014, 13 of the 20 largest Internet companies by revenue were American. None were European. The fact that current US data protection law differs from other countries is well known. However, there is a knowledge gap in systematic oversight of the key elements of DPLs in other countries. There is a scientific and societal demand to map those differences between those laws and analyze them. Accordingly, this paper aims to answer the following research question:

1 Organizations such as the webindex [<http://thewebindex.org>] of the World Wide Web Foundation, the privacy index [<https://www.privacyinternational.org>] of privacy rights international and the United Nations [<http://www.unodc.org>] have been striving for categorizing different aspects of cybersecurity and cybercrime.

2 M. Pérez. 'Data protection and privacy must be excluded from TTIP' (2015) EDRi.

3 Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner.

4 G. Greenleaf. 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) Journal of Law, Information and Science, Special Edition, Privacy in the Social Networking World.

5 S. Breitenbach. 'States at odds with feds on data breach proposals' (2015) Stateline.

7 *How do countries outside the U.S. design their data protection laws with respect to key elements such as consent, the presence of data protection authorities and penalties for non-compliance?*

II. The law and economics of Data Protection Laws

8 DPLs aim to reduce market failures in the information security and privacy market. The cost of a personal data breach is not fully internalized by an organization that invests in cyber security - externalities exist. Therefore there are incentives to under-invest in data protection. Moreover, "[data collection enables] authorities or businesses to monitor the habits and movements of individuals in the quest for anomalies, performance or profit".[6] Thus, commercial use of personal information benefits organizations.[7] On the other hand, this data collection damages (rights of) consumers when they do not want this data to be disclosed. Recently, there was intensive public debate about Facebook privacy settings[8], judicial decisions such as the Google Case (the right to be forgotten)[9] and Google Glass.[10] These events illustrate that organizations might have insufficient incentives to give customers privacy control. In this situation, the market fails in reaching a socially desirable situation. Hence, DPLs are adopted to correct this market failure and ensure a minimal level of control and protection. DPLs do this by obligating organizations to protect the data of consumers, update consumers about the usage of their data, and allow consumers to alter the user rights of these organizations.

III. The limitations of this study

9 This research has some inherent limitations, which are necessary to outline upfront. First, it is important to note that I quantify elements from the *literal text* of the law.[11] Hence, the eventual index created is a proxy for *de jure* privacy control of DPLs. *De jure* privacy control is different from *de facto* (real) privacy control, which is the real control people have over their personal data. Most probably, *de jure* privacy control affects real *de facto* privacy control. But there are also other factors that (might) affect *de facto* privacy control; for example, but not limited to:

- The *de facto* (actual) enforcement of DPLs by the authorities, the number of security audits, their capacity and budget;
- Internet usage per capita;
- The number of virus scanners installed;
- The number of data breaches per year;
- ...

10 These and many other factors influence real privacy control. Some of them cannot even be observed directly.[12] The impossibility to observe and quantify an exhaustive list of elements that together form de facto privacy control[13] ensures that the focus of this research relies on observable de jure privacy control. Hence, this research does not quantify the legal aspects of DPLs outside the literal text of the law. I also do not consider the sociological and political background of the countries that have adopted DPLs; for instance, governmental access to medical, financial and movement data, data retention and transborder issues. Privacy International analyses and groups these aspects of privacy per country.[14] Within the DPL, six characteristics based on four criteria are selected. This means that this paper omits other characteristics of DPLs - for instance the general requirement for fair and lawful processing of personal data. A long-list of other characteristics of DPLs is displayed in the appendix. A final limitation of this research is that U.S. DPLs are not considered since these laws are very fragmented over certain sectors and States[15] and this paper aims to, amongst others, contribute to the debate about a federal law by gaining insights on the status of DPLs in other parts of the world. For research on (proposed) US DPLs I refer to Barclay.[16]

6 S. Elahi. 'Privacy and consent in the digital era' (2009) 14(3) Information Security Technical Report 113:115.

7 J. Akella, S. Marwaha and J. Sikes. 'How CIOs can lead their company's information business' (2014) 2 McKinsey Quarterly.

8 See: <http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf>.

9 Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos.

10 Biometric Technology Today. 'Global data protection authorities tackle Google on Glass privacy' (2013) (7) Biometric Technology Today 1.

11 Except from the naming of the exact name of the data protection authority, which is not always literally mentioned in the law.

12 They can only be measured through the usage of proxies, such as the intensity of metrics that are measurable, such as the amount of deep packet inspection, or surveys among citizens.

13 G. Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' in Volume 23 (2014):10.

14 See <www.privacyinternational.org>.

15 K. A. Bamberger and D. K. Mulligan. 'Privacy in Europe, Initial Data on Government Choices and Corporate Practices' (2013) 81 George Washington Law Review 1529:1547.

16 'A comparison of proposed legislative data privacy protections in the United States' (2013) 29(4) Computer Law

11 A summary of the focus of this research is displayed visually in Figure 1 below:

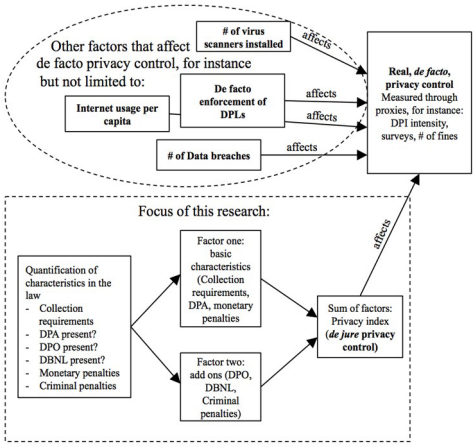

Figure 1: focus of this research

IV. Structure of this paper

12 The next section consists of a literature review on recent quantitative text analysis in the field of data protection legislation. Following this, I outline the methodology of constructing the index. Next, I will discuss the descriptive statistics of the six coded characteristics. Hereafter, using principle component analysis I identify unobserved variables within the six coded characteristics. I then discuss the privacy index formed by combining the two underlying factors. The last section summarizes the conclusions of this research.

B. Literature review on quantitative text analysis of DPLs

13 Comparisons of DPLs that are both academic and quantitative are scarce. Some comparisons are quantitative, but do not reveal their methodology. As a result, their scientific applicability is limited. An example is the index of Privacy International, which uses qualitative descriptions and expert experience to build up an index about the degree of privacy protection in a country.[17] However, the way in which this index is constructed is unclear. Moreover other indices, such as "heat maps" made by law firms, are constructed based on the impression of legal experts.[18] Those heat maps indicate that European and other developed countries have the most stringent DPLs in the sense of privacy control, although in the latest rankings there are some newcomers such as Mauritius.[19] The definition of privacy control varies, and the method of construction of the indexes is sometimes not entirely clear. Moreover, studies contradict each other. For instance, DLA Piper regards Iceland as having limited protection and enforcement while the Webindex places Iceland in its top 10. The scores of these indices are shown in Appendix B.

14 Table 1: quantitative studies on DPLs

Firm	Definition of privacy control	Percentage of top 10 that is an EU country	Percentage of top 10 that is an developed country*
DLA piper 2012-2014	Degree of enforcement and protection measures of data protection	75%	100%
Webindex 2014	To what extent is there a robust legal or regulatory framework for protection of personal data in your country?	64%	86%
Privacy International 2007	Degree of privacy enforcement (subset of the index)	71%	100%

**Percentage of top 10 that is an developed country*[20]

15 Other comparisons are more qualitative. This stream of literature describes the origins of the laws and its embedment in legal cultures. Current qualitative studies state that European laws have the most advanced data protection regimes.[21] Greenleaf for instance argues that non-western DPLs are influenced by the EU,[22] implying that they are setting standards. In qualitative research, privacy control is naturally interpreted as a broader concept than the literal text of the data protection legislation. For instance, Bamberger and Mulligan indicate that the dynamics between public and private actors are possibly of more importance than formal legislation.[23] A DPL

& Security Review 359.

17 see <https://www.privacyinternational.org/sites/privacyinternational.org/files/filedownloads/phrcomp_sort_0.pdf>.

18 Interview Mr. Richard van Schaik [July 23, 2014].

19 Appendix B displays the values of all the parameters of the data protection heat maps.

20 Upper quartile in the human development index 2014.

21 P. Boillat and M. Kjaerum, 'Handbook on European data protection law' Publication Office of the European Union (Luxembourg):3.

22 G. Greenleaf. 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' (2012) 2(1) International data privacy law.

23 K. A. Bamberger and D. K. Mulligan, 'Privacy in Europe, Initial Data on Government Choices and Corporate Practices'

should be nested within broader ethical frameworks to function correctly.[24] Consequently, similar laws can have different outcomes and different laws can have similar outcomes. In that sense it is hard to commensurate, because something different is measured. One could only make statements such as: "while from a broad perspective privacy control, developed countries have far better privacy control regimes, the legal texts of developing countries are mostly as stringent or more stringent." However, they also argue that there is a large difference between "law on the books" and "law in practice". This paper only takes into account "law on the books".[25] There is much qualitative comparative legal research on DPLs. Hence, this overview only highlights a few examples.

16 Another problem is time. Information technology is dynamic, and so are the laws governing it. Hence, information security laws, such as DPLs, are increasingly subject to change. Governments are becoming progressively more concerned with online privacy. As a result, studies regarding Internet related legislation become quickly out-dated. 20 out of the 71 laws I analyzed were introduced or had significant amendments in 2012, 2013 or 2014. One study of the United Nations is scientific, quantitative and recent, but focuses on a different subject: cybercrime legislation.[26] According to one of the co-authors, one of the key challenges of quantifying laws is making meaningful categorizations while keeping variety in variables low in order to avoid over- interpretation.[27] In Table 2 below, I scored current studies and their limitations regarding application in this study.

17 Table 2: comparative studies and their limitations

Study	Limitations			
	Methodology not revealed	Not quantitative	Out dated or limited n	Different subject
National privacy ranking*	V		V	
The Webindex (Subparameter: personal data protection framework)**	V			
Internet privacy law: a comparison between the United States and the European Union***		V	V	
A comparative study of online privacy regulations in the U.S. and China*I		V	V	
UNODC Comprehensive study on cybercrime*II				V
The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108		Half*IV		
Privacy in Europe, Initial Data on Government Choices and Corporate Practices*V		V	V	
Data protection 1998-2008*VI		V	V	
New challenges to data protection*VII		V		
European privacy and human rights 2010 *VIII		V	V	

**National privacy ranking[28] **The Webindex (Subparameter: personal data protection framework)[29] ***Internet privacy law: a comparison between the United States and the European Union[30] *I A comparative study of online privacy regulations in the U.S. and China[31] *II UNODC Comprehensive study on cybercrime[32] *III The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108[33] *IV Half[34] *V Privacy in Europe, Initial Data on Government Choices and Corporate Practices[35] *VI Data protection 1998-2008[36] *VII New challenges to data protection[37] *VIII European privacy and human rights 2010[38]*

C. The methodology

I. The approach: quantitative text analysis

18 I use coding to gain insights on six of the key elements of 71 data protection laws. There are two reasons for this. First, qualitative legal research is the most common approach among legal scholars

in Volume 81 (2013) 1529:1648.

24 ibid.

25 ibid.

26 UNODC, 'Comprehensive Study on Cybercrime' (2013).

27 Interview Ms. Tatiana Tropina [June 2, 2014].

28 Privacy International, 'National Privacy Ranking' (2007).

29 Webindex. '<https://thewebindex.org/visualisations/#!year=2012&idx=Personal%20data%20protection%20framework&handler=map>'.

30 D. L. Baumer, J. B. Earp and J. C. Poindexter. 'Internet privacy law: a comparison between the United States and the European Union' (2004) 23(5) Comput Secur 400.

31 Y. Wu and others. 'A comparative study of online privacy regulations in the U.S. and China' (2011) 35(7) Telecommun Policy 603.

32 UNODC, 'Comprehensive Study on Cybercrime' in (2013).

33 G. Greenleaf, 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' in Volume 2 (2012).

34 The Greenleaf study quantifies several characteristics of non-European DPLs. The aspects are quantified on a dummy scale but no final index is constructed.

35 K. A. Bamberger and D. K. Mulligan, 'Privacy in Europe, Initial Data on Government Choices and Corporate Practices' in Volume 81 (2013) 1529.

36 H. Grant. 'Data protection 1998–2008' (2009) 25(1) Computer Law & Security Review 44.

37 D. Korff and I. Brown, 'New Challenges to Data Protection - Final Report' European Commission DG Justice (2010).

38 Privacy International, 'European Privacy and Human Rights 2010' (2010).

and coding complements qualitative comparative analysis.[39] Traditionally, qualitative comparative law entails the analysis, scrutiny and comparison of national legal texts and legal systems.[40] This is done in a legal manner: "the comparatists use just the same criteria as any other lawyer"[41], but "has more material at his disposal". For instance, the recent study about DPLs by Bamberger and Mulligan[42] utilizes qualitative comparative legal research focusing on data protection. Through this kind of traditional comparative research, DPLs can be understood in detail. There are also drawbacks; usually, a limited amount of jurisdictions can be analyzed because a deep dive in a single jurisdiction requires a lot of time and resources. Moreover, the results are not suitable for statistical analysis. Quantification enables a fast overview of laws. A quantitative analysis of legal texts enables direct comparison of a limited amount of variables between an extensive number of jurisdictions (in the case of this paper: 71). In this way, the potential drawback of qualitative legal analysis - its limited number of jurisdictions - can be mitigated. In a globalized world, a quantitative method allows for enhanced understanding of the similarities and differences between laws.[43] However nuances within laws and legal systems are omitted in quantitative analysis. Thus, qualitative and quantitative legal analyses can complement each other. By using both, we enhance our understanding of the national approaches to address societal problems through the use of the law.

19 Second, quantification of DPLs enables disclosure for statistical analysis. By quantifying the law, existing theories of effective laws can be falsified or supported, which creates a better understanding of the law. Additionally, coding is needed to measure effects of laws on events in the real world. Currently, scholars collect, measure and structure statistics of information security. This includes data breaches,[44] deep packet inspection,[45] details of Internet domain names,[46] malware,[47] and e-service adoption.[48] While on the basis of these studies, researchers are able to draw conclusions concerning statistics of information security, this research does not allow for linking effects with differences within regulations. Currently, much legislation is solely described qualitatively. Regulations are displayed in the form of text in a code, and not as a form of code in an index. For example, a recent study related Deep Packet Inspection intensity with privacy regulation strictness.[49] This study encountered difficulty in finding a decent metric for privacy regulation strictness.[50] In short, researchers in information security desire quantitative disclosure of different legislation - coded data that is constructed in verifiable and repeatable way. Measuring the impact of regulations on society improves the quality of the legal system. [51] Coding the law is the first step for a quantitative impact assessment.

II. The perspective of privacy control

20 This paper codes DPLs elements that contribute to what is called privacy control. Privacy control defines the aims of DPLs to give consumers control over their own data.[52] Judges and legal scholars mention the notions of privacy control frequently when discussing the main purpose of DPLs. For instance judge Posner noted that within the "economic analysis of the law of privacy ... should focus on those aspects of privacy law that are concerned with the control by individuals of the dissemination of information about themselves".[53] Privacy control is

39 A. Meuwese and M. Versteeg, 'Quantitative methods for comparative constitutional law' in M. Adams and J. Bonhoff (eds), Practice and Theory in comparative law (Cambridge University Press, 2012) 231.

40 K. Zweigert and H. Kötz, Introduction to comparative law (Third revised edition edn Clarendon Press, Oxford 1998):4.

41 ibid.

42 'Privacy in Europe, Initial Data on Government Choices and Corporate Practices' in Volume 81 (2013) 1529.

43 M. Watt, Globalization and comparative law (Oxford University Press, 2006):589.

44 B. F. H. Nieuwesteeg, The Legal Position and Societal Effects of Security Breach Notification Laws (Delex, Amsterdam 2014); S. Romanosky, R. Telang and A. Acquisti. 'Do data breach disclosure laws reduce identity theft?' (2011) 30(2) Journal of Policy Analysis and Management 256 accessed 27 December 2013.

45 H. Asghari, M. J. G. van Eeten and M. Mueller. 'Unravelling the Economic and Political Drivers of Deep Packet Inspection' (2012).

46 R. Clayton and T. Mansfeld. 'A Study of Whois Privacy and Proxy Server Abuse' (WEIS 2014).

47 S. Tajalizadehkhoob and others. 'Why Them? Extracting Intelligence about Target Selection from Banking Trojans' (2014) 13th Annual Workshop on the Economics of Information Security.

48 M. Riek, R. Böhme and T. Moore. 'Understanding the influence of cybercrime risk on the e-service adoption of European Internet users.' (WEIS 2014).

49 H. Asghari, M. J. G. van Eeten and M. Mueller, 'Unravelling the Economic and Political Drivers of Deep Packet Inspection' in (2012).

50 The index used (the privacy index of Privacy International) was designed in 2007 and is hence out-dated. Moreover, Privacy International does not reveal the methodology of construction. Cybersecurity laws are subject to rapid change. The privacy index gave a value about privacy protection but it was unclear what this value is based upon. Although there were these doubts, Asghari et al found a significant relation.

51 R. Posner, *The Economics of Public Law* (Edward Elgar Publishing, 2001).

52 P. Schwartz. 'Internet Privacy and the State' (1999) 32 Connecticut Law Review 815:817.

53 'Privacy' in The New Pelgrave Dictionairy of Economics and

also the aim of many DPLs that have been adopted. Control is for instance reflected in European privacy laws. Article 8 of the Charter of fundamental rights was the basis on which the European Court of Justice granted individuals control over their data in the Google case.[54]

21 Privacy control imposes requirements for control and safety. Individuals should have control over what organizations do with their personal data. Moreover, data should be safe and protected by those organizations. Personal data is any data that can be linked to individual persons (hereafter: individuals).[55]

22 Another important aspect of privacy control is compliance with this control. I use the theory of regulatory deterrence to discuss this perspective. The deterrence theory is based on the assumption that complying with a regulation is to a large extent a cost benefit analysis. Organizations will comply if the cost of compliance is lower than the cost of non-compliance. If a penalty for non-compliance is very high, an organization will be more willing to comply than if a penalty for non-compliance is very low.[56] If enforcement is stringent and hence the likelihood of detection is high, organizations are also more willing to comply. Scholars argue that higher sanctions lead to more compliance.[57] Some argue that employees of an organization are incentivized by the *perceived* severity of the sanctions.[58] In addition, DPAs expect fines to be "strongly deterrent".[59] Within the context of this paper, I exclusively look at enforcement mechanisms within the law that increase the likelihood of detection or the height of the penalty.

23 Hence, to summarize, the (*de jure*) privacy control perspective in DPLs is interpreted as a combination of the amount of privacy control and the enforcement mechanisms of this control (see Figure 2):

1. The severity of the requirements in DPLs that ensure:
   - Control: individuals have control over their data.
   - Safety: personal data is safe in the hands of organizations.
2. The severity of compliance mechanisms
   - Enforcement: mechanisms that increase the likelihood of detection
   - Sanctions: penalties

Figure 2: elements of de jure privacy control

24 Within the literature, there are objections about the operationalization of privacy as control and protection. Schwartz mentions three of them, the autonomy trap, security seclusion and commodification of privacy.[60] Hence, this paper does not claim a normative standpoint, in the sense that privacy-control should be the best or only aim of DPLs. It takes a neutral descriptive approach. The index gives us a descriptive understanding about those characteristics in the law that contribute to privacy control in DPLs. Moreover, by constructing a privacy control index, it can be falsified or confirmed whether elements of privacy control in the literal text of the law have an impact on desirable policy outcomes. Moreover, the school of behavioral economics disputes the deterrence theory. This academic school questions its rationality in calculating costs and benefits. However, scholars argue that, when actors tend to be more professional, such as large organizations, their behavior will be more rational.

III. The source: DLA Piper data protection handbook

25 I use the literal text of the DPLs as the main source for coding the law. An assessment of the literal text requires knowledge regarding the origins of the laws and local legal language. How do we gather the knowledge we need with limited resources?

the Law (Privacy edn Grove Dictionairies, 1998):104.

54 Case (c131-12), par. 99.

55 Some countries need more words than others to describe personal data. See for instance the following examples. Singapore: personal data is data, whether true or not, about an individual who can be identified. South Africa: 'personal Information' includes information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person/legal entity. The Netherlands: personal data is any data relating to an identified or identifiable natural person.

56 G. S. Becker. 'Crime and Punishment: An Economic Approach' (1968) 76(2) The Journal of Political Economy 169.

57 W. B. Chik. 'The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform' (2013) 29(5) Computer Law & Security Review 554:536.

58 L. Cheng and others. 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory' (2013) 39, Part B(0) Comput Secur 447:227.

59 H. Grant, 'Data protection 1998–2008' in Volume 25 (2009) 44:49.

60 Schwartz (n 52) explains the autonomy trap by first assessing this as a problem of self-determination. This is caused by two phenomena. The first is that there is a large information asymmetry between the vendor and the consumer. caused by obscure and hard to understand privacy notices (Schwartz, 822). The second is the fact that people do not really have a choice not to account for because than they are excluded for services. Information asymmetry and little choice causes a general inertia toward default terms Moreover, autonomy is limited further through the legitimate use of personal data by the government or other parties. The uses of personal data by third parties also causes the security seclusion problem: people think they have control and information is isolated, but this is not the case. The last problem consists of the commodification of privacy, it can be traded and sold at the lowest price. More about this in the work of Schwartz.

Local legal experts are able to efficiently distract characteristics of the law from the literal text. Global international law firms have such local experts. Therefore, I relied on reports on data protection legislation constructed by international law firms to serve their clients. There are several reports available as displayed in Table 3 below:

26 Table 3: summary of current qualitative data protection law comparisons

Name	Firm	Last updates	Coverage (number of countries)
Global Data Protection Handbook*	DLA Piper	2013-2014	71
International Compendium of Data Privacy Laws*	Baker Law	2014	42
Data Privacy Heat Map	Forrester	2014	54 (only available for paying clients)

**Global Data Protection Handbook*[61] ***International Compendium of Data Privacy Laws*[62]

27 I use the DLA Piper Global Data Protection Handbook as my main source due to two reasons. First, it is the most complete report, covering 71 laws. Second, the validity of the data is assured; the information is the direct representation of the law and not the interpretation of experts according to a DLA Piper partner that I interviewed.[63] In this report, they do not discuss any *de facto* aspects of the law. Different experts of partners or offices of DLA piper delivered the information. I could not reach the authors of the International Compendium of Data Privacy Laws by Baker law. The Forrester report is only available for paying clients and thus not usable.[64]

IV. Coding six characteristics

28 For this research I code six characteristics from the perspective of privacy control. Excluded characteristics can be found in the long list in Appendix B. Section D discusses the included characteristics. I aim to code more characteristics for future research. The characteristics are coded on a dummy or interval scale. In order to avoid over-interpretation, I do not allow for much variety in variables.[65]

29 The characteristics are selected on three criteria: first, they need to affect privacy control; second, the characteristics need to be quantifiable, in the sense that they can be coded on a dummy or interval/ratio scale; and third, the characteristics need to be different among countries. If all countries would have the same variable, this variable will not elicit differences between countries. Special attention should be given to the validity of the coding procedure. A limitation of the applied coding procedure is namely the use of a secondary source. Furthermore, the dichotomous or ordinal scale is a concern. For instance, the degree of independence of DPAs varies considerably across countries.

D. The six coded characteristics

30 This research aims to answer the following question:

31 *How do countries outside the US design their data protection laws with respect to key elements such as consent, the presence of data protection authorities, and penalties for non-compliance?*

32 In this section, the results of the coded characteristics are discussed, either as a dummy variable or on an ordinal scale. The footnotes highlight choices made in the coding process.[66] Below there is overview of the theoretical effects of characteristics on various elements of privacy control (Table 4).

33 Table 4: characteristics and their contribution to privacy control

Aspects of privacy control (horizontal)	1. Requirements		2. Compliance	
Characteristics in the law (vertical)	1a. Control	1b. Safety	2a. Enforcement	2b. Sanctions
Data collection requirements	1			
Data breach notification requirement	1	1		
Data protection officer		1	1	
Data protection authority			1	

61 DLA Piper, 'Global Data Protection Handbook ' DLA Piper (2014).

62 Baker Law, 'International Compendium of Data Privacy Laws' Baker Law (2014).

63 I extensively interviewed one of the authors. Interview with one of the main experts (core team) of the report, Richard van Schaik [July 23, 2014].

64 I asked for disclosure for academic purposes but did not get a response from the firm.

65 Interview Tatiana Tropina [June 2, 2014].

66 There are more relevant characteristics that are worth researching. This should be one of the key next steps for future research. For instance, requirements for processing and security guidelines are for example arguably also a proxy for privacy control. But processing requirements are roughly equal over all countries. A quantification of those requirements would not elicit differences between DPLs. Security guidelines are hard to quantify on a dummy or interval scale.

Monetary Sanctions				1
Criminal Sanctions				1
Characteristics per determinant	2	2	2	2

I. Data collection requirements

34 Data collection requirements prescribe that organizations should interact with data owners before personal data collection.[67] Hence, data collection requirements affect the amount of control that individuals have over their personal information.[68] There are roughly two forms - an information duty and prior consent. An information duty means that individuals have to be informed about when their data is collected and how it is treated.[69] Prior consent means that individuals have to give consent before a data processor wants to disclose personal information.[70] An information duty is less severe, since organizations are not dependent on the consent of consumers and consumers might miss this information.[71] In Table 5 below, the results for collection requirements are shown:

35 Table 5: descriptive statistics data collection requirements

Characteristic	Function	State	Code	Results
Requirements for collecting personal data	Requirements (Control individuals)	Prior consent needed	2	55
		Information duty only	1	10
		No requirement / no law	0	6

67 Collecting data is often distinguished from processing personal data. Collection requirements can differ from processing requirements. Processing requirements are mostly stricter. Most states that have an information duty for collecting data require prior consent for processing data. Hence, this would not leave much space for differences between laws, and therefore the focus of this paper lies in collecting data.

68 E. A. Whitley. 'Informational privacy, consent and the "control" of personal data' (2009) 14(3) Information Security Technical Report 154.

69 The exact form varies. Some states require a purpose of use on the website (Japan). Other require 'making reasonable steps to make the individual aware' (Australia).

70 D. Le Métayer and S. Monteleone. 'Automated consent through privacy agents: Legal requirements and technical architecture' (2009) 25(2) Computer Law & Security Review 136:137.

71 Data collection requirements also have their disadvantages. Typically, consumers have to give consent for long pages of privacy rules and organizations do not have the obligation to check whether consumers understand these obligations. Hence, there are some new initiatives to enhance the communication about privacy, for instance the Dutch "datawijzer", see <http://www.nationale-denktank.nl/eindrapport2014/oplossing-1-hack-je-hokje/oplossing-2-datawijzer-2/> (Dutch).

36 The data shows that most countries require prior consent. Only a few require solely an information duty. This is not surprising, since prior consent is one of the corner stone principles of many DPLs. Countries that are labelled zero (no requirement) also do not have a law.

II. Data breach notification requirement (DBNL)

37 The data breach notification requirement (in the US this is commonly referred to as the Data Breach Notification Law [hereafter, DBNL]) influences both control and safety requirements in privacy control. A notification requirement obliges organizations to notify a data breach to affected customers and a supervisory authority. Schwartz and Janger suggest that this is a constructive measure because the quick awareness of a data breach by consumers has a positive impact on control of data of individuals.[72] A notification of a data breach also ensures safety of data. The damage following a breach can be mitigated faster. Moreover, a requirement incentivizes companies to invest in information security.[73] Organizations want to avoid a notification because of the perceived (mostly reputational) damage they suffer (c.f. the 'sunlight as a disinfectant' principle). The descriptive statistics for data breach notification requirements across the 71 states analyzed are displayed below (Table 6):

38 Table 6: descriptive statistics data breach notification requirements

Characteristic	Function	State	Code	Results
The existence of a Data Breach Notification Law	Requirements (Safety of data) (Control – mitigation measures)	DBNL	1	21
		No DBNL	0	50

39 21 out of 71 countries that were studied have a DBNL.[74] The US state of California already adopted a DBNL in 2003. Since this point in time, these laws have been widespread in the US - 47 out of its 50 states have a DBNL. However, this does not seem to be the case in the rest of the world. This possibly has to do with some concerns regarding administrative

72 P. Schwartz and E. J. Janger. 'Notification of data security breaches' (2007) 105(5) Mich Law Rev 913 accessed 27 December 2013:971.

73 S. Romanosky, R. Telang and A. Acquisti, 'Do data breach disclosure laws reduce identity theft?' in Volume 30 (2011) 256 accessed 27 December 2013.

74 This low amount of DBNLs contrasts with the US (which is not a part of this study). California was the first state to adopt a DBNL in 2003 and other states quickly followed. As of 2014, 46 out of 50 US States adopted a DBNL.

burdens for organizations to comply with a DBNL. However, in 2018, the proposed General Data Protection Regulation enters into force in the EU and consequently, all Member States will have a DBNL, increasing the amount of DBNLs by 18 countries to 39 countries.

III. Data protection authority (DPA)

40 A data protection authority (DPA) has to enforce compliance with the DPL.[75] A DPA executes security audits and imposes sanctions. DPAs review organizations based on complaints of individuals.[76] The actual degree of enforcement differs between countries, and is excluded from this analysis. Apart from enforcement, DPAs are an information and notification center. For instance, organizations should notify a data breach to the DPA according to a DBNL. The presence of a DPA is an indicator of the degree of compliance because a DPA executes parts of DPLs. The presence of a DPL indicates that there are resources for enforcement. Moreover in general, the importance of privacy and data protection is visible for consumers. For instance, DPAs communicate through media channels to educate individuals about who to complain to for (alleged) breaches of data protection.[77] Third, a DPA functions as a point of contact, which eases and urges compliance with DPLs. Without a DPA, enforcement would merely be passive in the sense that probably only non-compliance highlighted in the media would be sanctioned. The descriptive statistics of the presence of data protection authorities are displayed in Table 7 below.

41 Table 7: descriptive statistics of the presence of data protection authorities

Characteristic	Function	State	Code	Results
The presence of designated data protection authorities (DPAs) to enforce the law	Compliance	DPA present*	1	58
		No DPA	0	13

**DPA present*[78]

42 The analysis shows that most countries (58) have a DPA. This can be explained by the central place that DPAs have in the implementation of DPLs. 13 countries have no DPA. Most countries that do not have legislation also do not have a DPA - except Saudi Arabia and Thailand, who have a DPA but no legislation. This research did not account for differences between various DPAs. This mainly concerns the severity and intensity of enforcement, but also the degree of independence of a DPA with respect to the government. Several parameters of DPAs can be used as a proxy of the intensity of enforcement, for instance the annual budget of the DPA, the height and frequency of imposed penalties and the ability and frequency of executed security audits.

IV. Data protection officer (DPO)

43 A data protection officer (DPO) is responsible for safeguarding personal data of individuals. A DPO ought to be appointed by organizations to ensure compliance.[79] Hence, a DPO captures both elements of "safety" and "compliance". A DPO functions as a connection between the literal text of the law and the daily practice of organizations that process personal data. Organizations with DPOs are more likely to incorporate a privacy policy. DPOs aid to establish social norms within this corporate infrastructure.[80] Privacy minded employees induce compliance in the whole organization because of social norms.[81] The descriptive statistics of the presence of a data protection authority are displayed in Table 8 below:

44 Table 8: descriptive statistics of the presence of data protection officers

Characteristic	Function	State	Code	Results
Every organization has to assign a data protection officer (DPO) to ensure compliance	Compliance	DPO*	1	17
		No DPO	0	54

** DPO*[82]

75 R. Wong. 'Data protection: The future of privacy' (2011) 27(1) Computer Law & Security Review 53.

76 K. A. Bamberger and D. K. Mulligan, 'Privacy in Europe, Initial Data on Government Choices and Corporate Practices' in Volume 81 (2013) 1529:1613.

77 R. Wong, 'Data protection: The future of privacy' in Volume 27 (2011) 53:56.

78 A DPA is coded 1 if there is a DPA is required and in place. In the case of the Philippines, a DPA is named in the law, but is not constituted yet. Therefore, it is labeled '0'.

79 T. Kayworth, L. Brocato and D. Whitten. 'What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles' (2005) 16(6) Communications of the Association for Information Systems 110:115.

80 L. Cheng and others, 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory' in Volume 39, Part B (2013) 447; T. Kayworth, L. Brocato and D. Whitten, 'What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles' in Volume 16 (2005) 110.

81 K. A. Bamberger and D. K. Mulligan, 'Privacy in Europe, Initial Data on Government Choices and Corporate Practices' in Volume 81 (2013) 1529:1611.

82 Laws that have a general obligation for organizations to appoint DPOs are labelled 1. Some laws only require a DPO

45 17 DPLs require a DPO; this is less than a quarter of the total amount of laws observed. The requirement to appoint a DPO could be an administrative burden for organizations[83] This administrative burden could explain why most countries did not incorporate this requirement.

V. Monetary sanctions

46 Monetary sanctions aim to increase the cost of non-compliance. Interviewees suggested that managers in organizations are deterred by the maximum damage possibly incurred by non-compliance. Hence, the characteristic "monetary sanction" relates to the maximum sanction that can be imposed. The descriptive statistics of the height of monetary sanctions are shown in Table 9 below:

47 **Table 9: descriptive statistics of the height of monetary sanctions**

Characteristic	Function	State	Code	Results
The maximum penalty for non-compliance with the regulation	Compliance	Above 1M*	1	5
		Between 100k and 1M	.75	18
		Between 10k and 100k	.5	25
		Under 10k	.25	13
		No penalty at all	0	10

*Above 1M[84]

48 Only 5 out of 71 countries have a maximum penalty for non-compliance above 1 million euro. This is the amount that really starts to deter companies when taking into account that the likelihood of detection is low. Hence there are little possibilities to deter. The likelihood of being caught is likely to play a large role in determining the expected sanction. This likelihood is strongly related to the enforcement costs for DPAs, which are high according to scholars, but unobserved in this analysis.[85]

VI. Criminal sanctions

49 The possibility to impose criminal penalties for non-compliance with the regulation is an additional sanction. Personal accountability increases when persons are subject to criminal sanctions such as imprisonment. Hence, criminal sanctions cause personal responsibility for the actions of corporate employees. The descriptive statistics of the criminalization of non-compliance with DPLs is shown in Table 10 below. Approximately half of the countries I studied criminalize non-compliance with the DPA.

50 **Table 10: descriptive statistics of criminal penalties**

Characteristic	Function	State	Code	Result
Criminalization of non-compliance with the regulation	Compliance	Criminalization*	1	38
		No Criminalization	0	33

*Criminalization[86]

VII. Correlations between the individual characteristics

51 Table 11 below shows the internal relation of the characteristics as such. EU membership and developed countries are also included.

Correlations

		EU_member	Penalty_crim	DBNL	DPO	DPA	Req_Collect	Penalty_eur	Upper quartile HDI
EU_member	Pearson Correlation	1	-.022	-.025	-.137	.365**	.369**	.220	.456**
	Sig. (2-tailed)		.852	.833	.254	.002	.002	.065	.000
	N	71	71	71	71	71	71	71	71
Penalty_crim	Pearson Correlation		1	.171	.060	.106	.172	.200	.026
	Sig. (2-tailed)			.154	.621	.379	.151	.095	.828
	N		71	71	71	71	71	71	71
DBNL	Pearson Correlation			1	.143	.088	.125	.190	-.001
	Sig. (2-tailed)				.236	.463	.299	.112	.994
	N			71	71	71	71	71	71
DPO	Pearson Correlation				1	-.054	.068	.132	-.036
	Sig. (2-tailed)					.656	.575	.274	.763
	N				71	71	71	71	71
DPA	Pearson Correlation					1	.324**	.384**	.341**
	Sig. (2-tailed)						.006	.001	.004
	N					71	71	71	71
Req_Collect	Pearson Correlation						1	.378**	.123
	Sig. (2-tailed)							.001	.305
	N						71	71	71
Penalty_eur	Pearson Correlation							1	.211
	Sig. (2-tailed)								.077
	N							71	71
Upper quartile HDI	Pearson Correlation								1
	Sig. (2-tailed)								
	N								71

**. Correlation is significant at the 0.01 level (2-tailed).

52 **Table 11: pearson correlation between individual coded characteristics (significant circled)**

for designated sectors. This is not a general obligation; hence they are labelled '0'. Other laws reduce data breach notification requirements if a DPO is appointed. Since this is not an obligation to install a DPO, these states are labelled '0'. The same applies with laws that recommend organizations to install a DPO.

83 ibid.

84 Furthermore, sanctions that are displayed in other currencies are converted into euros. Average USD EUR currency = 1.35, Australian 1.4, Canadian 1.45, GBP 0.83. Also, sanctions are grouped in order of magnitude. The sanctions are not corrected for purchasing power.

85 H. Grant, 'Data protection 1998–2008' in Volume 25 (2009) 44:49.

86 Solely provisions that specifically criminalize non-compliance with the DPL are labelled '1'. General criminalization clauses are excluded, because every country criminalizes intentionally causing harm.

53 EU membership is correlated with the presence of a DPA, strong requirements for data collection, and the upper quartile of the Human Development Index. This makes sense since the European directive requires the presence of a DPA and prior consent before collection. Moreover, almost all EU Member States are in the upper quartile of the Human Development index. Furthermore, it is notable that DPA presence is correlated with collection requirements and monetary sanctions. This also makes sense: a legislator that constitutes a DPA is likely to give this guarding dog some extra teeth in the form of high monetary sanctions.

E. Identifying underlying unobserved variables

I. Principal component analysis

54 A principal component analysis is a decent tool to determine whether the six characteristics can be explained by fewer underlying factors. In theory, the data is suited for principal component analysis, with a significant Kaiser-Meyer-Olkin Measure of Sampling Adequacy above .6 (.671) and a significant Bartlett's test for sphericity (p=0.003).

II. Basic characteristics and add-ons

55 Two factors have eigenvalues above one.[87] Moreover, the scree plot (the diagram displaying the eigenvalues, shown in Appendix E) displays a relatively clear bend between the second and the third suggested factor. The pattern matrix shows clear correlations of each characteristic with one particular underlying factor. The correlation with the individual characteristics are shown in Table 12 below.

56 Table 12: Correlation of individual characteristics with their underlying factor

Factor 1: basic characteristics	Factor 2: add-ons
Presence of data protection authority (.766**)	Data protection officer (.729**)
Requirements of collection (.720**)	Data Breach Notification Requirement (.669**)
Monetary penalties (.745**)	Criminal penalties (.461**)

57 Figure 1: Correlation of individual characteristics with their underlying factor * = .05 significance level, ** = .01 significance level

87 The widely used Direct Oblimin rotation with Kaiser Normalisation is applied.

58 The first factor is called "basic characteristics". The factor has positive and significant correlations with the Webindex '13 (.532**) and '14 (.584**), the Privacy index '07 (.373*), the DLA piper heatmap score (.495**) and EU membership (.415**). Hence, the three underlying characteristics are basic building blocks of many DPLs. The second factor is called "add-ons". The three underlying characteristics are displayed within some DPLs. Moreover they are only positively correlated with laws that have been amended recently (.301*),[88] which might indicate that DPLs are really added later.

F. Aggregating underlying factors towards a 'privacy control index'

I. The privacy control index

59 The privacy control index is the sum of the two factors, "basic characteristics" and "add-ons". Hence, the index does not resemble the top 10 of "best" DPLs but scored high on the presence of the six underlying characteristics (see Table 13).

60 Table 13: top ten countries of the privacy control index

Rank	Privacy control index
1	Mexico
2	South Korea
3	Taiwan
4	Philippines
5	Germany
6	Mauritius
7	Italy
8	Luxembourg
9	Norway
10	Israel
# Developed countries |	7/10 |
# EU countries	2/10

61 Based on the literature, I would expect high positions for developed and European countries. However, non-western and underdeveloped countries such as Mexico, Mauritius, Taiwan and the Philippines occupy a significant part of the top 10. On the other hand, the bottom 10 countries also mainly consist of non-developed and non-EU countries, which partly have no DPL at all. Countries such as Mexico and Taiwan, which did not have a DPL before, recently adopted DPLs.[89] These countries have laws with

88 After excluding countries without a DPL.

89 The introduction date of non-western countries: Mexico (2011), South Korea (2011), Mauritius (2009), Taiwan (2012), South Africa (2013), Philippines (2012).

high *de jure* standards indicating that legislators may want to keep up with developed countries. Recent international calls for stringent privacy regimes could explain this. In addition to that, the data protection directive 95/46/EC (that serves as a minimum base for DPLs for all EU Member States) has been adopted in 1995. When the draft general data protection regulation enters into force in the EU in 2018, all 27 Member States will likely occupy the top position again based on the privacy control index. EU countries now have a middle- position in the index. The presence of those countries in the bottom 10 of the index is due to the fact that these countries have very limited or no DPLs. In Figure 3 below, the privacy index is broken down in parts for EU members (1) and non-EU members (0).

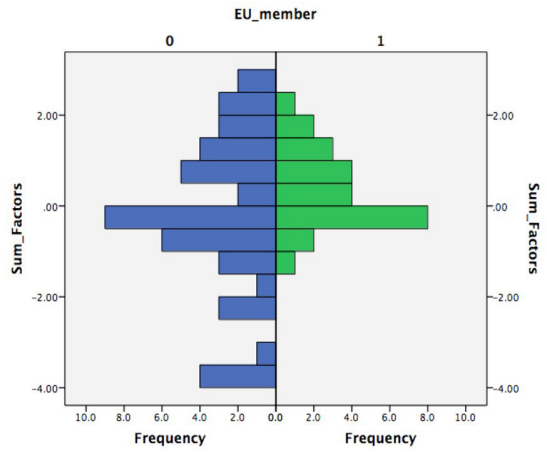

Figure 3: privacy index breakdown for EU members

II. Relation with other indices

62 Table 14 shows correlations of the privacy control index with other indices that were discussed.

63 **Table 14: correlation with known indices **significant on the 0.01 level; *significant on the 0.05 level**

Correlation statistics	Cases (countries)	Index
Heat map DLA piper	64	,353**
Webindex 2014	49	,542**
Webindex 2013	49	,475**
Privacy International*	42	Not significant

**Privacy International*[90]

The privacy control index does correlate with the heat map of DLA (based on the expert judgment of the authors). The privacy control index does not correlate with the privacy index of Privacy International. However this index is seven years old, while 20 out of 71 laws have been amended since. There are significant correlations with the two versions of the Webindex. There is no significant correlation between the date of adoption of the law and the last date of amendment.[91]

III. Explanatory power of the index

64 The privacy control index is based on six coded characteristics of the DPLs chosen from the perspective of privacy control.[92] In a narrow view, the privacy control index resembles the sum of two factors that measure six coded characteristics. The privacy index displays not perfect representation of *de jure* privacy control and an even less perfect representation of *de facto* privacy control. As Box said: "all models are wrong, but some are useful".[93] The privacy index measures solely the literal text of the law, and within this scope, exclusively six characteristics. Hence, this privacy index does not give an indication on "how good" privacy protection is in a certain country.[94] The aim is adding quantified knowledge to existing qualitative insights about DPLs.

65 Bamberger and Mulligan put it this way: "The law on the books differs from law in practice." Indeed, privacy control is broader than the privacy control index. The degree of privacy control of data protection regimes is also determined by non-legal factors such as, but not limited to, actual imposed penalties,[95] the enforcement capacity of data protection authorities, the number of data breaches, and Internet usage per capita as discussed in Section 1.3.

G. Conclusions

66 This paper coded the following six characteristics based on the literal text of 71 Data Protection Laws (DPLs): data collection requirements; the data

90 As far as the index of Privacy International is concerned, both the total index as well as the subindex for statutory protection is used. Both indices did not have a significant correlation with the privacy control index.

91 For this analysis, states without a DPL are excluded, because otherwise there would be always a very high correlation between the data of adoption or amendment and the privacy control index.

92 The full index is displayed in appendix A2.

93 G. E. P. Box and N. R. Draper, *Empirical Model Building and Response Services* (John Wiley and Sons, New York 1987):424.

94 I do not recommend storing data in the Mauritius or Mexico that have high scores.

95 It is an option to incorporate some of these factors in future versions of the privacy control index.

breach notification requirement; the presence of a data protection authority; the requirement of a data protection officer; the level of monetary sanctions; and the presence of criminal sanctions.

67 The results of this study show that 5 out of 71 countries have a maximum penalty for non-compliance above 1 million dollars. 55 out of 71 countries require prior consent before collecting personal data and 10 have an information duty. 21 out of 71 countries have an obligation to notify data breaches, while in the US, 47 out of 50 states have such a data breach notification law. Most of the countries observed - 54 out of 71 - do not require a Data protection officer. About half the DPLs analyzed have criminalized non-compliance with the DPL. Principal component analysis is used to distinguish two underlying factors called "basic characteristics" and "add-ons". The final privacy control index is constructed by combining these factors. EU Member States have DPLs with privacy control above average but no absolute top position. Countries that have low privacy control in DPLs are always non-European and mostly outside the upper quartile of the Human Development Index.

68 Future research should update this privacy control index every year. For instance, the European Data Protection Regulation, replaces all the EU DPLs in 2018 and will have a major impact on the position of these countries in the index. Future updates also allow for distinguishing patterns in the development of DPLs over time. Another next step is to include all countries that have DPLs (currently 101) and code more characteristics of the law. One might also code the literal text of the law, instead of depending on (validated) sources of international law firms such as DLA Piper. A more ambitious contribution would be to add indicators of genuine enforcement of the law, for instance, the amount of penalties imposed by data protection authorities.

Appendix A1 – The six characteristics

Country	Last_ amendment	Req_Collect	DBNL	DPA	DPO	Penalty_ eur	Penalty_ crim
Argentina	2000	2	0	1	0	1	1
Australia	2014	1	0	1	0	4	0
Austria	2000	2	1	1	0	2	0
Belgium	2001	2	0	1	0	3	1
Brazil	No DPL	0	0	0	0	0	0
British Virgin Islands	No DPL	0	0	0	0	0	0
Bulgaria	2013	2	0	1	0	2	1
Canada	2000	2	0	1	1	2	0
Cayman Islands	No DPL	0	0	0	0	0	0
Chile	2009	2	0	0	1	1	0
China (People's Republic)	No DPL	2	0	0	0	2	0
Colombia	2013	2	1	1	0	3	0
Costa Rica (2013)	2013	2	1	1	0	2	1
Cyprus	2003	2	0	1	1	2	1
Czech Republic	2000	2	0	1	0	3	0
Denmark	2000	2	0	1	0	2	1
Egypt	No DPL	2	0	0	0	0	0
Finland	2000	2	0	1	0	2	1
France	2004	2	0	1	0	3	0
Germany	2009	2	1	1	1	3	0
Gibraltar	2006	2	0	1	0	1	1
Greece	2012	2	0	1	0	2	1
Guernsey	2001	2	0	1	0	2	0
Honduras	2006	2	0	1	0	0	0
Hong Kong	2013	1	0	1	0	3	1
Hungary	2012	2	0	1	0	2	0
Iceland	2000	2	0	1	0	2	1
India	2013	2	0	0	1	3	1
Indonesia	2008	2	1	0	0	2	1
Ireland	2003	2	1	1	0	3	0
Israel	2006	2	0	1	1	3	1
Italy	2003	2	1	1	0	3	1
Japan	2005	1	1	0	0	1	1
Jersey	2005	2	0	1	0	4	1
Lithuania	2003	2	1	1	0	1	0
Luxembourg	2006	2	1	1	0	3	1
Macau	2005	2	0	1	0	2	1
Malaysia	2013	2	0	1	0	2	1
Malta	2003	2	1	1	0	2	1
Mauritius	2009	2	1	1	1	1	1
Mexico	2011	1	1	1	1	4	1

Monaco	2008	2	0	1	0	2	1
Morocco	2009	0	0	1	0	2	1
Netherlands	2001	2	0	1	0	1	0
New Zealand	1993	1	1	1	1	0	0
Norway	2000	2	1	1	0	3	1
Pakistan	No DPL	0	0	0	0	0	0
Panama	2012	1	0	1	0	3	0
Peru	2013	2	0	1	0	3	1
Philippines	2012	2	1	1	1	3	1
Poland	2007	2	0	1	1	2	1
Portugal	1998	2	0	1	0	2	1
Romania	2001	2	0	1	0	2	0
Russia	2006	2	0	1	1	1	0
Saudi Arabia	No DPL	0	0	1	0	0	0
Serbia	2012	2	0	0	0	1	1
Singapore	2014	2	0	1	1	4	0
Slovak Republic	2013	2	0	1	1	3	0
South Africa	2013	1	1	1	1	2	1
South Korea	2011	2	1	1	1	2	1
Spain	1999	2	0	1	0	3	0
Sweden	1998	2	0	1	0	2	1
Switzerland	1992	2	0	1	0	1	0
Taiwan	2012	2	1	1	0	4	1
Thailand	No DPL	1	0	1	0	0	0
Trinidad and Tobago	2012	2	0	0	0	0	0
Turkey	2012	1	0	1	0	1	1
Ukraine	2014	1	0	0	1	1	1
United Arab Emirates	2007	2	1	1	0	1	1
United Kingdom	2000	2	0	1	0	3	0
Uruguay	2009	2	1	1	0	2	0

Appendix A2 – The privacy control index and the two underlying factors

Country	Sum_Factors	FAC_basic_characteristics	FAC_add_ons
Mexico	2,80	0,50778	2,29023
South Korea	2,55	0,45472	2,09537
Taiwan	2,38	1,42940	0,95054
Philippines	2,33	-0,34448	2,67775
Germany	2,11	0,51623	1,59089
Mauritius	2,07	0,10804	1,96393
Italy	1,90	1,08273	0,81910
Luxembourg	1,90	1,08273	0,81910
Norway	1,90	1,08273	0,81910

Israel	1,82	0,70158	1,11743
South Africa	1,60	-0,35891	1,96163
Costa Rica	1,42	0,73605	0,68766
Malta	1,42	0,73605	0,68766
Singapore	1,38	0,76309	0,61295
Cyprus	1,34	0,35490	0,98599
Poland	1,34	0,35490	0,98599
Jersey	1,17	1,32958	-0,15884
India	1,12	-0,44430	1,56837
Colombia	0,98	0,79756	0,18318
Ireland	0,98	0,79756	0,18318
United Arab Emirates	0,95	0,38937	0,55622
Slovak Republic	0,90	0,41641	0,48151
Indonesia	0,73	-0,40983	1,13860
Belgium	0,69	0,98291	-0,29028
Peru	0,69	0,98291	-0,29028
Austria	0,50	0,45089	0,05174
Uruguay	0,50	0,45089	0,05174
Canada	0,42	0,06974	0,35007
Bulgaria	0,21	0,63623	-0,42172
Greece	0,21	0,63623	-0,42172
Monaco	0,21	0,63623	-0,42172
Portugal	0,21	0,63623	-0,42172
Lithuania	0,02	0,10421	-0,07970
Hong Kong	-0,02	0,34261	-0,35830
Denmark	-0,02	0,46289	-0,48744
Finland	-0,02	0,46289	-0,48744
Iceland	-0,02	0,46289	-0,48744
Macau	-0,02	0,46289	-0,48744
Malaysia	-0,02	0,46289	-0,48744
Sweden	-0,02	0,46289	-0,48744
New Zealand	-0,04	-1,16409	1,12855
Russia	-0,06	-0,27694	0,21863
Czech Republic	-0,23	0,69774	-0,92620
France	-0,23	0,69774	-0,92620
Spain	-0,23	0,69774	-0,92620

United Kingdom	-0,23	0,69774	-0,92620
Gibraltar	-0,26	0,28955	-0,55316
Argentina	-0,26	0,28955	-0,55316
Japan	-0,46	-1,39680	0,93913
Australia	-0,46	0,40413	-0,86278
Ukraine	-0,54	-1,77795	1,23746
Guernsey	-0,71	0,35107	-1,05764
Hungary	-0,71	0,35107	-1,05764
Romania	-0,71	0,35107	-1,05764
Chile	-0,75	-1,42282	0,66957
Panama	-0,94	0,05745	-0,99422
Serbia	-0,96	-0,85633	-0,10222
Turkey	-0,97	-0,35074	-0,62118
Netherlands	-1,18	0,00439	-1,18908
Switzerland	-1,18	0,00439	-1,18908
Morocco	-1,20	-0,64435	-0,55777
China (People's Republic)	-1,40	-0,79482	-0,60670
Honduras	-1,66	-0,34229	-1,32052
Egypt	-2,36	-1,48817	-0,86958
Trinidad and Tobago	-2,36	-1,48817	-0,86958
Thailand	-2,37	-0,98258	-1,38854
Saudi Arabia	-3,08	-1,62287	-1,45657
British Virgin Islands	-3,77	-2,76875	-1,00563
Cayman Islands	-3,77	-2,76875	-1,00563
Brazil	-3,77	-2,76875	-1,00563
Pakistan	-3,77	-2,76875	-1,00563

Appendix B - Scores of other indices

Country	Last_amendment	Webindex (subscore data protection framework)	Privacyindex (subscore statutory protection)	Privacy index (total score)	DLA piper heatmap
Argentina	2000	5	4	2,8	3
Australia	2014	7	2	2,2	2
Austria	2000	10	3	2,3	3
Belgium	2001	10	4	2,7	4
Brazil	No DPL	5	2	2,1	1
British Virgin Islands	No DPL	0	0	0,0	1
Bulgaria	2013	0	0	0,0	2

Canada	2000	10	4	2,0	4
Cayman Islands	No DPL	0	0	0,0	1
Chile	2009	7	0	0,0	2
China (People's Republic)	No DPL	5	2	1,3	1
Colombia	2013	7	0	0,0	2
Costa Rica (2013)	2013	7	0	0,0	2
Cyprus	2003	0	3	2,3	0
Czech Republic	2000	7	3	2,5	3
Denmark	2000	7	2	2,0	2
Egypt	No DPL	5	0	0,0	2
Finland	2000	10	3	2,5	3
France	2004	10	2	1,9	4
Germany	2009	10	4	2,8	4
Gibraltar	2006	0	0	0,0	0
Greece	2012	10	3	3,1	3
Guernsey	2001	0	0	0,0	0
Honduras	2006	0	0	0,0	1
Hong Kong	2013	0	0	0,0	4
Hungary	2012	10	4	2,9	3
Iceland	2000	10	4	2,7	1
India	2013	3	1	1,9	1
Indonesia	2008	0	0	0,0	1
Ireland	2003	7	3	2,5	3
Israel	2006	7	3	2,1	3
Italy	2003	10	4	2,8	4
Japan	2005	7	1	2,2	3
Jersey	2005	0	0	0,0	0
Lithuania	2003	0	3	2,0	2
Luxembourg	2006	0	3	2,8	0
Macau	2005	0	0	0,0	2
Malaysia	2013	3	2	1,3	2
Malta	2003	0	4	2,4	2
Mauritius	2009	10	0	0,0	2
Mexico	2011	10	0	0,0	2
Monaco	2008	0	0	0,0	3
Morocco	2009	10	0	0,0	3
Netherlands	2001	10	4	2,2	3
New Zealand	1993	10	2	2,3	3
Norway	2000	10	2	2,1	4
Pakistan	No DPL	0	0	0,0	1
Panama	2012	0	0	0,0	1
Peru	2013	10	0	0,0	1
Philippines	2012	5	2	1,8	1
Poland	2007	10	4	2,3	4
Portugal	1998	7	4	2,8	4

Romania	2001	0	3	2,9	3
Russia	2006	7	2	1,3	2
Saudi Arabia	No DPL	5	0	0,0	0
Serbia	2012	0	0	0,0	3
Singapore	2014	5	1	1,4	2
Slovak Republic	2013	0	3	2,2	3
South Africa	2013	10	1	2,3	2
South Korea	2011	10	0	0,0	3
Spain	1999	10	4	2,3	4
Sweden	1998	10	2	2,1	4
Switzerland	1992	5	4	2,4	3
Taiwan	2012	0	2	1,5	3
Thailand	No DPL	3	2	1,5	1
Trinidad and Tobago	2012	0	0	0,0	0
Turkey	2012	5	0	0,0	1
Ukraine	2014	0	0	0,0	2
United Arab Emirates	2007	5	0	0,0	2
United Kingdom	2000	10	2	1,4	4
Uruguay	2009	10	0	0,0	2

Appendix C – Long list of characteristics

Sources: [96], [97], [98], [99]

This appendix displays all the characteristics in the long list. I also give a description why the characteristics are excluded. An explanation of the included characteristics can be found in the main text. The criteria for exclusion are as follows:

1. Allowance for a maximum of six characteristics to avoid too much complexity.
2. The six characteristics are in total a proxy for the four aspects privacy control in the letter of the law: control, safety, enforcement and sanctions.
3. The proxies need to be quantifiable, in the sense that they can be coded on a dummy or interval/ratio scale.
4. The characteristics are different among countries

Characteristics	Why excluded?
Data collection requirements: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	Included
Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.

96 G. Greenleaf, 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' in Volume 2 (2012).

97 OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013).

98 Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)' (1981).

99 DLA Piper, 'Global Data Protection Handbook ' in (DLA Piper, 2014).

Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	Not meeting criterion 4. A use limitation is present in all DPLs.
Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with its purpose except: a) with the consent of the data subject; or b) by the authority of law	Not meeting criterion 4. A use limitation is present in all DPLs. (this is the core of the existence of DPLs)
Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller	Not meeting criterion 3. The concept of openness is hard to quantify.
Individual access: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Individual correction: to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Accountability: A data controller should be accountable for complying with measures which give effect to the principles of the DPL.	Not meeting criterion 4. In all DPLs, data controllers are accountable.
Requirement of an independent **data protection authority** as the key element of an enforcement regime	Included
Requirement of **recourse to the courts** to enforce data privacy rights	Not meeting criterion 4. In all DPLs, one has a recourse to courts. (apart from the countries that do not have a data protection law at all)
Requirement of **restrictions on personal data exports** to countries which did not have a sufficient standard of privacy protection (defined as 'adequate')	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Collection must be the **minimum necessary** for the purpose of collection, not simply 'limited'	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
A general requirement of '**fair and lawful processing**' (not just collection) where a law outside Europe adopts the terminology of 'fair processing' and a structure based on other obligations being instances of fair processing, this is both indicative of influence by the Directive, and makes it easier for the law to be interpreted in a way which is consistent with the Directive;	Not meeting criterion 3. The concept of 'fair and lawful processing' is hard to quantify.
Requirements to notify, and sometimes provide '**prior checking**', of particular types of processing systems	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Destruction or **anonymisation** of personal data after a period	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Additional protections for particular categories of **sensitive data**	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Limits on automated decision-making, and a right to know the logic of automated data processing	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Requirement to provide '**opt-out**' of direct marketing uses of personal data	We allow for a maximum of six characteristics (criterion 1) for simplicity reasons and hence, this characteristic is excluded.
Monetary sanctions for non-compliance with the DPL	Included

Criminal sanctions for non-compliance with the DPL	Included
The requirement to install a **DPO**	Included
A **Data Breach Notification Law** requirement	Included

Appendix D – Overview of coded characteristics

Characteristic	State	Code
Requirements for collecting personal data	Prior consent needed	1
	Information duty only	.5
	No requirement / no law	0
The existence of a Data Breach Notification Law	DBNL	1
	No DBNL	0
The constitution of designated data protection authorities (DPAs) to enforce the law	DPA required and constituted	1
	No DPA	0
Every organization has to assign a data protection officer (DPO) to ensure compliance	DPO required	1
	No DPO	0
The maximum penalty for non-compliance with the regulation	Above 1M	1
	Between 100k and 1M	.75
	Between 10k and 100k	.5
	Under 10k	.25
	No penalty at all	0
Criminalization of non-compliance with the regulation	Criminalization	1
	No Criminalization	0

Table 1: characteristics and codes.

Appendix E - Scree Plot Principal Component Analysis

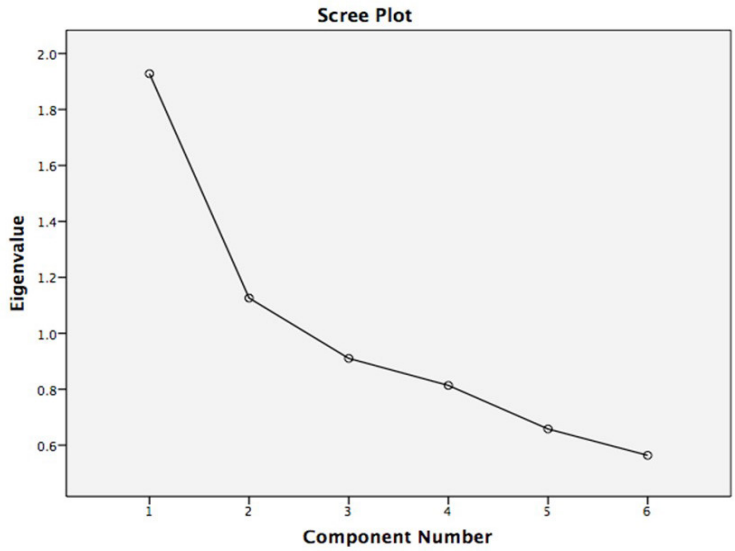

Figure 1: scree plot of principal component analysis.

* *Bernold Nieuwesteeg MSc LLM* holds degrees in both system engineering (Delft University of Technology) as well as European Law (Utrecht University). He currently is a PhD Candidate in the Law and Economics of Cyber Security, at the European Doctorate of Law and Economics at the Rotterdam Institute of Law and Economics, Erasmus University Rotterdam. The author would like to thank prof. Michel van Eeten for suggesting this research, Richard van Schaik, Tatiana Tropina, Hadi Asghari, Hanneke Luth, prof. Louis Visscher, prof. Sharon Oded, prof. Mila Versteeg, prof. Anne Meuwese, Stijn van Voorst, Maarten Stremler, Alexander Wulf, Jodie Mann, Giulia Barbanente, Shu Li, Damiano Giacometti, Amy Lan, Ahmed Arif and the other members of the EDLE community and beyond for their valuable and honest feedback.