jipitec

3 | 2016

Volume 7 (2016)
Issue 3 ISSN 2190-3387

Special Issue on Law and Governance in the Digital Era

Current Articles

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 7 Issue 3 December 2016
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J.,
Karlsruhe Institute of Technology,
Vincenz-Prießnitz-Str. 3,
76131 Karlsruhe

Prof. Dr. Axel Metzger, LL. M.,
Humboldt-Universität zu
Berlin, Unter den Linden 6,
10099 Berlin

Prof. Dr. Gerald Spindler,
Dipl.-Ökonom, Georg-August-
Universität Göttingen,
Platz der Göttinger Sieben 6,
37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Special Issue on Law and Governance in the Digital Era

Current Articles

Editorial: Special Issue on Law and Governance in the Digital Era

Data Protection and Beyond

by **Magdalena Jozwiak, Lotte Anemaet and Jilles Hazenberg**

Magdalena Jozwiak, PhD Candidate, VU Amsterdam (m.e.jozwiak@vu.nl)
Lotte Anemaet, PhD Candidate, VU Amsterdam (l.anemaet@vu.nl)
Jilles Hazenberg, PhD Candidate, University of Groningen (j.l.j.hazenberg@rug.nl).

We would like to thank Michiel Duchateau, Aurelia Colombi Ciacchi, and Martin Senftleben for their help and support.

Recommended citation: M. Jozwiak, L. Anemaet and J. Hazenberg, Editorial: Special Issue on Law and Governance in the Digital Era: Data Protection and Beyond, 7 (2016) JIPITEC 179, para 1.

A. Theme of the special issue

1 As noted by Lawrence Lessig in his seminal work *Code version 2.0*, the cyberspace is governed through a myriad of overlapping modalities: law, social norms, code, and market.[1] The contributions to this special issue explore different approaches to the governance of online content, and notably the flow of personal data and its engagement with these modalities.

2 Although the regulation of the digital domain remains a challenge, there is now a growing body of norms and institutions engaging with this task. In particular, in the European Union (EU) there is an ongoing trend of reinforcing the fundamental right to data protection, as guaranteed under Article 8 of the EU Charter. Such a trend is evidenced not only by the current reform of data protection law aimed at modernizing the EU regulatory framework but also by the judicial activity in this field, confirmed in several recent judgments such as *Digital Rights Ireland*[2], *Google Spain*[3] and *Schrems*.[4] However, it seems that regulating the internet with legal norms is being constantly challenged by the inherent characteristics of the online world. The global scope, massive scale of content exchange and data collection, and the relative anonymity of internet users stand out. Moreover, legal norms cannot keep up with the speed of technological innovations. This constellation arguably further complicates effective governance of online content. Thus, in an attempt to safeguard the European standards of protection of the fundamental right to data protection online, it is worth exploring alternative modes of governance, such as standardization or promotion of certain social norms, and to look beyond traditional legal actors and mechanisms.

1 Lawrence Lessig, *Code version 2.0*, Basic Books, 2006.

2 *Digital Rights Ireland*, C-293/12.

3 *Google Spain*, C-131/12.

4 *Schrems*, C-362/14.

3 The articles included in this special issue deal with diverging, albeit related aspects of law and governance in the digital era. They range from the issues of data-protection and private regulatory bodies such as ICANN to the governance of hate speech and legal innovation. While all innovative in their own regard, taken together these articles offer a novel perspective on law and governance in the digital era. Not only are the diverse effects of increased digitalization and trans-boundary exchanges of information on regulatory instruments analyzed, innovative proposals are made towards transforming law and governance for the digital era. What the articles show is that there is not simply one solution to adapt law and governance to modern technologies. The perspective these articles offer moves beyond the grand narratives of the transforming nature of the digital era. They delve into the specific challenges encountered in practice and mitigate particular problems in specific areas of law and governance. Together therefore, a body of work is constituted that engages with problems on the ground concerning the challenges the digital era poses to fundamental rights and changing role of law.

B. Brief discussion of the papers

4 The first paper by Bernold Nieuwesteeg discusses the topic of data protection law from a methodological perspective. The research is the first ever systematic study that unlocks six paramount characteristics in the literal text of 71 Data Protection Laws (DPLs). This paper shows that only 5 out of 71 DPLs have penalties that deter companies from non-compliance. Furthermore, compared to the U.S. states, few countries have data breach notification laws. Additionally, the author develops a privacy index reflecting the robustness of the data protection laws analyzed. Countries that are not known for their stringent privacy controls, such as Mauritius and Mexico, cover a top position of this index. Member States of the EU have DPLs with a privacy control score above average but no absolute top position.

5 The second paper by María Rún Bjarnadottir on revenge porn argues that in the current legal regime victims of revenge porn are not being protected in line with state responsibilities due to jurisdictional challenges posed by the borderless nature of internet. The paper further shows that to efficiently handle crimes committed via the internet, considerable efforts have to be made to facilitate cooperation with social media networks and other online platforms to ensure effective investigations. It can be argued that human rights protection of individuals in European countries actually lies in the hands of US technology companies.

6 The third paper by Natalie Alkiviadou points out that regulation of internet hate speech is dysfunctional, predominantly due to the vast divergence of US-European approaches to the issues of free expression both on and offline. The author argues that due to the very nature of the internet as a borderless and global entity, this normative divergence cannot be overcome so long as traditional approaches to the issue of regulation continue to be taken.

7 The fourth paper by Caroline Bricteux shows that the process introduced by the Internet Corporation for Assigned Names and Numbers to assess and allocate new generic top-level domains (gTLDs) offers a vehicle for content regulation at two levels. First, regarding the gTLD itself, objection procedures were set to allow third parties to challenge an applied-for gTLD deemed to be contrary to "general principles of international law for morality and public order" or detrimental to broadly defined communities. The real concern of these objections managed by the International Chamber of Commerce was clearly not the gTLD itself but the potentially controversial content that might be published under it. Second, these preventive measures were coupled with a strengthened anti-abuse policy for new gTLDs. These provisions, if actually enforced by ICANN, could lead to content policing by private entities without any measure to ensure due consideration of freedom of expression for domain name holders.

8 The final paper by Joshua Warburton on regulating digital content points out that the currently retracted Common European Sales Law needs to be reformulated to allow both legal development and mutual learning, whilst creating a parallel system that allows uniformity in cross-border digital transactions.

C. Relevance

9 Regulating the internet with legal norms raises several questions concerning the fundamental challenges facing this particular form of regulation. This special edition explores the new aspects of digitalization in the legal context, the way the law evolves to adapt to this changing reality, and illustrates how the digitalization affects new modes of governance. Additionally, the selection of papers looks into the alternative modes of shaping the digital reality in cases where the legal solutions turn out to be ineffective. As the JIPITEC journal aims to provide a forum for in-depth legal analysis of current issues of European intellectual property rights, E-Commerce, data protection and IT-security, this special edition on law and governance in the digital era written by authors from several European countries offers a balanced and novel perspective on

how changes stemming from increased digitalization are and could be dealt with in different legal terrains.

D. Selection of the papers

10 The papers comprising this special issue have been critically selected from participants in the international 3rd Annual Netherlands Institute for Law and Governance (NILG) PhD Roundtable Forum. The theme of this Forum was "Law and Governance in the Digital Era" and brought together PhD candidates from across the world working on issues related, but not limited to, law and governance approaches to issues emerging from all aspects of our current age of digitalization. The papers published in this special issue have gone through the regular double blind peer review process of JIPITEC.

11 The Netherlands Institute for Law and Governance is an inter-university research institute comprising the Groningen Centre for Law and Governance at the University of Groningen, the Kooijmans Institute for Law and Governance at the Free University Amsterdam, as well as the Universities of Wageningen and Twente.

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:

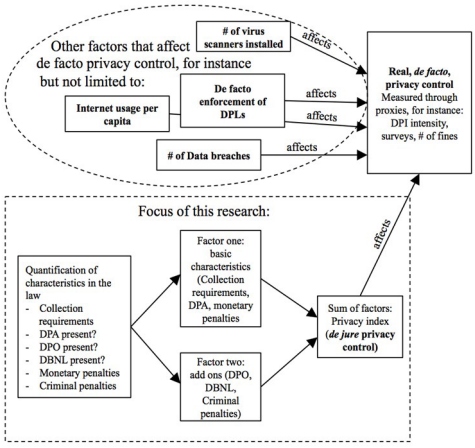

Figure 1: focus of this research

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 | # EU countries	7/10 | 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).

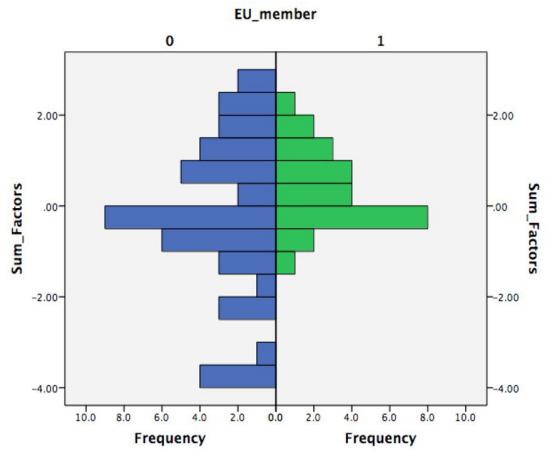

Figure 3: privacy index breakdown for EU members

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

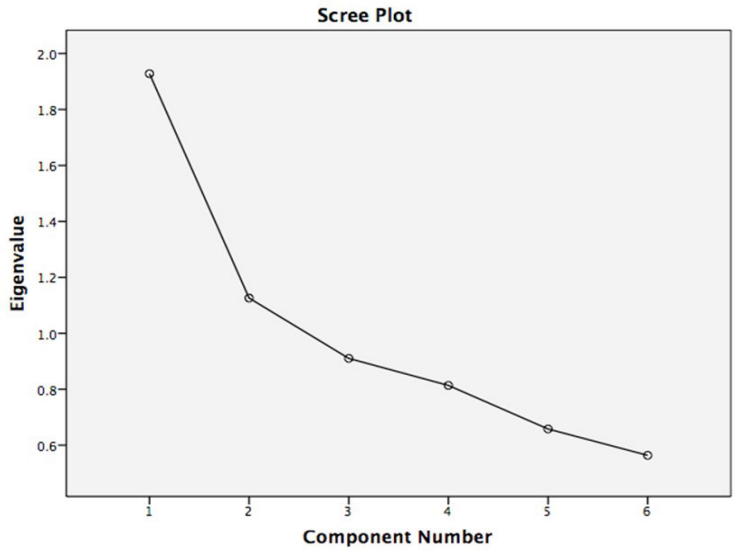

Figure 1: scree plot of principal component analysis.

* *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.

Does the Internet Limit Human Rights Protection?

The Case of Revenge Porn

by **María Rún Bjarnadóttir***

Abstract: With the enhanced distribution possibilities internet brings, online revenge porn has gained spotlight, as reports show that the act can cause serious consequences for victims. Research and reported cases have led to criticism of states lack of legal and executive means to protect victims, not least due to jurisdictional issues. Framing the matter within states responsibility to protect rights under Article 8 of the ECHR, presents the issue of possible breach of human rights obligations of states bound by the Convention. A number of domestic calls for criminalisation of posting of revenge porn have been replied with arguments for freedom of expression, worries that such means will contribute to a fragmented internet, and of a slippery slope of state interference. Further, as revenge porn touches upon the balancing between competing human rights, the possible result of outsourcing human rights assessment to private entities becomes a point of discussion in the paper.

Keywords: Human rights; Article 8 ECHR; revenge porn; freedom of expression; internet jurisdiction

Recommended citation: María Rún Bjarnadóttir, Does the Internet Limit Human Rights Protection? The Case of Revenge Porn, 7 (2016) JIPITEC 204 para 1.

A. Introduction

1 With the borderless nature of the internet[1], the ambit of state interference regarding individuals and their actions has become ever more relevant, as technology has brought about challenges in respect to jurisdiction and enforcement of domestic legislation and human rights obligations. Actions that in the offline context are clear in a legal and societal sense have proven to be challenging in the online sphere. This poses questions concerning whether human rights obligations of states are being upheld in the online sphere, or if going online enacts a different standard for states to measure up to.

2 With respect to human rights, the role of states has been described as threefold: the obligation to respect, to protect and to fulfil human rights. The obligation to protect necessitates that individuals within the jurisdiction of a state should enjoy the protection of their rights. When, due to internet architecture a state cannot uphold its role as guarantor of human rights in the online sphere, what is the acceptable outcome from a legal perspective? Does the domestic legislation have to be put aside for the greater good of a free internet, or does the situation undermine human rights protection on a domestic level? The answers to these questions can vary, but this paper will examine the case of online revenge porn.

3 With the enhanced distribution possibilities the internet brings, online revenge porn has gained more attention as reports show that the act can cause serious consequences for victims. Research and reported cases have led to criticism of states and their lack of legal and executive means to protect victims, not least due to jurisdictional issues.[2]

1 Johnson, David R. and Post, David G. Law and Borders: The Rise of Law in Cyberspace. 48 Stanford Law Review 1367. 1996.

2 Citron, D.K. Hate Crimes in Cyberspace. 2014. Harvard University Press and Hill, R. "Cyber-misogyny. Should

Domestic calls for criminalization of the posting of revenge porn have been responded to with arguments for freedom of expression, worries that such means will contribute to a fragmented internet, and of a slippery slope of state interference online. Further, as revenge porn touches upon the balancing between competing human rights, the outsourcing of human rights assessment to private entities could become a point of discussion.

4 In order to address this issue, I will first introduce and define the term revenge porn, draw out the main aspects, and summarize a trend for criminalization of such acts. Next I will address aspects of the international human rights framework highlighting the current legal obligations for states bound by the European Convention on Human Rights.[3] Thereafter I will look at jurisdictional issues that arise in cases of cross jurisdictional nature. Then I will briefly address the role of private entities such as social media platforms and hosting services before summarizing the main issues.

B. Revenge porn

I. Definition - or a lack thereof

5 The term revenge porn already poses a problem in terms of definition. Since introduced, the term has been used in public discourse as an acronym for unconsented distribution of sexual or intimate material, often with personal information attached, and intent to inflict harm or damage to the person depicted.[4] The material can have been produced with or without the consent or knowledge of the person depicted, it´s sharing intended for personal use and not wider distribution, and with or without malicious intent of the distributor. This wide variation in circumstances has led to criticism of the term claiming it to be misleading,[5] resulting in calls for a different terminology such as, "non-consensual pornography" (NCP).[6] The Oxford dictionaries definition: "revealing or sexually explicit images or videos of a person posted on the Internet, typically by a former sexual partner, without the consent of the subject and in order to cause them distress or embarrassment",[7] shows that revenge is not always a key component of the act. However, cases show that the underlying intent to harm sometimes comes from an ex-lover scorned by the end of an intimate relationship with the person depicted.[8] The definition also refers to revenge porn as a phenomenon of the internet. It could be argued that this is unprecise terminology. Most of the acts and expressions that the internet provides us access to have been a part of human society for a long time. They just took place in a narrower frame with a more limited geographical and mass distribution compared to the internet. In the 1970s, the US magazine Hustler dedicated a specific section in their publications to the publishing of photos sent in by its readers and depicted naked women along with personal information such as their names and addresses, and as cases showed, sometimes without the consent of the women depicted. The publishing of such photos in the magazine ceased in the 1980s after one of the women featured sued the magazine as she had not given her consent for publishing.[9] This differs only from online revenge porn in terms of the platform the material is shared on, not the nature of the act, highlighting that not all components of the dictionary definition are precise.

6 Although the internet did not alter the concept, it has effected the amount. Material that could become revenge porn is increasingly digitally captured and stored on smartphones, now ubiquitous amongst teenagers,[10] such devices have made video recording and photographing ourselves and others, with or without their knowledge, an everyday event. Young people only know a connected world where the internet serves as a general platform for information, entertainment and social interaction, and generally embrace evolving dynamics in social media platforms even before their parents or carers have heard of them. Today's young will also become of age in a connected world, something that differs from today's professionals, researchers and policymakers. Mistakes and misbehavior that have been a part of teenagers' and young people's growth from the dawn of time are no longer left as a memory of younger times. Today, the memories of teenagers are stored on computer clouds, on hard drives and

revenge porn be regulated in Scotland and if so, how?" SCRIPTed, 2:12. 2015.

3 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. CETS No. 5. Entry into force 3. September 1953. (ECHR).

4 Citron, D.K. Hate Crimes in Cyberspace. 2014. Harvard University Press. P. 17.

5 The Independent. Proudman, C.R. "Revenge porn: enough still isn't being done to stop it" 2. July 2014.

6 Hill, R. "Cyber-misogyny. Should revenge porn be regulated in Scotland and if so, how?" SCRIPTed, 2:12. 2015. P. 118.

7 <http://www.oxforddictionaries.com/definition/english/revenge-porn>.

8 Hill, R. "Cyber-misogyny. Should revenge porn be regulated in Scotland and if so, how?" SCRIPTed, 2:12. 2015. P. 118.

9 Lajuan and Billy Wood vs. Hustler Magazine. 736 F 2d 1084 (5th Cir.1984).

10 73% of teenagers (13-17 year old) in the United States of America have access to a smartphone according to the findings of Pew Research Center published in April. Accessible at: <http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/pi_2015-04-09_teensandtech_06/>.

uploaded to social media platforms accessible to everyone, anywhere, at any time.[11] A recent study from the Internet Watch Foundation found that young people make and share self-generated sexual material[12] from an even younger age than previous research showed. During the three month period of the study, 269 cases of material depicted children deemed in the age-group of 7-10.[13] Almost 90% of the cases examined in the report detailed that the content had been forwarded or re-disseminated in cases where the child had shared the material with someone they trusted.[14] Such dissemination entails the risk of the material becoming revenge porn.

7 The common denominator distinguishing revenge porn from other sexual material online is that the dissemination is not consented to by the person depicted. Due to the lack of consent, the material can be used to pressure the individuals depicted or cause them harm, as the publishing of revenge porn can have serious reputational and academic/professional consequences for those portrayed.[15] Even if the material may have been shared with a partner as part of an intimate relationship, that does not mean that the material has been made available to the general public, nor does it imply consent that the material can be posted online.[16] Another common denominator is that due to the borderless nature of internet, domestic legislation and enforcement has struggled to fully grasp the phenomenon leaving those who fall victim to such acts feeling unprotected and let down by their domestic justice system. Indications suggest that revenge porn affects women disproportionately - or in 90% of the cases.[17] In her 2014 book, *Hate Crimes in Cyberspace*, Citron compares views towards revenge porn and online harassment of women to dominant views on domestic violence and sexual harassment in the work place being a private matter that could not be regulated which existed up until the mid- to late 1970s.[18] Her claim that online harassment of women, including revenge porn, must be criminalized has gained traction on both sides of the Atlantic.[19]

II. A trend towards criminalization

8 On 14 October 2014, the UK Crown Prosecution Service issued guidelines on how to prosecute cases of revenge porn. It stipulated that such acts could fall within the scope of existing legislation even if there was not a specific act criminalizing revenge porn.[20] The same applied in many European countries, where the posting of revenge porn could constitute a breach of civil law, and in certain cases lead to criminal charges such as, harassment, decency and defamation, without specific reference to revenge porn. Out of 149 cases on file from eight police precincts in England and Wales during the time of the issuance of the guidelines until April 2015 when revenge porn was criminalized in the UK, six cases resulted in charges or police caution.[21]

9 In March 2015 a District Court in Iceland convicted the 18 year old ex-boyfriend of a 17 year old girl for publishing naked photos of the girl on his Facebook page for a few minutes before deleting them from the social media platform. The girl had taken the photos in question herself and sent them to the defendant during their relationship. He confessed to the act and was sentenced to 60 days suspended imprisonment, for a violation of the decency and defamation clauses of the General Penal Code,[22] causing her harm and distress under the Tort Act,[23] and found in violation of the Child Protection Act.[24] He was ordered to pay

11 See Mayer-Schönberger, V. *delete. The virtue of Forgetting in the Digital Age*. Princeton University Press. Princeton and Oxford. 2011. P. 85.

12 The IWF suggests that the term will be renewed and addressed as: "Nude or semi-nude images or videos produced by a young person of themselves engaging in erotic or sexual activity and intentionally shared by any electronic means". Internet Watch Foundation in partnership with Microsoft. *Emerging Patterns and Trends Report #1 Online-Produced Sexual Content*. 10 March 2015. P. 1.

13 Ibid P. 12.

14 Ibid P. 3.

15 Keats Citron, D. *Hate Crimes in Cyberspace*. 2014. Harvard University Press. Cambridge, Massachusetts. P. 1-17.

16 Hill, R. "Cyber-misogyny. Should revenge porn be regulated in Scotland and if so, how?" SCRIPTed, 2:12. 2015. P. 123.

17 Ibid. P. 119. See also Keats Citron, D. *Hate Crimes in Cyberspace*. 2014. Harvard University Press. Cambridge, Massachusetts. P.17.

18 Citron, D.K. Hate Crimes in Cyberspace. P. 95.

19 Ibid. P. 142 – 143.

20 The guidelines were published 14 October 2014 and are accessible at: Crown Prosecution Service (2015) < http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/>.

21 The Daily Mail. *Revenge porn laws come to force*. 13. April 2015.

22 The defendant was found in breach of Articles 209. And 233.b. of the General Penal Code No. 19/2940. Article 209 reads: "Any person who, through lewd conduct, offends people's sense of decency or causes a public scandal, shall be imprisoned for up to 4 years, or [up to 6 months]1) or fined if the offence is minor." Article 233.b. reads: "Anyone who insults or denigrates his or her spouse or ex-spouse, child or other closely-related person, the offence being considered as constituting serious defamation, shall be imprisoned for up to two years."

23 Article 26, paragraph 1of the Tort Act No. 50/1993 reads: "A party who a) by intention or by gross negligence, causes personal injury, or b) is responsible for an unlawful, malicious action directed against the freedom, peace, honour or person of another individual may be ordered to pay the injured party damages for loss of amenities of life."

24 Article 99, paragraph 3 of the Child Protection Act No. 80/2002 reads: "Any person who subjects a child to

the victim damages and to bear all costs for the court proceedings.[25] On 10 December 2015, the Icelandic Supreme Court upheld the judgement.[26] A month later, in January 2016, a bill was re-introduced to the Icelandic parliament proposing a legal amendment to the General Penal Code criminalizing revenge porn. The commentary to the draft bill states that it draws on the UK Criminal Justice and Courts Law enacted in April 2015.[27] As laid out in the commentary to the draft bill, it's presentation to parliament is rooted in the notion that such serious attacks on a person's personal integrity, protected under human rights, could not be overlooked by the criminal legislation, and despite the current legislation being applicable, further legislative actions were needed in order to provide victims of revenge porn sufficient protection to personal integrity and privacy as enshrined in the ECHR.[28]

10 This view corresponds with the picture Citron unveils concerning the application of a legal framework and remedies for victims of revenge porn in the United States of America.[29] The author claims that the current civil law remedies under tort and the copyright framework do not provide sufficient protection for individuals, as the financial cost of civil suits makes them an unrealistic choice for some.[30] Citron additionally claims that current criminal legal remedies will not protect victims of revenge porn sufficiently, as even in cases where criminal charges could be pursued against the distributor of the material, the lack of police capacity and outdated views towards online activity resulted in cases not being processed properly through the US justice system.[31] She argues that in order for states to protect victims of revenge porn, civil rights law should be amended to penalize online harassers.[32] Citron, alongside Professor Mary Ann Franks, has also drawn on social condemnation arguments in favor of criminalization of revenge porn[33] and has emphasized that invasion of privacy amounting to criminal liability is not a new notion. In their article *Revenge Porn Should be Criminalized*, Citron and Franks draw on Warren and Brandeis argument published in 1890 stating "[i]t would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law."[34]

11 A critique on the legal and executive frameworks in respect to revenge porn has gained global media attention with a string of high profile cases,[35] reports of justice systems failing to protect victims of revenge porn, and the formation of advocacy groups and Non-Governmental Organizations (NGOs) that have pushed for the criminalization of revenge porn both in the US and in European countries.[36] These efforts have been somewhat successful, resulting in legal amendments in 26 US states, Israel[37] and a number of European countries, notably England and Wales in April 2015.[38] Draft bills have been presented recently to the Scottish[39] and Icelandic[40] parliaments respectively to criminalize the posting of revenge porn, and preparatory research work has taken place in Sweden[41].

12 The first specific criminal legislation on revenge porn was passed in the US State of New Jersey in

aggressive, abusive or indecent behaviour or hurts or insults him/her is liable to fines or imprisonment for up to two years."

25 The Eastland District Court. Case No. S-36/2014. 27 March 2015.

26 The Icelandic Supreme Court. Case No. 312/2015. 10. December 2015.

27 The draft bill is accessible only in Icelandic at the website of the Icelandic Parliament: <http://www.althingi.is/altext/145/s/0011.html>.

28 Ibid.

29 U.S.

30 Keats Citron, D. *Hate Crimes in Cyberspace*. 2014. Harvard University Press. Cambridge, Massachusetts. P. 122.

31 Ibid. P. 123.

32 Ibid. P. 142.

33 Citron, D.K. and Franks, M.A. *Criminalizing Revenge Porn*. 2014. 49 *Wake Forest Law Review* 349.

34 Ibid. P. 346.

35 See for example the case of Tulisa Contostavlos: The Telegraph. Radhika Sanghani, R. "*Tulisa sex tape hell. Trolls aren´t usually to blame for revenge porn, our loved ones are*." 29. July 2014, and the case of Jennifer Lawrence Vanity Fair. "*Jennifer Lawrence calls Photo Hacking a Sex Crime*." November 2014.

36 To name some: End Revenge Porn <http://www.endrevengeporn.org/>, Civil Rights Initiative <http://www.cybercivilrights.org/> and Stop Revenge Porn Scotland <https://stoprevengepornscotland.wordpress.com/>.

37 Posting revenge porn constitutes to a breach of the Prevention of Sexual Harassment Act as amended in 2015. It classifies posting of revenge porn as sexual harassment and entails that the offender will be registered as a sex offender. See further analysis in Hill, R. "Cyber-misogyny. Should revenge porn be regulated in Scotland and if so, how?" SCRIPTed, 2:12. 2015. P. 136=137.

38 Article 33 of the Criminal Justice and Courts Act as amended of April 2015 states the disclosure of a private sexual photograph or film is an offence if the disclosure is made without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress. The act is punishable with up to two years imprisonment. <http://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted>.

39 The Abusive Behaviour and Sexual Harm (Scotland) Bill was introduced in the Parliament on 8 October 2015. - See more at: <http://www.scottish.parliament.uk/parliamentarybusiness/CurrentCommittees/93068.aspx#sthash.LrQvogRT.dpuf>.

40 An amendment bill to the General Penal Code making the posting of revenge porn criminal was re-introduced to the Parliament on 10 September 2015. Available in Icelandic at: <http://www.althingi.is/thingstorf/thingmalalistar-eftir-thingum/ferill/?ltg=145&mnr=11>.

41 Statens Offentliga Utredningar. *Integritet och straffskydd*. Stockholm. SOU 2016:7. (In Swedish).

2003.[42] Since then, 25 more States in the US have enacted legal reforms criminalizing the publishing of revenge porn. In most cases the perpetrator has to have had an intent to inflict harm and should have known that publishing the material was non-consensual.[43] This is the case in California, which is a relevant judicial precinct as many of social media sharing platforms operate under California law.[44] The legal amendments made to the UK Criminal Justice and Courts Law enacted in April 2015 are similar as the provision demands that the person was acting in bad faith and had the intention to inflict harm to the individual exposed.[45] Following the amendment[46] in April 2015, UK police authorities saw 200 cases of revenge porn reported from England and Wales.[47]

13 The NGO 'End Revenge Porn' states that the revenge porn legislation put in place in the U.S. state of Illinois provides the best protection for individuals harmed by revenge porn and at the same time provides a balanced approach to the freedom of expression protected by the First Amendment to the US Constitution.[48] In particular it is emphasized that the legislation not only applies to the person that posts the material initially, but also to subsequent distributors that should have known the material was not posted with the consent of the individual portrayed. The aim is to try and limit the distribution of the harmful material.

C. The human rights framework

14 The international framework for the promotion and protection of human rights takes place in many contexts. The overarching role of the United Nations (UN) has a global effect, with what has been described as the international bill of rights[49] and a system of promotion and protection of human rights under the ambit of the UN Human Rights Council while stretching to every aspect of the UN system.[50] Further, regional cooperation in the field of human rights has become a strong part of the drive towards strengthening of human rights in domestic legal contexts. In wider Europe, the cooperation within the Council of Europe and the development of the *Convention system*[51] following the disastrous events of the World War in the mid-20th Century. Similar systems were set up on a regional basis in other parts of the world.[52]

I. Responsibility to protect

15 It is generally undisputed that states are the main guarantors of human rights within their borders.[53] Their obligations have been described as threefold: the obligations to respect; to protect; and to fulfil

42 Keats Citron, D. *Hate Crimes in Cyberspace*. 2014. Harvard University Press. Cambridge, Massachusetts. The legal text is accessible at: <http://law.onecle.com/new-jersey/2c-the-new-jersey-code-of-criminal-justice/14-9.html>.

43 Overview of revenge porn legal acts from the US is available at the website of the NGO End Revenge Porn accessible at: <http://www.endrevengeporn.org/revenge-porn-laws/>. Similar conditions are put up in a draft legislation currently discussed in the Icelandic parliament accessible here only in Icelandic: <http://www.althingi.is/altext/145/s/0011.html>.

44 Section 647, Article 4(a) of the California Penal Code states: "Any person who intentionally distributes the image of the intimate body part or parts of another identifiable person, or an image of the person depicted engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates, under circumstances in which the persons agree or understand that the image shall remain private, the person distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress." The legislation is accessible at: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=639-653.2>.

45 An updated list of states with such legislation in the US as of 1. October 2015 is accessible at: <http://www.endrevengeporn.org/revenge-porn-laws/>.

46 Article 33 of the Criminal Justice and Courts Act states the disclosure of a private sexual photograph or film is an offence if the disclosure is made without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress. The act is punishable with up to two years imprisonment. <http://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted>.

47 The Guardian. *Revenge porn cases increase considerably, police figures reveal*. 16 July 2015.

48 A graphic description of the legislation is accessible at the NGO´s website: <http://www.endrevengeporn.org/anatomy-effective-revenge-porn-law/>.

49 The term refers to three core documents: *the Universal Declaration of Human Rights*, adopted by General Assembly resolution 217 A (III) of 10 December 1948, The International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights were adopted by the General Assembly by its resolution 2200 A (XXI) of 16 December 1966 and the International Covenant on Economic, Social and Cultural Rights adopted by General Assembly resolution 2200A (XXI) of 16 December 1966.

50 Extensive literature exists on the UN Human Rights system. See the official webpage for the Office of the High Commissioner for Human Rights: <http://www.ohchr.org/EN/Pages/Home.aspx>.

51 Extensive literature exists on the European Convention System. See the official webpage for the Convention at: <http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer>.

52 See for example Nmehielle, V.O. *The African Human Rights System: Its Laws, Practice, and Institutions*. 2001. Martinus Nijhoff. The Hague/London/New York.

53 Doswald-Beck, L. *Human Rights in Times of Conflict and Terrorism*. 2011. Oxford University Press. Oxford. P. 30. Steiner, H.J., Alston, P, Goodman, R. *International Human Rights in Context. Law, Politics, Moral. Text and Materials*. 3rd Edition. 2008. Oxford University Press. Oxford. P. 1087.

human rights.[54] The responsibility to protect[55] has been described as a duty to protect individuals from human rights violations, entailing a responsibility to proactively prevent individuals from within their jurisdiction to not suffer human rights violations by third parties, be that individuals, groups or legal persons.[56] This includes ensuring preventive measures in place in order for threats of violation of rights of individuals not to materialize. An example of this is providing for a functioning police force that has balanced investigative powers. Under the classification, state responsibility also extends to situations where safeguards fail, and violations are caused by non-state actors, effectively necessitating that states shall ensure effective remedies for those who are violated against.[57] This is further stipulated through various regional[58] human rights instruments.

16 In the Council of Europe's 2014 Recommendation *Guide to human rights for internet users*,[59] it is emphasized that states have to ensure that individuals can enjoy their rights effectively and that the obligations of states to respect, protect and promote human rights "include the oversight of private companies."[60] The Council of Europe's 2001 Cybercrime Convention[61] and recent human rights instruments, such as the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[62] explicitly address State obligations to tackle online activity through legislation and "other effective means".

17 In the case of *K.U. v. Finland* of 2 December 2009 (Application No. 2872/02), the European Court of Human Rights was presented with the case of a child whose information was posted by an anonymous person to a dating website insinuating that the child was interested in sexual relations with a grown man. No effective means were in place in order for the police to obtain information from relevant Internet Service Providers as to who posted the information, resulting in no one being found responsible for the harm caused to the child. In its findings the Court stated (Para. 42) that:

> *"...although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life..."* and that *"...these obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves..."* (Para. 43).

18 The Court further noted that there were "difficulties involved in policing modern societies", but a positive burden on the state to take measures in order to protect the applicants rights to privacy under Article 8 must be "interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case, the legislator..." while at the same time ensuring that "powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on criminal investigations and bringing offenders to justice [...]"[63]

19 Before ruling in favor of the applicant in the case, the Court noted a general principle (Para. 49) stating that:

> *"Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. [...] [I]t is nonetheless the task*

54 De Schutter, O. I*nternational Human Rights Law. Cases, Materials, Commentary. 2nd edition.* 2014. Cambridge University Press. Cambridge. P. 280 – 281.

55 This does not refer to the idea of 'Responsibility to Protect' that deals with state and international community responsibility to avert atrocities, but to the doctrinal meaning of the obligation to protect under human rights obligations of states. See further: Mégret, F. Nature of obligations. *International Human Rights Law. Second Edition.* Edited by Daniel Moeckli, Sangeeta Shah and Sandesh Sivakumaran. 2014. Oxford University Press. Oxford. P. 102.

56 Ibid.

57 De Schutter, O. *International Human Rights Law. Cases, Materials, Commentary. 2nd edition.* 2014. Cambridge University Press. Cambridge. P. 427.

58 See European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. CETS No. 5. Entry into force 3. September 1953. Article 13 *Right to an effective remedy* "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

59 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States adopted on 16. April 2014.

60 Ibid. Article 2.

61 Cybercrime Convention. CETS No.185. Entry into force 1 July 2004. Also referred to as the Budapest Convention. The Convention was the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

62 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. CETS No. 201. Entry into force 1 July 2010. Also referred to as the Lanzarote Convention.

63 *K.U. v. Finland* of 2 December 2009 (Application No. 2872/02). Excerpts from Para. 47 and 48.

of the legislator to provide the framework for reconciling the various claims which compete for protection in this context ...”

20 The Court’s findings in the case highlight the competing rights that come into play when examining revenge porn in the context of human rights – the freedom of expression on one hand, and the rights to privacy and personal integrity on the other.

II. Does the freedom of expression include the freedom to distribute harmful content?

21 Freedom of expression is closely linked to the fundamental elements of democracy and democratic principles.[64] The scope of state interferences on actions of individuals and legal persons on the internet has revolved around the core issue of freedom of expression. One of the main arguments against states setting up legal safeguards as described in Section A.II., is that categorical restrictions on the freedom of expression will undermine the free nature of the internet leading to its fragmentation and, subsequently, collapse. The general argument goes that, although well intentioned, it could prove to be a slippery slope towards censorship on the internet.[65] Some governments have tried means such as internet censorship to create “national” intranets in line with national borders to maintain their legal and sovereign powers online as well as offline.[66] This has proved challenging in practice but has not dissuaded states from pursuing such initiatives on a domestic and international level.[67] That does not alter the scope of obligation of states, as the UN Human Rights Council and the Council of Europe´s Committee of Ministers[68] have both specifically declared that human rights shall apply equally online and offline.[69]

22 The core human rights document of the United Nations is the Universal Declaration of Human Rights adopted in 1948.[70] Article 19 of the declaration stipulates that the freedom of opinion and expression applies regardless of the medium used and irrespective of frontiers. The importance of the right is further stated in Article 19 of the subsequent International Covenant on Civil and Political Rights where conditions for interference with the freedom of expression are laid out.[71] Furthermore, according to Article 20, states are obliged to restrict expression that can threaten peace and security.[72]

23 Regional cooperation and conventions in the field provide additional stakes in the safeguards of the competing rights. States that are subject to the European *Convention System* can rely on the Convention text[73] but also extensive case law from the Strasbourg Court for guidance in the balancing act between freedom of expression and the factors that can be limiting to it, such as the rights of others and

64 Ovey, C., and White, R.C.A. *Jacobs and White European Convention on Human Rights.* 3rd Edition. 2002. Oxford University Press. Oxford. P. 279.

65 See for example the Internet Governance Principles accepted at the Netmundial Conference in Brazil 2014 accessible at: <http://content.netmundial.br/contribution/internet-governance-principles/176>.

66 This includes restrictive means such as filtering and blocking. Noteworthy cases from the European Court on Human Rights such as *Ahmet Yıldırım v. Turkey* of 18. December 2012 (Application No. 3111/10) where a governmental restriction on internet access due to content that the applicant had uploaded to the internet was unlawful and therefor did not meet the standards of protection awarded by article 10 of the Convention.

67 The International Telecommunications Union met in Cairo in 2012 with the intention to update several of its treaties. A draft treaty intended to ensure stronger governmental influence in the regulation of internet infrastructure in the name of better upholding national legislation was not approved. The Guardian. Arthur, C. “*Internet remains unregulated after UN Treaty Block*.” 14. December 2012.

68 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States adopted on 16. April 2014.

69 The promotion, protection and enjoyment of human rights on the Internet. A/HRC/20/L.13.

70 Adopted by the United Nations General Assembly in Paris on 10 December 1948. Res. 217 A.

71 Article 19 of the ICCPR reads: 1) Everyone shall have the right to hold opinions without interference. 2) Everyone shall have the right to freedom of expression: this right shall include freedom to seek, receive and impart information and ideas of all kids, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as provided by law or necessary: a) For respect of the rights or reputation of others: b) For the protection of national security or of public order (ordre public), or of public health or morals.

72 Article 20 of the ICCPR reads: 1) Any propaganda for war shall be prohibited by law. 2) Any advocacy of national, racial or religious violence shall be prohibited by law.

73 Article10 of the ECHR provides: (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

societal interests.[74] The Court has established that the protection provided to the freedom of expression under Article 10 does not apply to all expression as the Court has found that expressions that go against the fundamental values of the Convention will not be tested before the Court and will be deemed under the scope of Article 17, prohibiting the misuse of the Convention.[75] Nevertheless the Court has stated that Article 10 protects not only "'information' or 'ideas' that are favorably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population."[76] Thus, offensive expression can enjoy the protection of the Convention under Article 10, although it may be subject to limitations under paragraph 2, such as in the interests of the rights of others. Rights of others includes among other things the rights protected under Article 8. The borders between these rights have been tested in a number of cases regarding defamation and media freedom of expression. In the case *RUSU v. Romania* of 8 March 2016 (Application No. 25721/04) the Court stated:

24 "[...] Lastly, in cases which require the right to respect for private life to be balanced against the right to freedom of expression, the Court considers that the outcome of the application should not, in theory, vary according to whether it has been lodged with the Court under Article 8 of the Convention by the person who was the subject of the news report, or under Article 10 by the publisher. Indeed, as a matter of principle these rights deserve equal respect [...]" (Para. 24).

25 From the above it could be established that in states bound by the ECHR, freedom of expression does not exist without limitations neither online nor offline. This indicates that there exists no such right as to exercise freedom of expression without any regard to a wider context such as the rights of others. John Stuart Mill argued: "[...] even opinions lose their immunity, when the circumstances in which they are expressed are such as to constitute [...] a positive instigation to some mischievous act."[77] Although written in another time, the principle seems to still apply. The dissemination of expression such as a photo depicting a naked person can be a perfectly valid action that deserves the full protection of the freedom of expression. But the context that such dissemination takes place in is of utmost importance when examined from a human rights perspective. In the context of revenge porn, the rights of others (the person depicted) weighs heavily against the disseminator's freedom of expression.

III. Does criminalization meet the human rights obligations of states?

26 The role of the state in a democratic society is a topic of endless discussion and the subject of many more disciplines than law. The digital dimension does not simplify the matter. Law provides only a part of the picture. Framed in national constitutions and described in international and domestic legislation, the solutions legislation provides is bound by the notion of the nation state and both its application and enforcement limited to state jurisdictions. Human rights obligations provide principles for the states, but their application depends on various factors such as political stability and culture. States' varied compliance of fundamental values further add to the lack of coherence. This colorful palette framed within the human rights framework raises the question of how much is enough for states to do in order to uphold their responsibility to protect?

27 The measurement for success in terms of effective human rights protection has usually ensued in application or enforcement of legislation. As discussed above, reports indicate that very few cases have been decided on the basis of the recent revenge porn legislation in the UK, so the effectiveness of the legislation is yet to be determined. Experience from the US shows that although some legal safeguards are in place, they may not be effective.[78] In 74% of Web Index countries, the Web Foundation found that domestic justice systems are failing to take appropriate actions for violence against women online - revenge porn being listed as an example of such violence.[79] A recent study on crimes committed

74 An overview of relevant case law regarding hate speech is accessible at: <http://echr.coe.int/Documents/FS_Hate_speech_ENG.pdf>.

75 "[T]here is no doubt that any remark directed against the Convention's underlying values would be removed from the protection of Article 10 [freedom of expression] by Article 17 [prohibition of abuse of rights]" *Seurot v. France*. Decision on the admissibility of 18 May 2004. (Application No. 57383/00).

76 In the Case *Handyside v. United Kingdom* of 7 December 1976 (Application no. 5493/72) the ECHR set out ground principles for the scope of Article 10 of the European Convention on Human Rights stating that: "Freedom of expression constitutes one of the essential foundations of [a democratic] society, one of the basic conditions for its progress and for the development of every man. Subject to paragraph 2 of Article 10 [of the European Convention on Human Rights], it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population."

77 Mill, J.S. *On liberty and Other Essays*. 1991. Oxford University Press. Oxford. P. 56.

78 Citron, D.K. *Hate Crimes in Cyberspace*. 2014. Harvard University Press. Cambridge, Massachusetts. P. 105 and 141.

79 The Broadband Commission for Digital Development. *Cyber*

via the internet by The Swedish National Council for Crime Prevention states that 96% of cases reported to the police will not go further within the justice system.[80] Out of the cases that the police examined but were found to have insufficient evidence to proceed, the main reason was that technical information was lacking to establish who the perpetrator was. According to the police, the main reason was that the social media and ISPs holding the information were not willing to provide the police with the information despite such evidence being a necessary component of the investigation. Police expressed that the biggest problem was when dealing with companies outside of Swedish jurisdiction; in particular companies that were under US jurisdiction.[81] The Icelandic police claims that it faces the same problem in dealing with sites set up to share naked photos of women and girls, and despite using the international legal assistance scheme, they have run into the same barriers as their Swedish counterparts. An Icelandic Police officer summed up the situation stating: "cases like these are difficult for the police, in particular when the websites are foreign. We cannot control the internet."[82]

D. Jurisdictional issues

28 The global nature of the internet does not abide to the same borders as states, adding a new dimension to the jurisdiction of states. [83] The internet is not wholly bound by nations, cultures, or geo-borders, but is in no way unaffected by those factors. The physical and wireless infrastructure in the transport layer of the internet is connected within and across borders of nation states, running on components that have been referred to as "code".[84] Code is such an important factor in the running of the internet, that it has famously been stated that code is law. [85] A fundamental difference between the two is that law applies only within a prescribed and clearly authorized jurisdiction, while code applies wherever it works. In light of the fact that the internet serves everyone that can access it, the application of law that is bound by the jurisdiction of nation states will barely be uniform – even if it has its basis in human rights that are intended to apply universally.

29 Scholars have argued that human rights and sovereignty cannot be fully compatible, as the international order of human rights challenges the principle of sovereignty.[86] Globalization poses challenges to the independent function of the state, and presents challenges to traditional legal theory, for instance "black box theories", that treat nation states, societies, legal systems, and legal orders as closed, impervious entities that can be studied in isolation.[87] The same theory could be applied to the internet, which is an advanced example of globalization of information as well as services.[88] This has resulted in challenges to the universal application of human rights that are not least bound to the issue of state sovereignty, posing the question: can states uphold their human rights obligations in the same capacity online and offline?[89] Furthermore, in light of the aforementioned principle of the responsibility to protect; to what extent can an individual expect that the state will fulfil and enforce a legal framework that abides by tighter boundaries than in cyberspace?

30 The scope of application is a key component of human rights instruments, just as in most conventions and contracts intended to have a bearing for the contracting parties. Most treaties specify that they apply within the scope of the contracting parties' jurisdiction.[90] Article 1 of the ECHR states that: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention". By case law the Court has established that *jurisdiction* does not only mean within the physical or geographical borders of a state,[91] although it has been claimed that

Violence against Women and Girls. A World-Wide Wake up call. 2015. P. 39.

80 *Polisanmälda brott hot och kränkningar mot enskilda personer via internet*. Rapport 2015:6. The study is accessible in Swedish with an English summary via the Council´s website at: <https://bra.se/5.5e2a4a6b14ab166759983d.html#>.

81 Ibid. P. 90.

82 Visir.is. "*Lögreglan máttlaus gagnvart nektarmyndum á netinu*" ("Police powerless facing naked photos online"). 8. September 2014. Friðrik Smári Björgvinsson, Police Officer. The original statement is in Icelandic „Svona mál eru erfið fyrir lögregluna, sérstaklega þegar um erlendar síður er að ræða. Við getum ekki stjórnað internetinu".

83 Schultz, T, "Carving up the internet", The European Journal of International Law, vol. 19, no. 4, 2008, pp. 799–839.

84 Brown, I. and Marsden, C. *Regulating Code. Good governance and better regulation in the information age*. 2013. MIT Press. London, England and Cambridge, Massachusetts.

85 Lessig, L. *Code 2.0*. 2006. Basic Books. New York. P. 5.

86 Duzinas, C. *The End of Human Rights: Critical Legal Thought at the Turn of the Century*. 2000. Hart Publishing. Oxford. P. 374 and Dickinson, R. *Universal human rights: a challenge too far. Examining Critical Perspectives on Human Rights*. Edited by Dickinson, R., Katselli, E., Murray, C., and Pedersen, O.W. 2012. Cambridge University Press. New York. P. 175.

87 Ibid. P. 177 and Twining, W. *Globalisation and Legal Theory*. 2000. London. Butterworths. P. 252.

88 Marsden, C.T. *Information and communications technologies, globalisation, and regulation*. In: *Regulating the Global Information Society*. Edited by Marsden, C.T. 2000. Routledge. London/New York. P. 2.

89 The question does not entail that states uphold their human rights obligations to the full extent offline.

90 This is not without exemption. The UN Covenant on Economic, Social and Cultural Rights does not contain a clause on jurisdiction.

91 See the ECHR factsheet on extra-territorial jurisdiction

the Court has been inconsistent in the application of the article.[92]

31 The UN International Covenant on Civil and Political Rights refers to its application as "within its territory" as well as "subject to its jurisdiction". In the *Lopez Burgos v. Uruguay* case the Human Rights Committee formed a view stating that "it would be unconscionable to so interpret the responsibility under the Article 2 of the Covenant as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory."[93] The same views are expressed in the International Court of Justice advisory opinion on the *Palestinian Wall*, noting that although jurisdiction is "primarily territorial, it may sometimes be exercised outside the national territory".[94]

32 Within the limits of the sovereignty principle, a state carries the *trias politica* powers[95] entailing a multifaceted role of states online as well as offline. It is generally undisputed that states have a legitimate claim to a role on the internet. The extent and essence of this role on the other hand is still subject to ongoing discourse.[96]

33 Parts of the internet are regulated in different capacities but no holistic regulation is in place. Parts of the infrastructure, the information highway, are regulated under telecommunications legislation while companies and entities whose operation is essential to the functioning of the internet are regulated through general legislation on companies and competition on a domestic and regional level. With the single market, the EU has taken steps towards a harmonized European regulation affecting both infrastructure, business and content, and recent judicial development indicates a more direct application of current legal frameworks to influence online services.[97] Recent efforts signal an increase in the role of companies such as media outlets and social media platforms in the online context.[98] In light of the essential part such companies play in order for states to be able to live up to their human rights obligations as described earlier, does the internet infrastructure entail that in cases as sensitive as revenge porn, that human rights protection of individuals in European countries lie in the hands of US technology companies?

E. The role of private entities

34 Private entities are of significant importance for the functioning of the internet. Internet service providers, the backbone of the internet, are entities that are largely privately owned on both sides of the Atlantic, although internet infrastructure, such as broadband deployment has across the 'OECD' membership been at least partly funded by public means. States have a multifaceted interest in the internet functioning at its best, and wear many hats to this end. One is legislative, another regulatory, but also another facilitating an environment for incentive, innovation and economic growth. However, states also have a hat branded with providing a functioning and fair justice system for their citizens. The trick is to fit this with the other – and maintain a balance so that they all stay put.

I. Intermediary[99] liability

35 Following legal uncertainties with respect to liability and responsibilities of intermediaries, legislative means were taken on both sides of the Atlantic. In the US a legal framework established with the Communications Decency Act and the **Digital Millennium Copyright Act**, describes that intermediaries will not be held accountable for user generated material on their sites unless they were notified of the material being a copyright infringement or a criminal act and did not have in place an effective notice and takedown system to relieve an infringement.[100] With respect to defamatory content, the same does not apply as section 230 of the Communications Decency Act states: "The Act provides that no provider or user of an interactive computer service shall be treated as

accessible at: <http://echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf>.

92 Milanovic, M. *Applicability of the ECHR to British soldiers in Iraq*. Cambridge Law Journal. Volume 70. Issue 1. 2011. P. 7-11.

93 HRCte, Lopez Burgos v. Uruguay Com 52/1979, Views, 29 July 1981, paragraph 12.3.

94 Doswald-Beck, L. *Human Rights in Times of Conflict and Terrorism*. 2011. Oxford University Press. Oxford. P. 11.

95 The three branches of government; legislature, executive and judiciary.

96 Brown, I. and Marsden, C. *Regulating Code. Good governance and better regulation in the information age*. 2013. MIT Press. London, England and Cambridge, Massachusetts. P. 2-4.

97 The European Court of Justice is a key player in this development with its decision in the *Google vs. Spain* (Case C-131/12) verdict entailing the right to be forgotten and the recent advisory opinion in the so called *Safe Harbour* case (Case C-362/14) effectively stating that the data sharing practices current online operations are based on are not compliant with the EU Charter on Fundamental Rights and need to be revised.

98 <http://www.osce.org/secretariat/190571>.

99 Intermediaries are key players in a functioning internet. They are internet service providers (ISPs), service providers (such as mailbox service, website hosting, cloud services) and transit providers.

100 World Intermediary Liability Map. The Center for Internet and Society. Stanford University.

the publisher or speaker of any information provided by another information content provider. No cause of action may be brought and no liability may be imposed under any State or local law."[101] Similarly, the EU adopted the e-Commerce directive[102] that has been transposed in domestic legislation within the Single Market in a fairly uniform manner making intermediaries who run a merely technical operation not liable for third party content and describes a *notice and takedown* system to be in place regarding "illegal activities" but in line with freedom of expression as protected under Article 10 in the ECHR. While the directive prohibits member states from imposing a monitoring obligation of a general nature on intermediaries, the ECJ has found that the liability exemptions under the directive do not preclude states from enacting legislation entailing civil liability for defamation for online news outlets. The Court stated that:

> *"The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 do not apply to the case of a newspaper publishing company which operates a website on which the online version of a newspaper is posted, that company being, moreover, remunerated by income generated by commercial advertisements posted on that website, since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge."*[103]

36 These findings were cited in a recent judgement from the ECHR in the *Delfi vs. Estonia* case, when the Grand Chamber of the Court upheld the findings of the Estonian Supreme Court, stating that the internet news outlet *Delfi* could be held liable on civil grounds for a defamatory comment posted on the site by a third party. The Court did not base the findings on the e-Commerce directive, as the Estonian Supreme Courts found the relevant domestic legislation transposing the E-Commerce directive inapplicable and based its findings on the company's breach of the Obligations Act.[104]

37 Both the cases concerned the civil liability of a private entity operating in a wider capacity than merely technical, meaning that they could be held liable for defamatory material generated by third party. Up until recently most states applied defamation clauses in cases of revenge porn. In light of the findings of the above mentioned cases from the ECJ and ECHR it is interesting that case law from European countries does not indicate that service providers have been challenged to bear liability in revenge porn cases. That may also suggest that most of the providers in question do not operate under the jurisdiction of European states, but rather US states, freeing them from possible liability for third party content that may be in breach of defamation clauses. Further, it remains to be seen what effect the criminalization of revenge porn will have with respect to possible liability of intermediaries in such cases.

II. Providing information on the disseminator

38 Online anonymity and the use of pseudonyms can be immensely valuable for individuals and underlying societal, democratic, or economic interests. This can be the case for people that disseminate information with an intent to expose corruption or violations. The posting of revenge porn has no such grander goals.

39 The acquisition of essential information in order to establish responsibility in revenge porn cases is reliant on cooperation with private entities that control the information in connection with their operations. Swedish police report that they have found an effective way to cooperate with some major social media platforms, while others are not as willing to cooperate.[105] Requests from European police forces in cases of revenge porn are both based on criminal charges and breach of civil code within their jurisdiction. This entails that the charges are based on a legal framework formed and enactment under legal and societal orders that in general are democratic and are a part of the European *Convention System*. It is somewhat paradoxical to claim that states that are subject to an effective human rights monitoring system would demand that the companies interfere with information contrary to human rights. Yet cases show that the companies are often faced with a complex situation as not all states are based on a democratic order, and democratic states have put forth unbalanced requests for information about individuals to companies.[106] Recent revelations show that some states engage in invasive practices in cyberspace in the interest of anti-terrorism without what seems to be a proper

101 Ibid.

102 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *OJ L 178, 17.7.2000, p. 1–16.*

103 C-291/13. Papasavvas. ECJ. 11. September 2014.

104 *Delfi v. Estonia*. GC of 16 June 2015. (Application no. 64569/09).

105 The report states also that recently the National Police Commissioner has following consultation with Facebook and Instagram gained access to the essential information. Brottsforebyggande Radet. *Polisanmälda brott hot och kränkningar mot enskilda personer via internet*. Rapport 2015:6. 2015. P. 90.

106 The Case of the Icelandic PM Birgitta Jonsdottir is summarized in a resolution of the International Parliamentary Union *PU Governing Council. 189th session. Bern, 19 October 2011*. <http://www.ipu.org/hr-e/189/is01.htm>.

balance to human rights.[107] Further, the companies that hold information due to their operations that are based within US jurisdiction are not altogether bound by the same legal framework, even though some also operate partly under EU legislation.

III. Removal of revenge porn from the online sphere

40 It has proven problematic to have revenge porn content removed from the internet.[108] In cases where the victim is the author of the material, such as in the cases of nude "selfies",[109] the victim could claim copyright over the content and thus oblige website operators to delete the content on those grounds. Such action will only apply to the website in question so the content might still be accessible on other platforms. Cases also show that victims can seek redress from those responsible for the publishing and dissemination of the content on tort grounds such as defamation and distress.[110]

41 Some companies have built efforts against revenge porn into their terms and conditions. Google issues and updates its Transparency Report[111] with information on requests the company receives from governments, copyright owners, and individuals that want their information removed from Google's search results.[112] In June 2015 Google revealed that revenge porn will also be removed from search results upon request stating that:

> *"[...] revenge porn images are intensely personal and emotionally damaging, and serve only to degrade the victims—predominantly women. So going forward, we'll honor requests from people to remove nude or sexually explicit images shared without their consent from Google Search results. This is a narrow and limited policy, similar to how we treat removal requests for other highly sensitive personal information, such as bank account numbers and signatures, that may surface in our search results."*[113]

42 The efforts by Google are likely to limit the harm caused by revenge porn, but they will not remove the content from the relevant websites, social media platforms or forums where originally posted and thus they would be subject to further distribution online.

F. Summary

43 The legal framework on revenge porn has developed fast in the last years. Despite states claiming that revenge porn was regulated under the general legislation, amendments have been made to penal codes in a number of nation states and US States specifically criminalizing what is described as revenge porn. The legal framework up until now has proven very complex to enforce, with the recent regional criminalization still to be put to the efficiency test. Information from European police forces highlight that challenges of efficiency remain in order for the justice system to sufficiently protect victims of revenge porn.

44 Private entities play a crucial role in the functioning of the internet. With the leverage provided for intermediaries with the current legal framework on both sides of the Atlantic, terms and conditions and internal rules of private entities seem to trump legal orders of sovereign states that are formed within a democratic system framed by human rights. This poses a challenge to the state obligations under the ECHR in light of the theory of the responsibility of states to protect. With the notice and takedown procedures already awarded to copyright protected material under US and EU legislation, the technical procedures for companies to take down revenge porn material are available. In the current regime it can be claimed that the protection of the human rights of victims of revenge porn remains a challenge with respect to states' responsibilities due to jurisdictional challenges posed by the borderless nature of the internet. In order to uphold their duties, a cross jurisdictional effort of states in cooperation with private entities would have to take place. Otherwise there will continue to be two different streams of legislation and technology with victims of revenge porn stuck in the middle without any chance of crossing either. That is a situation that does not align with the human rights obligations of states.

* *María Rún Bjarnadóttir* is a doctoral researcher at the University of Sussex.

107 The Snowden revelations. See for example: <http://www.theguardian.com/us-news/edward-snowden>.

108 See Chapter 5 in Citron, D.K. Hate Crimes in Cyberspace. 2014. Harvard University Press. Cambridge, Massachusetts. P. 120 – 141.

109 *A photograph that one has taken of oneself, typically one taken with a smartphone or webcam and shared via social media.* <http://www.oxforddictionaries.com/definition/english/selfie>.

110 Citron, D.K. *Hate Crimes in Cyberspace*. 2014. Harvard University Press. Cambridge, Massachusetts. P. 121 – 122.

111 Accessible at: <http://www.google.com/transparencyreport/removals/?hl=en>.

112 Accessible at: <http://www.google.com/transparencyreport/removals/europeprivacy/>.

113 19. June 2015. *Revenge Porn and Search*. <http://googlepublicpolicy.blogspot.co.uk/2015/06/revenge-porn-and-search.html>.

Regulating Internet Hate

A Flying Pig?

by **Natalie Alkiviadou***

Abstract: This paper will assess the regulation of the internet in the ambit of hate speech expressed digitally through the internet. To do so, it will provide a definitional framework of hate speech, an overview of the internet's role in the ambit of hate speech and consider the challenges in legally regulating online hate speech through a discussion of relevant case-law as well as the Additional Protocol to the Cybercrime Convention. The jurisprudential analysis will allow for a comparison of the stances adopted by the ECtHR and national courts of European countries on the one hand, and courts of the United States on the other, in the sphere under consideration. By looking at regional and national case-law and the initiative of the Council of Europe in the form of the Additional Protocol to the Cybercrime Convention, the paper seeks to provide an overview of the current state of affairs in the realm of regulating hate but also to demonstrate that such regulation, as occurring to date, is dysfunctional, predominantly due to the vast divergence of US-European approaches to the issues of free expression both on and off line. It is argued that due to the very nature of the internet as a borderless and global entity, this normative divergence cannot be overcome so long as traditional approaches to the issue of regulation continue to be taken. The paper's analysis will emanate from the premise that there exists a need to strike an equitable balance between the freedom of expression on the one hand and the freedom from discrimination on the other.

Keywords: Internet hate; regulation; hate speech; Cybercrime Convention; freedom of expression

Recommended citation: Natalie Alkiviadou, Regulating Internet Hate: A Flying Pig?, 7 (2016) JIPITEC 216 para 1.

A. Introduction

1 The internet is one of the most powerful contemporary tools used by individuals and groups to express ideas and opinions and receive and impart information.[1] It "magnifies the voice and multiplies the information within reach of everyone who has access to it."[2] Notwithstanding the positive aspects of this development in the realm of free speech and the exchange of ideas, the internet also provides a platform for the promotion and dissemination of hate.[3] In fact, the internet has seen a sharp rise in the number of extreme-right websites and

1 The number of Internet users for 2015 was 3,185,996,155: <http://www.internetlivestats.com/internet-users/> [Accessed 28th June 2016].

2 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye (22 May 2015) A/HRC/29/32, para 11.

3 Fernne Brennan, 'Legislating against Internet Race Hate' (2009) 18 Information and Communications Technology Law 2, 123.

activity.[4] As well as facilitating the promotion of hate, the internet has also strengthened the far-right movement more generally by bringing hate groups together, converging the lines of previous fragmentation, thereby contributing to the creation of a "collective identity that is so important to movement cohesiveness."[5] This has occurred on an international level, "facilitating a potential global racist subculture."[6] Although hate existed long before the creation of the internet, this technological advancement has provided an effective and accessible means of communication and expression for hate groups and individuals whilst simultaneously adding a new dimension to the problem of regulating hate,[7] particularly due to the nature of the internet as a global and, to an extent, anonymous medium. It is the anonymity of the internet which deeply hampers the implementation of traditional legal procedures and enforcement of traditional laws,[8] as the perpetrator cannot readily be determined; whilst the global nature of the internet means that, even if a perpetrator can be identified, bringing him or her to justice may not be possible due to jurisdictional limitations.[9] Thus, technological advances in the form of the internet have altered our conceptualisation of a State which habitually had jurisdiction over the activities occurring within its boundaries. To put it simply, this medium knows no borders.

2 In light of the significant role of the internet *vis-à-vis* the promotion and dissemination of hate, this paper will look at the issue of regulating the internet in the ambit of hate speech as digitally expressed by individuals and groups. To do so, it will provide a definitional framework of hate speech, an overview of the internet's role in the ambit of hate speech and consider the challenges in legally regulating online hate speech through a discussion of relevant case-law as well as the Additional Protocol to the Cybercrime Convention. The paper's analysis emanates from the premise that, if the internet is to be dealt with in a manner which reflects an adherence to principles such as non-discrimination and equality, "a new template for addressing cross-border contracts"[10] is urgently required. To this end, a comprehensive and unified multijurisdictional approach must be adopted. However, this has proved difficult to date particularly given the stark contrast in the approach *vis-à-vis* free speech adopted by the United States of America (USA), on the one hand, and Europe on the other. Essentially, as will be reflected hereinafter, it is the conceptual understanding of the scope of the freedom of expression which deeply hampers the creation of an effective regulatory framework for internet hate speech.

B. Definitional Framework: Hate Speech

3 Hate speech does not enjoy a universally accepted definition,[11] with most States and institutions adopting their own definitions,[12] notwithstanding that the term is often incorporated in legal, policy, and academic documents.[13] Although non-binding, one of the few documents which has sought to define hate speech is the Recommendation of the Council of Europe Committee of Ministers on hate speech.[14] It states that this term is to be "understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expression by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin." Interestingly, this definition incorporates the justification of hatred as well as its spreading, incitement and promotion, allowing for a broad spectrum of intentions to fall within its definition. However, it leaves out characteristics such as sexual orientation, gender identity and disability. Hate speech has also been mentioned, but not defined, by the European Court of Human Rights (ECtHR). For example, the Court has refers to hate speech as: "all forms of expression which spread, incite, promote or justify hatred based on intolerance including religious intolerance."[15] In

4 James Bank, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 233.

5 Barbara Perry & Patrick Olsson ' Cyberhate: The Globalization of Hate' 18 Information and Communications Technology Law 2, 185.

6 Ibid.

7 Dragos Cucereanu 'Aspects of Regulating Freedom of Expression on the Internet' (Intersentia 2008) 7.

8 James Banks, 'Regulating hate speech online' (2010) 24 Computers & Technology 3, 233.

9 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2, 783.

10 Michael L. Rustad & Tomas H. Koenig, 'Harmonizing Internet Law: Lessons from Europe' (2006) 9 Journal of Internet Law 11, 3.

11 European Court of Human Rights, Fact Sheet on Hate Speech, 2013, 1.

12 Council of Europe Committee of Experts for the Development of Human Rights 2007, Chapter IV, pg.123, para.4.

13 Tarlach McGonagle, 'The Council of Europe against Online Hate Speech: Conundrums and Challenges' Expert Paper, Institute for Information Law, Faculty of Law, <http://hub.coe.int/c/document_library/get_file?uuid=62fab806-724e-435a-b7a5-153ce2b57c18&groupId=10227> [accessed 15th August 2015] 3.

14 Council of Europe's Committee of Ministers Recommendation on Hate Speech 97 (20).

15 Gűndűz v Turkey, App. No 35071/97 (ECHR, 4 December 2003) para. 40, Erbakan v Turkey, App. No 59405/00, (6 July 2006) para.56.

Vejedland v Sweden, in the framework of homophobic speech, the Court held that it is not necessary for the speech "to directly recommend individuals to commit hateful acts",[16] since attacks on persons can be committed by "insulting, holding up to ridicule or slandering specific groups of the population"[17] and that speech used in an irresponsible manner may not be worthy of protection.[18] Through this case, the Court drew the correlation between hate speech and the negative effects it can have on its victims, demonstrating that it is not merely an abstract notion, but one with potential to cause harm. In addition, the Fundamental Rights Agency (FRA) of the European Union has offered two separate definitions of hate speech with the first being that it "refers to the incitement and encouragement of hatred, discrimination or hostility towards an individual that is motivated by prejudice against that person because of a particular characteristic."[19] In its 2009 Report, the FRA held that the term hate speech, as used in the particular section "includes a broader spectrum of verbal acts including disrespectful public discourse."[20] The problematic part of this definition is the broad reference to disrespectful public discourse, especially since institutions such as the ECtHR extend the freedom of expression to ideas that "shock, offend or disturb."[21] The Council Framework Decision 2008/913/JHA of 28 November 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia does not directly define hate speech, but instead prohibits different forms of expression and acts that fall within the framework of "Offences Concerning Racism and Xenophobia."[22] More specifically, Article 1 therein holds that each Member State shall punish the public incitement to violence or hatred directed against a group of persons or a member of a group defined by reference to race, colour, religion, descent or national or ethnic origin, the commission of such an act through public dissemination of material as well as the acts of publicly condoning, denying or grossly trivialising particular crimes such as genocide. This definition could be used in the realm of hate speech but is limited only to particular groups, leaving out others such as sexual minorities. In addition, the threshold of this definition is set to hatred or violence, and does not integrate other "softer" elements of hate speech, such as discrimination. No particular reference to internet hate was made in the above document; however, nothing in its wording prevents it from being used for cases of internet hate. In 2016, the "Code of Conduct on Countering Illegal Hate Speech Online" was signed by different IT companies and the European Commission. This document underlines that the aforementioned Council Framework Decision must be enforced by Member States in online, as well as offline, environments. In the framework of academic commentary, there has been a plethora of definitions put forth to describe hate speech. According to Mari Matsuda, hate speech contains a tripartite definition, namely that the message is "of racial inferiority, the message is directed against historically oppressed groups and the message is persecutory, hateful and degrading."[23] Wrestling offers a broad interpretation of hate speech including "virtually all racist and related declensions of noxious, identity-assailing expression could be brought within the wide embrace of the term."[24] Alexander Tsesis has described it as a "societal virus",[25] while Rodney Smolla refers to the lack of contribution hate speech makes to the development of society since it "cannot contribute to a societal dialogue and therefore can be ethically curtailed."[26] Scholars, such as Kent Greenawalt have argued about the damaging consequences of such speech, arguing that "epithets and slurs that reflect stereotypes about race, ethnic group, religion and gender may reinforce prejudices and feelings of inferiority in seriously harmful ways."[27] In discussing bans on racist speech, Post examines several arguments that have been put forth as justifications for such bans including, the "intrinsic harm of racist speech"[28] insofar as there is an "elemental wrongness"[29] to such expression, the infliction of harm to particular groups and individuals, as well as to the marketplace

16 Vejdeland and Others v Sweden, App. No 1813/07 (ECHR 09 February 2012) para.54.

17 Ibid. para.55.

18 Ibid.

19 Hate Speech and Hate Crimes against LGBT Persons, Fundamental Rights Agency, 1.

20 Homophobia and Discrimination on Grounds of Sexual Orientation and Gender Identity in the EU Member States: Part II - The Social Situation, Fundamental Rights Agency, 44.

21 The Observer and The Guardian v The United Kingdom, App. no 13585/88 (ECHR, 26 November 1991) para. 59.

22 Article 1, Council Framework Decision 2008/913/JHA of 28 November 2008 on Combatting Certain Forms and Expressions of Racism and Xenophobia.

23 Mark Slagle, 'An Ethical Exploration of Free Expression and the Problem of Hate Speech' 24 Journal of Mass Media Ethics, 242.

24 Tarlach McGonagle, 'Wresting Racial Equality from Tolerance of Hate Speech' (2001) 23 Dublin University Law Journal 21, 4.

25 Mark Slagle, 'An Ethical Exploration of Free Expression and the Problem of Hate Speech' 24 Journal of Mass Media Ethics, 242.

26 Mark Slagle, 'An Ethical Exploration of Free Expression and the Problem of Hate Speech' 24 Journal of Mass Media Ethics, 242.

27 Kent Greenawalt, 'Speech, Crime and the Uses of Language' (1989 New York: OUP), Chapter 2.

28 Robert C. Post, 'Racist Speech, Democracy and the First Amendment' (1990-1991) 32 William and Mary Law Review 267, 272.

29 Post R.C, 'Racist Speech, Democracy and the First Amendment' (1990-1991) 32 William and Mary Law Review 267, 272 quoting Wright 'Racist Speech and the First Amendment' 9 Miss. C.L.Rev. 1 (1988).

of ideas.[30]

4 From the above definitions and the variations therein, although some common elements can be discerned, it could be argued that "hate speech seems to be whatever people choose it to mean."[31] For the purpose of this paper, and taking into consideration that there is no one universal definition of hate speech, a broad definitional basis is embraced. As such, hate speech is hereinafter considered to mean speech that is targeted towards individuals due to their particular characteristics, such as race, ethnic origin, nationality, religion, language, sexual orientation, gender identity and/or disability.

C. The Role of the Internet vis-à-vis Hate Speech

5 The significant role of the internet in any modern society was recognised by the European Court of Human Rights in *Times Newspaper Ltd v UK*:

> *"in light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally."*[32]

6 However, as noted above, the internet can also result in harmful expression and this reality began to surface predominantly during the 1990s. In 1994, the UN Secretary General noted that new technologies such as computer programmes, video games and the Minitel system in France were used to disseminate anti-Semitic ideas.[33] In 1995, the UN Special Rapporteur on contemporary forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance recorded the growing use of electronic media for purposes of international communications between far-right groups.[34] In 1996, the UN Secretary General officially recognised the use of the internet and electronic mail as being increasingly used by racist organisations to spread their ideology.[35] In 1997, the aforementioned Rapporteur noted that "the Internet has already captured the imagination of people with a message, including purveyors of hate, racists and anti-Semites."[36] The first racist website to enter the online world was *Stormfront.org* set up by a former *Ku Klux Klan* member and launched in 1995.[37] The dramatic rise of internet hate is reflected by the figures gathered by the *Simon Wiesenthal Centre* which, in 1995 recorded only one racist website[38] whereas by 2011 its Digital Terrorism and Hate Report had found 14,000 websites, forums and social networks which promoted hate.[39] However, these figures must be considered with a degree of caution, since monitoring becomes more complicated given that websites surface and re-surface at a very fast pace.[40] Websites are not the only sub-tool of the internet with forums, blogs, social networking sites, emails, newsletters, chat rooms and online games being used and abused by extremist groups. Social networking sites have become "breeding grounds for racist and far-right extremist groups to spread their propaganda",[41] with the sheer number of users, the accessibility to such platforms and the lack of pre-screening of posts or the establishment of, *inter alia*, Facebook groups, rendering the prospect of regulation a daunting one. In 2008, following a complaint lodged by Martin Shulz, Facebook banned several pages used by Italian extremists to promote violence against Roma.[42] It must be noted that those who spread hate speech may use the internet to harass the victims of their rhetoric directly, to communicate amongst

30 Ibid. 273.

31 Roger Kiska, 'Hate Speech: A Comparison between the European Court of Human Rights and the United States Supreme Court Jurisprudence' (2012) 25 Regent University Law Review 107,1 10.

32 Times Newspaper Ltd (Nos 1 & 2) v UK, (10 March 2009) Application nos 3002/03 and 23676/03, para.27.

33 Secretary-General, Elimination of Racism and Racial Discrimination, UN GA, 48th Sess., UN Doc, A/49/677 (1994).

34 Maurice Glele-Ahanhanzo, Implementation of the Programme of Action for the Second Decade to Combat Racism and Racial Discrimination – Report of the UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, CHR Res.1994/64, UN ESCOR, 51st Sess., UN Doc. E/CH.4/1995/78 (1995).

35 Secretary – General, Elimination of Racism and Racial Discrimination: Measures to Combat Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, UN GA, 51st Sess. UN Doc. A/51/301 (1996).

36 Maurice Glele-Ahanhanzo, Implementation of the Programme of Action for the Second Decade to Combat Racism and Racial Discrimination – Report of the UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, CHR Res.1996/21, UN ESCOR, 53rd Sess., UN Doc. E/CN.4/1997/71 (1997).

37 Simon Wiesenthal Report: Online Terror and Hate – The First Decade: <http://www.wiesenthal.com/atf/cf/%7BDFD2AAC1-2ADE-428A-9263-35234229D8D8%7D/IREPORT.PDF> pg. 7.

38 Simon Wiesenthal Report: Online Terror and Hate – The First Decade: <http://www.wiesenthal.com/atf/cf/%7BDFD2AAC1-2ADE-428A-9263-35234229D8D8%7D/IREPORT.PDF> pg. 3.

39 Simon Wiesenthal Report: Digital Terrorism and Hate Report 2011.

40 Barbara Perry & Patrick Olsson 'Cyberhate: The Globalization of Hate' 18 Information and Communications Technology Law 2, 188.

41 James Bank, 'Regulating Hate Speech Online' (2010) International Review of Law, 24 Computers & Technology 3, 234.

42 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008), 16.

themselves and build up a "sense of belonging and social identity"[43] to a unified movement, but also to recruit new members through the dissemination of their ideology to unsuspecting users who may be confronted with such speech through, amongst others, web links or emails.[44] Further, hate groups attract new members, particularly young people, through the use of innovative methods such as online hate games including "Ethnic Cleaning" and "Shoot the Blacks".

7 Thus, the internet which has been named the "network of networks"[45] offers endless possibilities for hate groups to communicate with each other, recruit new members and harass their victims due to its vastness, accessibility and nature as a boundary-free entity governed by no single institution or State. It is the very nature of the internet, and the fact that its effective regulation is contingent upon a common universal approach, which has contributed to its regulation posing a particularly challenging problem for law-makers.

D. Regulation of Online Hate: An Overview

8 Commencing in the 1990s, several calls were made for more to be done regarding regulating online hate speech. In 1996, the European Commission against Racism and Intolerance (ECRI) requested Council of Europe States to ensure that expression disseminated through the internet which incites discrimination, hate or violence against racial, ethnic, national or religious groups be classed by national law as criminal offences and that such offences should also incorporate the production, dissemination and storage for distribution of harmful material.[46] In 2000, ECRI issued a general policy recommendation on combating the dissemination of racist, xenophobic and anti-Semitic material via the internet, recommending that States ensure that relevant national laws also apply to material uploaded on the internet and to prosecute the perpetrators of relevant offences.[47] ECRI also recommended the clarification of the responsibility of the content host, content provider and site publishers in the framework of the dissemination of racist, xenophobic, and anti-Semitic content over the internet.[48] In 2001, the Declaration and Programme of Action of the Third World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance noted that States must "implement legal sanctions, in accordance with relevant international human rights law, in respect of incitement to racial hatred through new information and communication technologies, including the internet."[49] In 2003, partly as a response to the fact that the ECRI recommendations on internet hate regulation were not adhered to by the Member States, the Council of Europe took the first and only concrete step in seeking to provide a harmonised approach to the regulation of online hate speech, through its Additional Protocol to the Cybercrime Convention. It must be noted that, although there is a general consensus amongst organisations such as the Council of Europe, the United Nations, the European Union and the Organisation for Security and Co-operation in Europe, that internet hate should be regulated,[50] the UN Special Rapporteur on Freedom of Expression held that excessive regulation of the internet in order to "preserve the moral fabric and cultural identity of societies is paternalistic."[51] However, no extrapolation was made on what could fall within the framework of excessive regulation and, thus, no further conclusions can be drawn thereof.

9 It is common practice for States to take the position that "what is illegal and punishable in an offline format must also be treated as illegal and punishable online."[52] However, as the internet is owned by nobody and everybody and knows no physical, electronic, cyber, abstract or other boundaries, it allows its users to transmit messages beyond any such boundaries; thereby, rendering control, censorship and regulation a difficult task.

43 Barbara Perry & Patrick Olsson 'Cyberhate: The Globalization of Hate' 18 Information and Communications Technology Law 2, 192.

44 Priscilla Marie Meddaugh & Jack Kay 'Hate Speech or Reasonable Racism? The Other Stormfront' (2009) 24 Journal of Mass Media Ethics: Exploring Questions of Media Morality 4, 252.

45 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 22.

46 ECRI General Policy Recommendation Number 1 on Combatting Racism, Xenophobia, Anti-Semitism and Intolerance (4 October 1996), CRI(96) 43 rev.

47 ECRI General Policy Recommendation N°6: Combating the Dissemination of Racist, Xenophobic and Antisemitic Material via the Internet (15 December 2000) CRI(2001)1.

48 Ibid. pg.5.

49 Declaration and Programme of Action: <http://www.un.org/WCAR/durban.pdf> [Accessed 25 October 2015].

50 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 67.

51 Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1997/26 (28 January 1998) E/CN.4/1998/40, para. 45.

52 Yaman Akdeniz 'Racism on the Internet' (Council of Europe publishing 2009) 21.

E. The Jurisdictional Problem of Regulating Online Hate

10 It is generally accepted that the complexities created by jurisdictional issues constitute the biggest challenge in the sphere of regulating online hate.[53] This is because the internet is not marked by boundaries, cannot be controlled or censored comprehensively by individual States in particular situations and, as a consequence, questions are raised as to "which law should apply and how to delimit competing jurisdictions."[54] This results in States finding it "difficult to govern and control the flow of information inside and outside their nation states."[55] More specifically, regulation problems arise where, for purposes of the present discussion, the hateful material is created within a State which does not prohibit the dissemination of xenophobic or racist material on the internet but, due to the boundary-free nature of the internet it is accessible to or, in fact, uploaded by persons residing in a Contracting State. In fact, on a technical level, it is a relatively simple task for individuals who wish to publish information that may be prohibited in some countries, including their own, to go "forum shopping" by choosing internet service providers which are located in countries which permit such content so as to be sure that, notwithstanding potential restrictions in some jurisdictions, the material will be available online.[56] Forum shopping results in the establishment of hate havens, which individuals and groups conveniently choose as hosts for their material. This is the situation in the USA, which is a haven for hate websites.[57] The majority of hate websites are based in the USA and these include those which seek to avoid anti-hate legislation in their own country.[58] Countries such as Spain, have sought to overcome the consequences of such havens by allowing the judiciary to block internet sites that do not adhere to Spanish law.[59] However, this method presupposes the continuous monitoring of internet sites that are in violation of national law, a huge and complex task which cannot possibly be efficiently carried out. Either way, the availability of havens essentially results in the erosion of the weight and role of national laws that seek to restrict online hate as they can be circumvented by carrying out internet activity in, for example, countries which place more emphasis on the freedom of expression rather than on the negative effects of hate. This results in a "de facto extraterritorial application of the laws of some countries known for their robust protection of freedom of expression",[60] which in turn contributes to the weakening of the more general principle of State sovereignty *vis-à-vis* the regulation of internet hate.

11 In *Perrin v UK*, the ECtHR was confronted with the question of jurisdiction in the sphere of the internet. It interpreted jurisdiction in a broad sense, arguing that the fact that the applicant's material was uploaded by the applicant on a website operated and legal in the USA did not free the applicant of his responsibilities under UK law which prohibited such material.[61]As such, the Court considered itself to have competence *ratione loci* regarding material uploaded[62] on the internet, notwithstanding the location in which the material was uploaded. Furthermore, certain countries have also sought to overcome the issue of jurisdiction on a national level. For example, in Germany the Federal Court held that all material uploaded on the world wide web is answerable to German anti-hate legislation regardless of the country in which this material was created, with the only element posing any sort of significance being its accessibility to German internet users.[63]

12 The variation in approaches of different States to the issue of hateful expression lies at the heart of jurisdictional limitations in the ambit of regulating internet hate. A State's approach to the issue of restricting forms of expression will be affected by its own "political, moral, cultural, historical and constitutional values"[64] and it is, in fact, this sharp divergence of legal culture in the realm of speech between the USA and Europe which has hindered the efficacy of any regulatory measures and which has rendered the issue of jurisdiction a serious obstacle thereto. As will be reflected in the discussion on the Additional Protocol to the Cybercrime Convention, the variation of approaches between the USA and

53 Fernne Brennan, 'Legislating against Internet Race Hate' (2009) 18 Information and Communications Technology Law 2, 276.

54 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 254.

55 Ibid. 22.

56 Ibid.354.

57 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2, 822.

58 Agence – France Press, 'Neo-Nazi websites reported to flee Germany' N.Y. Times (August 21 2000).

59 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2, 784.

60 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 254.

61 Perrin v UK, App. No 5446/03 (18 October 2005).

62 Nina Vajic & Panayiotis Voyatzis, 'The Internet and Freedom of Expression: a brave new world and the ECtHR's evolving case-law.' In '*Freedom of Expression: Essays in Honour of Nicolas Bratza*' (eds. 2012 Wolf Legal Publishers) 401.

63 Fernne Brennan, 'Legislating against Internet Race Hate' (2009) 18 Information and Communications Technology Law 2, 263.

64 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 16.

Europe has limited any formulation of a functioning regulatory framework of online hate simply because the former adheres to an almost absolutist protection of free speech as per the First Amendment, with the latter seeking restrictions for purposes of ensuring that other fundamental rights and freedoms are exercised, such as that of non-discrimination. More specifically, in the USA, hate speech can be proscribed if it constitutes a "true threat", a test which was developed in the case of *Brandenburg v Ohio*, and underlines that free speech can only be limited insofar as advocacy of the use of force "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[65] However, the possibility of this test's application in the sphere of the internet is doubtful, since the internet's "impersonal contact cannot be seen as readily meeting the true threat requirement of being likely to incite imminent lawless action."[66] As well as the true threat test, "fighting words" can also be prohibited under US law, a restriction developed in the case of *Chaplinsky v New Hampshire*. There, the Court held that expression can be restricted if it is made up of fighting words which were deemed to be those which "inflict injury or tend to incite an immediate breach of the peace".[67] This doctrine was considered within the framework of racist expression in *R.A.V. v City of Saint Paul*, in which the Supreme Court held that an ordinance which criminalised the placing of symbols, such as a burning cross or a Nazi swastika on a public or private property, was unconstitutional under the First Amendment.[68] The Court held the ordinance unconstitutional because it "imposes special prohibitions on those speakers who express views on the disfavored subjects of race, color, creed, religion or gender"[69] and that St Paul's objective to "communicate to minority groups that it does not condone the group hatred of bias-motivated speech does not justify selectively silencing speech on the basis of its content."[70] Thus, given that the Supreme Court was willing to find that the burning of a cross on a black family's lawn did not fall within the ambit of fighting words and was thus acceptable speech, it seems improbable that the threshold incorporated from the fighting words test could be derived from racist or other hateful speech that takes place online.

13 Comparatively speaking, freedom of expression in Europe is more readily limited for purposes of preventing not only violence, but also discrimination and hate targeted towards an individual or a group which has a particular characteristic. This is reflected firstly by the fact that the freedom of expression, as protected by Article 10 of the European Convention on Human Rights, is marked by a series of limitation grounds. Subsequently, the ECtHR developed a multi-fold test to be applied in considering whether the freedom of expression should be permitted including: ascertaining whether the limitation has a legitimate aim; is proportional to the aim pursued; is necessary in a democratic society; and is effectuated for purposes of, *inter alia*, protecting the rights and freedoms of others. To date, the Court's jurisprudence shows no tolerance for hate speech as reflected in a variety of cases,[71] one of which will be discussed further below. When seeking to restrict hateful expression, the Court usually opts to use the limitation grounds found in Article 10, but has in some situations[72] applied the prohibition of the abuse of rights clause of the ECHR. As noted by the ECtHR, States must "fight against abuses, committed in the exercise of freedom of speech, that openly target democratic values."[73] Thus, even though this freedom is undoubtedly significant, it must nevertheless coexist harmoniously with other rights and freedoms, with democracy having the duty militantly to protect itself from the abuse of expressive freedom.

14 Although it is beyond the scope of this paper to carry out an extensive comparative analysis of the stances adopted by the USA and Europe, as an entity in the form of the Council of Europe as well as individual countries which have harmonised their legislation with the European Convention on Human Rights, it is evident that the approaches of the two are oceans away from each other. With such oceans constituting dividing lines, and taking into account the necessity of coherence *vis-à -vis* online regulation given the nature of the internet, the question of jurisdiction remains a key issue.

F. Case-Law on Regulating Internet Hate

I. European Court of Human Rights

15 In a recent case on online defamation, the Court acknowledged that although "important benefits

65 Brandenburg v Ohio, 395 U.S. 447,445-49 (1969).

66 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2 810.

67 Chaplinsky v New Hampshired, 315 U.S. 568, 572 (1942).

68 R. A. V. v. St. Paul 505 U.S. 377, 378 (1992).

69 R. A. V. v. St. Paul 505 U.S. 377, 391-393 (1992).

70 R. A. V. v. St. Paul 505 U.S. 377, 393 (1992).

71 See, inter alia, Norwood v UK (Application no. 23131/03) (16 November 2004) and Féret v Belgium (application no. 15615/07) (16 July 2009).

72 Norwood v UK (Application no. 23131/03) (16 November 2004).

73 Jean-François Flauss, 'The European Court of Human Rights and the Freedom of Expression' (2009) 84 Indiana Law Journal, 809, 837.

can be derived from the internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained."[74] Although this statement was made within the framework of defamatory speech, reference was made to other unlawful speech, thereby, incorporating hate speech as well. Moreover, it is clear that the Court is mindful that this medium can establish a framework through which unacceptable speech can emanate. Cases have come about during which the Court made some significant distinctions on the general nature of the internet and the consequences arising thereof. For example, in *K.U. v Finland*, which dealt with a minor who was the subject of an advertisement of a sexual nature on an internet dating site, the Court held that the anonymous character of the internet which could be used by individuals for the committal of criminal offences meant that the State has a positive obligation to provide a legal framework through which anonymous perpetrators could be identified and prosecuted.[75] It was also noted that the sheer vastness of the internet means that regulation is a tricky task and could potentially affect the rights and freedoms found in the ECHR. More specifically, in *Perrin v UK*, which dealt with obscene material, the Court noted that:

> *"the electronic network, serving billions of users worldwide is not and potentially will never be subject to the same regulations and control. The risk of harm posed by content and communications on the internet to the exercise and enjoyment of human rights and freedoms....is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the internet may differ. The latter undeniably have to be adjusted according to technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned."*[76]

16 In relation to how the Court has considered the question of the internet and the freedom of expression, it could be argued that although the ECtHR has looked at several free speech cases which are interrelated to the internet, it has not yet established a coherent and all-encompassing approach to the issue. The Court has been faced with just one case relevant to the theme of internet hate, during which it decided to replicate its positions and stances developed in general Article 10 cases in internet cases. Specifically, in *Féret v Belgium*, the Court dealt with racist and xenophobic statements of the leader of the far-right party *Front National-National Front*, which were transmitted by him during his party's election campaign through leaflets and posters as well as being posted on his internet site. The Court applied already established principles, such as the fact that political speech that stirred hatred based on religious, ethnic or cultural prejudices was a threat to social peace and political stability in democratic States.[77] Thus, the fact that the internet was used as one of the communication mediums did not affect the Court's stance on hate speech and nor did it make particular distinctions as to the effect of the internet on the dissemination of these ideas.[78] However, it is too soon to draw concrete conclusions on the Court's stance on online hate and whether it will, in fact, continue simply transposing its Article 10 reasoning without any further qualifications as to the relevance of the nature of the medium used. As noted, "as the wide picture of internet related issues is still unfolding, it is too early to evaluate the Court's position in this regard."[79]

II. National Case-Law

17 There have been some cases which have dealt with the regulation of online hate, particularly in the form of anti-Semitic material. These cases have demonstrated the difficulty in ensuring regulation of such material given the antithesis of approaches adopted by European countries, on the one hand, and the USA on the other. This has resulted in problems within the realm of the jurisdictional and technical implementation of regulatory orders.

18 In 1999, Frederick Toben was arrested during a visit to Germany for violating German law because of the anti-Semitic material he uploaded onto his website. A lower court found that Germany could not regulate the website as it was based in Australia, but this was later reversed by Germany's High Court which held that "German authorities may take legal action against foreigners who upload content that is illegal in Germany – even though the Websites may be located elsewhere."[80] This case reflected

74 Delfi AS vs Estonia, (Application no. 64569/09) (16 June 2015) para.110.

75 K.U. v Finland, (Application no. 2872/02) (2 March 2009) para 48-49.

76 Perrin v UK (Application no. 5446/03) (10 October 2005) para.63.

77 Féret v Belgium, App. no. 15615/07, (ECHR, 16 July 2009) para.73.

78 Nina Vajic & Panayiotis Voyatzis, 'The Internet and Freedom of Expression: A Brave New World and the ECtHR's Evolving Case-Law.' In '*Freedom of Expression: Essays in Honour of Nicolas Bratza*' (eds 2012 Wolf Legal Publishers) 396.

79 Nina Vajic & Panayiotis Voyatzis, 'The Internet and Freedom of Expression: A Brave New World and the ECtHR's Evolving Case-Law.' In '*Freedom of Expression: Essays in Honour of Nicolas Bratza*' (eds 2012 Wolf Legal Publishers) 405.

80 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2 804.

that German courts adopted a broad interpretation of the notion of jurisdiction in the realm of the internet. However, had Toben chosen not to travel to Germany, he would not have been arrested and even following arrest, his website continued to run as it was located in a foreign server.

19 In the case of *Yahoo! Inc. v La Ligue Contre Le Racism et L'Antisemitisme et al*,[81] two French student organisations[82] commenced proceedings against Yahoo! for allegedly violating French Law by offering Nazi memorabilia for auction on its website. Yahoo! held that its activities did not fall within French jurisdiction as the content was uploaded in the USA where such conduct and material is permitted under the First Amendment. However, this was not accepted by the French Court, which "applied an effects-based jurisdictional analysis and granted prescriptive jurisdiction describing the sale of Nazi paraphernalia."[83] As such, the French Court held that Yahoo! was liable for its effects in France and particularly for violating R. 645-1 of the French Criminal Code which outlaws the sale, exchange or display of Nazi related materials or Third Reich memorabilia. The Court required Yahoo! to ensure that: French citizens could not access the auctions of Nazi objects; to eliminate their access to web pages on Yahoo.com displaying text, extracts or quotations from Mein Kampf and the Protocols of the Elders of Zion; to post a warning to French citizens on Yahoo.fr that any search through Yahoo.com may lead to sites containing material prohibited under Section R645-1 of the French Criminal Code; and that such viewing of the prohibited material may result in legal action against the internet user and to remove it from all browser directories accessible in the French Republic. The order subjected Yahoo! to a penalty of 100,000 Francs for each day it failed to comply with the order.[84] The order concluded that Yahoo! must "take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes".[85] Although Yahoo! took certain steps such as including the required warning regarding the French Criminal Code on its Yahoo.fr website and amending its auction policy, it did not conform to all the orders and instead sought a declaratory judgment from a US Court that the French Order could not be enforced in the USA. In granting the judgment, the Court considered the issue of jurisdiction and approach to free expression underlining that:

> *"what is at issue here is whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation."*[86]

20 It further held that the First Amendment does "not permit the government to engage in viewpoint-based regulation of speech absent a compelling governmental interest which compelling interest was not present in this case."[87]

21 The case of Yahoo! demonstrates the technical and legal consequences of jurisdictional issues *vis-à -vis* the regulation of the internet. The material was uploaded in a State which permitted the selling of such material, but was accessible to citizens of another State where the selling of such material was a criminal offence. Given the borderless nature of the internet, this can happen easily and readily. Although the French Court viewed jurisdiction in a broad sense, basing its interpretation on the effects of the material on its own citizens and its own laws, and notwithstanding the issuance of a Court Order, this was deemed by the USA to be invalid since it could not be constitutionally justified in that country. This subsequently demonstrates that, given the vast divergence of opinion and approaches between Europe and the USA in the realm of free speech and given that jurisdiction in the ambit of internet regulation is nothing but a lucid notion, those States which seek to impose restrictions to expression and material available online will meet both legal and technical obstacles, whilst their previous ideals pertaining to national sovereignty and the conservation of their own legal culture become increasingly diluted. In fact, as noted by one commentator "the judicial impasse of the Yahoo! case exemplifies the cultural tension inherent in attempts to regulate online speech extraterritorially"[88] with of course the notion of territory taking on a different meaning in the digital era.

22 Further, Ernst Zündel, a German living in Canada was "one of the world's most prominent distributors of revisionist neo-Nazi propaganda."[89] In 1997, the

81 Yahoo, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, et al 145 F. Supp. 2d 1168, Case No. C-00-21275JF (N.D. Ca., September 24, 2001).

82 The League Against Racism and Anti-Semitism and The Union of Jewish Students of France.

83 James Bank, 'Regulating Hate Speech Online' (2010) International Review of Law, 24 Computers & Technology 3, 235.

84 Yahoo, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, et al. 145 F. Supp. 2d 1168, Case No. C-00-21275JF (N.D. Ca., September 24, 2001).

85 Ibid.

86 Ibid.

87 Yahoo, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, et al 145 F. Supp. 2d 1168, Case No. C-00-21275JF (N.D. Ca., September 24, 2001).

88 James Bank, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 235.

89 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression*

Canadian Human Rights Tribunal considered a complaint brought against Zündel and his website Zündeliste,[90] which was registered on a US server, on the grounds that it promoted hatred or contempt of Jews.[91] In 2002, the Tribunal decided that hate could not be tolerated on the internet or on other mediums and ordered Zündel to cease and desist from publishing hate messages on his website.[92] In 2005 Zündel was deported to Germany on security grounds where he was found guilty of inciting racial hatred, libel and disparaging the dead, and in 2007 was sentenced to five years in prison.[93] Notwithstanding that the ideas and messages disseminated through his website led to the decision of the Canadian Tribunal and his subsequent imprisonment in Germany, the Zündeliste is still running through a US server. This demonstrates that the technological nature of the internet, in addition to the divergence marking the US and European approaches to free speech, has essentially nullified one of the purposes of the Canadian and German proceedings; namely the removal of what they considered to be hate speech from the internet. The difference in approach was further manifested on a technical level and particularly following a request from Germany to the internet service provider Deutsche Telekom to prevent users from accessing Zündel's site. Deutsche Telekom accepted and, in response to this, users based in the USA created mirror sites, thereby, making the content available to German users in alternative ways.[94] Thus, even seeking to ensure regulation of ISPs cannot actually ensure the prevention of access to material which a State seeks to limit.

23 In the 2002 case of *Warman v Kyburz*, which dealt with anti-Semitic content of Kyburz' website, the Canadian Human Rights Tribunal considered the problems posed in the realm of cease and desist orders as issued in Zündel's case, by the nature of the internet as a borderless medium and the possibility for the creation of mirror sites.[95] Either way, the Tribunal found that "despite these difficulties and technical challenges, a cease and desist order can have both a practical and symbolic effect"[96] as it prevents the ongoing publishing of hateful material and demonstrates public dismay at such hate. In relation to the former, it could safely be said that this is not the case since, for example, even following the Tribunal's decision regarding the Zündeliste, material continued and continues to be uploaded thereto through the US server.

24 The above cases reflect the difficulties related to regulating online hate given the notion of jurisdiction, which is unclear in the realm of the internet and its borderless nature. Both the European Court of Human Rights and national courts of States such as Germany and France, have interpreted this notion broadly. However, as seen from Yahoo!, American courts are ready and willing to limit any sort of effect that restrictive orders may have on internet users in the USA, always in the spirit of the First Amendment.

G. The Additional Protocol to the Convention on Cybercrime

25 The Council of Europe's Convention on Cybercrime is the first multilateral treaty that aims to combat crimes committed through computer systems and has, to date, been ratified by 47 countries.[97] This Convention was signed and ratified not only by Council of Europe States, but also by the USA which, although is not a member of this entity, has an observer status. Interestingly however, the USA acceded to the Convention only after the issue of online hate was removed from the table of discussions.[98] This reality demonstrates that "fundamental disagreements remain as to the most appropriate and effective strategy for preventing dissemination of racist messages on the Internet",[99] which subsequently contribute to the weakening or even nullification of regulatory measures that may be adopted by particular States given that internet regulation requires co-operation for both technical and legal reasons as discussed above. To fill the resulting gaps, the Council of Europe subsequently developed the Additional Protocol to the Cybercrime Convention. This has been ratified by 24 countries.[100] The Council of Europe recognised the

on the Internet' (Intersentia 2008) 67.

90 Institute for Historical Review: The Importance of the Zündel Hearing in Toronto: <http://www.ihr.org/jhr/v19/v19n5p-2_Weber.html> [Accessed 23 October 205].

91 Institute for Historical Review: The Importance of the Zündel Hearing in Toronto: <http://www.ihr.org/jhr/v19/v19n5p-2_Weber.html> [Accessed 23 October 205].

92 Nathan Hall, Abbee Corb, Paul Giannasi, John G.D. Grieve, '*The Routledge International Handbook on Hate Crime*' (eds. Routledge 2015).

93 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 68.

94 James Bank, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 281.

95 Warman v Kyburz, (2003 CHRT 18) (2003/05/09) para. 81.

96 Ibid. Para.82.

97 List of signatures and ratifications available at: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures>.

98 James Banks, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 236.

99 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 17.

100 List of signatures and ratifications available at: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures>.

limitations in implementing a unilateral approach to the issue of online hate in the form of racist or xenophobic hate and, thereby sought to ensure a common set of standards for participating States and promote co-operation amongst them in the criminalisation of relevant acts.[101] This document is seen as a "supplement"[102] to the Convention so as to ensure that the latter's procedural and substantive provisions encompass racism and xenophobia online. Thus, a series of the Convention's articles apply *mutatis mutandis* to the Protocol under consideration including, amongst others, Article 13 on sanctions and measures and Article 22 on jurisdiction.

26 However, even at first sight, this document comes with several significant limitations which will be discussed hereinafter. Firstly, as demonstrated in its title, this Protocol tackles only racist and xenophobic hate, completely disregarding other forms of hate on grounds including, but not limited to, sexual orientation, gender identity and disability, whilst religion is considered a protected characteristic within the definitional framework set out by Article 2. Thus, there seems to be an unjustified prioritisation of online hate with the Council of Europe almost arbitrarily seeking to regulate the effects of racism and xenophobia online, leaving victims of other types of hate without a respective legal framework.

27 The Additional Protocol to the Cybercrime Convention defines what is meant by racist and xenophobic material, underlines the measures to be taken at national level in relation to the dissemination of such material,[103] prohibits racist and xenophobic threats and insults professed through computer systems[104] as well as the denial, gross minimisation, approval or justification of genocide or crimes against humanity.[105] The Protocol also renders the intentional aiding and abetting of any of the above a criminal offence. It must be noted that, unlike Article 9 of the Cybercrime Convention which deals with child pornography, the Protocol does not criminalise the possession and procurement of racist and xenophobic material.[106] As noted in the Explanatory Note of the Protocol, in order to amount to an offence, racist and xenophobic material, insults and revisionist rhetoric must occur on a public level, a point which has been incorporated for purposes adhering to Article 8 of the European Convention on Human Rights.[107]

28 In relation to the acts that are to be deemed offences, it becomes clear that the freedom of expression is "the sacred cow against which the legislation seeks to justify its apparent encroachment for the sake of providing a measure to prohibit cybercrimes motivated by race hate."[108] To illustrate this, one can turn to Article 3 on the dissemination of racist and xenophobic material through computer systems, with part 1, therein, providing that:

> *"each party shall adopt such legislative and other measures as may be necessary to establish as criminal offence under its domestic law, when committed intentionally and without right, the following conduct: distributing or otherwise making available, racist and xenophobic material to the public through a computer system."*

29 However, Part 3 holds that a party may reserve the right not to apply the above paragraph to those cases of discrimination for reasons of upholding free expression. Thus, the Protocol, as an initiative to combat online hate, has been "thwarted through the compromise they have made to concerns about freedom of expression"[109] with much less regard evidently being given to freedoms such as that of non-discrimination. It could thus be argued that the Protocol undermines itself by its approach in that the Council of Europe has given an unequal and unjustifiable emphasis on expression rather than non-discrimination and equality. [110]

30 In relation to general limitations that may be imposed on the applicability of Article 3, Part 2 therein, holds that a State may choose not to attach criminal liability to conduct referred to in Part 1 if this does not promote violence or hatred insofar as other effective remedies are available. This is notwithstanding the fact that in the Protocol's title, reference is made to the criminalisation of racist and xenophobic acts committed through computer systems. Whilst criminalising racist and xenophobic threats has no option to disregard parts of its provisions, Article 5 on racist and xenophobic insults provides that a State has the right not to apply in whole or in part, Part 1 of this Article, which sets out the legislative and other measures that may be adopted to criminalise racist and xenophobic insults. Although no direct reference to free expression is made here as the justifier of such limitation, it could

101 James Banks, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 236.

102 Article 1, Additional Protocol t the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.

103 Additional Protocol, Article 3.

104 Additional Protocol, Article 4 and Article 5.

105 Additional Protocol, Article 5.

106 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 50.

107 Explanatory Note to the Additional Protocol, para. 29.

108 Fernne Brennan, 'Legislating against Internet Race Hate' (2009) 18 Information and Communications Technology Law 2, 124.

109 Ibid. 123.

110 Ibid. 126.

implicitly be assumed that concerns regarding the freedom of expression led to the formulation of the aforementioned reservation available to those who want it. Reserving the right not to apply a particular provision is also incorporated into the denial, gross minimisation, approval, or justification of genocide or crimes against humanity. Many of the States which ratified the Protocol took the opportunity to incorporate reservations. It generally appears that Article 4 on racist and xenophobic threats is the one granted the most protection as it extends to private as well as public communications, unlike the other acts found in the Protocol, while it gives no opt-out possibility as the others do.

31 The issue of intent is also significant when seeking to appraise the Protocol. This document renders the dissemination of material, threats, insults and revisionist rhetoric offences illegal as well as aiding and abetting the committal of such offences in the event that such acts and/or expressions are effectuated and/or uttered intentionally. This is particularly significant in the realm of the liability of internet service providers who simply constitute the platform through which problematic speech may arise. The Explanatory Report to the Additional Protocol to the Cybercrime Convention holds that the precise meaning of "intentionally" should be interpreted on a national level.[111] However, it did clearly stipulate that it is not sufficient for an internet service provider which simply constitutes the host of the material to be found guilty of any of the Protocol's offences if the required intent under domestic law did not exist.[112] Thus, on the one hand it does limit the liability of unknowing ISPs but leaves the general conceptualisation of intent unsure and contingent on national positions. However, the Protocol does not regulate or prohibit the finding of permissive intent in the event that an ISP is made aware of racist or xenophobic material or expression and does not take the necessary measures to remove it, thereby, leaving some doors open for finding potential liability in the inaction of ISPs. Such permissive intent is found, for example, in Germany's Information and Communications Service Act of 1997, which underlines the liability of ISPs in the event that they knew of hateful content, had the ability to block it, but chose not to.[113] Further, in the realm of ISPs, the Protocol remained silent on the very significant question of jurisdiction in the event of a conflict of law between the hosting country and the other.[114] Although for EU countries, the Directive on Electronic Commerce[115] is applicable with Article 3, therein providing that ISPs are governed by the laws of the Member State in which they are established,[116] the situation is not clear in the event that a non-EU country is involved in a particular dispute.[117]

32 Although the Protocol may contribute to promoting harmonisation regarding agreed upon principles and procedural, technical and legal cooperation amongst States, the Protocol remains problematic. This is the case not only due to its inherent limitations as described above, but also due to the fact that the USA is not part of it. This, in addition to the absence of any form of extradition treaties between the USA and other countries in the sphere of online hate speech, deeply restricts the efficacy of the Protocol's aims and objectives. Moreover, it may well appear that the Protocol has sought to achieve the lowest possible common denominator, maybe for purposes of maximising ratification. Either way, the aforementioned delimitations may serve as stumbling blocks when seeking to meet the objectives of the Protocol. Furthermore, as well as limitations as a result of an over-emphasis on the freedom of expression, it could be argued that the Protocol constitutes an ineffective base through which online hate can be restricted since it adopts traditional conceptions of State boundaries, State sovereignty on issues such as the freedom of expression mentioned above, and, more generally, treats the issue of online hate as any other issue of traditional means of communication throwing in the concept of international co-operation without effectively and pragmatically considering the challenges of the internet. However, "the Internet is a very different animal from that we are used to, which requires handling in a different way",[118] but this has not been taken on board.

111 Explanatory Note to the Additional Protocol, para. 25.

112 Ibid. para. 25.

113 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2, 796.

114 Ibid. 801.

115 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

116 It must be noted that the Directive provides for an exception to that choice of law when the receipt country's choice of law is necessary for the prevention, investigation, detection and prosecution of criminal offense including the 'fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons.'

117 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Merging American Haven' (2005) 62 Washington and Lee Law Review 2, 801.

118 Fernne Brennan, 'Legislating against Internet Race Hate' (2009) 18 Information and Communications Technology Law 2, 141.

H. Conclusion

33 Hate and hateful expression existed before the creation of the internet and will continue to exist even if tight regulation of online activity were to be achieved.[119] However, the internet has brought about "socio-technological and legal dilemmas that are difficult to handle from a legal point of view".[120] Moreover, the issue of online hate is moving in new dimensions, with those who disseminate hate speech finding themselves before an array of possibilities to use and abuse the internet for purposes of communication, recruitment and victimisation. However notwithstanding that some case-law has been formulated on a national, transnational and regional level and, even though the Additional Protocol to the Cybercrime Convention has been formulated, the issue of online regulation has not essentially taken any pragmatically significant steps. Firstly, the Protocol itself is lacking as per its scope, as it is arbitrarily limited to racist and xenophobic speech whilst simultaneously limiting its efficacy for purposes of giving particular protection to the freedom of expression. Secondly, the normative US-European divergence of the understanding of free expression has dramatically affected the regulation that Europe seeks to achieve. As noted by one commentator, the global, boundary-free nature of the internet in conjunction with the absolutist approach to expression, as so adopted by the USA, means that "like chasing cockroaches, squashing one does not solve the problem when there are many more waiting behind the walls – or across the border".[121] More particularly, even if a website is shut down in Germany for example, it may almost immediately pop up again through an American host. At the same time, American courts are not ready to apply any court orders issued in European countries insofar as they are considered to be contrary to the First Amendment. Thus, at the heart of these differences lie fundamental conflicts of legal thought on speech. Interestingly in the case of Yahoo!, the US court recognised that, given that no international treaty or standards were available in the realm of tackling issues on internet speech, the Court is bound by the First Amendment. However following the Yahoo! judgement, the USA finally had the opportunity to be part of such an agreement, however not only opted out of the Additional Protocol to the Cybercrime Convention, but also made its accession to the convention contingent on the exclusion of this theme from the Convention. In brief, there is no intent at the moment on the part of the USA to be part of such an international collaboration in the field of free speech simply because this State's understanding of free speech does not endorse regulation of hatefulness unless certain high and immediate thresholds, as discussed above, are applied. The result of this approach is that, due to the technical nature of the Internet, the First Amendment has now taken the position as a "default standard for free speech on the Internet"[122] whether other States like it or not. Thus for the moment, it is safe to say that realistic prospects of internet regulation seem unlikely, especially if traditional and purely legal methods are adopted for this purpose.

* *Natalie Alkiviadou* is a PhD Candidate at the VU Amsterdam and a Lecturer at the University of Central Lancashire Cyprus.

119 James Bank, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 233.

120 Barbara Perry & Patrick Olsson 'Cyberhate: The Globalization of Hate' 18 Information and Communications Technology Law 2, 196.

121 James Bank, 'Regulating Hate Speech Online' (2010) 24 Computers & Technology 3, 237.

122 Dragos Cucereanu '*Aspects of Regulating Freedom of Expression on the Internet*' (Intersentia 2008) 232.

Regulating Online Content through the Internet Architecture

The Case of ICANN's new gTLDs

by **Caroline Bricteux***

Abstract: The process introduced by the Internet Corporation for Assigned Names and Numbers (ICANN) to assess and allocate new generic top-level domains (gTLDs) offers a vehicle for content regulation at two levels. First, regarding the gTLD itself, objection procedures were set up to allow third parties to challenge an applied-for gTLD deemed to be contrary to "general principles of international law for morality and public order" or detrimental to broadly defined communities. The real target of these objections managed by the International Chamber of Commerce was not the gTLD itself, but the potentially controversial content that might be published under it. Second, these preventive measures were coupled with a strengthened anti-abuse policy for new gTLDs. ICANN amended its standard agreements with domain name registries and registrars to impose additional safeguards, compliance with "all applicable laws", and remedies such as suspension of the domain name, which is a powerful tool to deny access to online content. Surprisingly these amendments were not discussed under ICANN's consensus policy development process but added at the request of governments after the launch of the New gTLDs Program. These provisions, if actually enforced by ICANN, could lead to content policing by private entities without any measure to ensure due consideration of domain name holders' freedom of expression.

Keywords: ICANN; gTLD; content regulation; International Chamber of Commerce; freedom of expression

Recommended citation: Caroline Bricteux, Regulating Online Content through the Internet Architecture: The Case of ICANN's new gTLDs, 7 (2016) JIPITEC 229 para 1.

A. Introduction

1 Technical control of crucial Internet resources has well-known political, economic and social dimensions. Numerous studies have shown that Internet intermediaries – such as access providers, web hosting services or search engines – face pressure from various sources to regulate online content.[1] Intermediaries are increasingly subjected to injunctions to deny access to illegal content,[2] and under certain conditions they may additionally be held liable for content uploaded by third parties.[3]

1 See, among others: J. Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 *Harvard Law Review* pp. 2296-2342; L. DeNardis, 'Hidden Levers of Internet Control' (2012) 15(5) *Information, Communication and Society* pp. 720-738; B. Frydman and I. Rorive, 'Regulating Internet Content through Intermediaries in Europe and the USA' (2002) 23(1) *Zeitschrift für Rechtssoziologie*, pp. 41-59.

2 See P. Savola, 'Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers' (2014) 5(2) *JIPITEC* pp.116-138; M. Husovec, 'Injunctions against Innocent Third Parties: The case of Website Blocking' (2013) 4(2) *JIPITEC* pp. 116-129.

3 For an overview of existing models of intermediary liability, see R. MacKinnon, E. Hickok, A. Bar and H. Lim, *Fostering*

Targeting intermediaries rather than content providers overcomes the difficulty of identifying the source and recipients of a particular piece of content on the Web. However efficient this strategy is to tackle illegal activities and abuse online, it has come under considerable criticism. Proponents of freedom of expression have repeatedly claimed that putting intermediaries under pressure to regulate content carries a significant risk of over-censorship, without transparent processes and guarantees that the competing rights and interests at stake will be carefully balanced by the intermediary.[4]

2 I will argue in this paper that domain name registries and registrars might also serve as points of control[5] for the content posted in the domain that they administer, in particular with regard to the new processes brought by the Internet Corporation for Assigned Names and Numbers (ICANN) to assess and allocate new generic top-level domains (gTLDs). Since 1998, ICANN has been in charge of the management of the Domain Name System (DNS), which operates the translation of user-friendly domain names into computer-friendly IP addresses. In June 2011 its Board of Directors announced the launch of the New gTLDs Program, a plan to implement an unprecedented expansion of the DNS by significantly increasing the number of generic top-level domains (gTLDs such as *.com*, *.org* or *.net*), with the aim of fostering diversity and encouraging competition at the top level of the Internet's namespace. Worryingly, the process introduced by ICANN to assess and allocate new gTLDs offers a vehicle of content regulation at two levels. First, regarding the gTLD itself, objection procedures were set up to allow third parties to challenge an applied-for gTLD deemed to be contrary to "general principles of international law for morality and public order" or detrimental to broadly defined communities. The real target of these objections managed by the International Chamber of Commerce (ICC), was clearly not the gTLD itself but the potentially controversial content that might be published under it. Second, these preventive measures were coupled with a strengthened anti-abuse policy for new gTLDs. ICANN amended its standard agreements with domain name registries and registrars to impose additional safeguards, compliance with "all applicable laws", and remedies such as suspension of the domain name, which is a powerful tool to deny access to online content. Surprisingly these amendments were not discussed under ICANN's consensus policy development process but added at the request of governments after the launch of the New gTLDs Program. These provisions, if actually enforced by ICANN, could lead to content policing by private entities without any measure to ensure due consideration of domain name holders' freedom of expression.

3 The rest of this paper is divided into four sections. I will start in Section B by examining the evolution of the DNS from its inception in the 1980s through the following three decades, in order to fathom the ambition of the New gTLDs Program. We will see that expanding the DNS raises more than technical questions, as delicate policy decisions have to be taken to set the standards and procedures governing the creation and allocation of new gTLDs. The following two sections will be devoted to two mechanisms introduced by the New gTLDs Program that ultimately produce a form of content regulation. Section C deals with the objection procedures and Section D deals with the new contractual obligations of domain name registries and registrars regarding abuse. Section E sums up the arguments and identifies potential future developments.

B. The Evolution of the Domain Name System

4 In June 2011, ICANN's Board of Directors gave the green light for the New gTLD Program, which was announced to be "one of the biggest changes ever to the Internet's Domain Name System".[6] The DNS is a crucial feature for human Internet users, as it operates the translation of alphanumeric domain names (such as *ulb.ac.be*) into the corresponding IP addresses (such as *164.15.59.215*) needed for the transmission of information across the network. The DNS differs significantly from the rest of the Internet's decentralized and distributed architecture: it must be operated on a centralized basis to ensure that every domain name is unique and that a website name will always lead to the same address, regardless of the geographical location of the user typing the name in his web browser.[7] In the early days of the Internet, the naming and addressing system relied on a single distributed file, which had to be updated whenever a new computer joined the network. This highly centralized directory rapidly became unable to accommodate the Internet's fast

Freedom Online: the Role of Internet Intermediaries (Paris: UNESCO/Internet Society, 2014), pp. 39 et seq.

4 See, for example, the Report of the Special Rapporteur on the promotion and protection of the right to freedom and expression, Frank La Rue, to the UN Human Rights Council, A/HRC/17/27, 16 May 2011, spec. §§ 42-43.

5 J. Zittrain, 'Internet Points of Control' (2003) 44(2) *Boston College Law Review* pp. 653-688.

6 ICANN, Regular Meeting of the Board, Resolution 2011.06.20.01, 20 June 2011, <www.icann.org/resources/board-material/resolutions-2011-06-20-en>.

7 According to the Internet Society, this global reach is a fundamental characteristic of the Internet (Internet Society, Internet Invariants: What Really Matters, 3 February 2012, <www.internetsociety.org/internet-invariants-what-really-matters>).

growth. Therefore, the DNS was developed in the 1980s to enable the decentralization of the naming and addressing functions, while retaining some degree of centralized control to ensure consistency and uniqueness of the identifiers. The key was the hierarchical division of the namespace into different levels of domains. This tree-shaped hierarchy is reflected in the arrangement of domain names, from right to left and separated by dots: (1) a top-level domain (TLD); (2) a second-level domain (SLD or 2LD); (3) an eventual third-level domain (3LD), and so on. To give an example, with *ulb.ac.be*, *.be* is the TLD, *.ac* is the SLD and *ulb* is the 3LD. Two main categories of TLDs coexist: generic top-level domains (gTLDs) such as *.com, .biz* and *.xxx*, and two-letter country-code top level domains (ccTLDs), such as *.be* for Belgium, *.de* for Germany and *.cn* for China. The hierarchical structure of the DNS enables the storing of information about each level at different name servers, which can in turn perform the domain name resolution function, i.e. the name-to-number translation. At the top of the hierarchy lies the root, a single file that contains the list of the authoritative servers for each top-level domain.

5 The hierarchical design of the DNS is reflected in its management, with powers devolving from TLDs to sub-domains. ICANN is placed at the apex of the hierarchy and has administered the DNS root since 1998. Until 1998 the DNS was maintained relatively informally by contractors of the U.S. government, which was funding research on packet switching technology and its applications. As the Internet evolved into a major commercial and communication platform in the mid-1990s, businesses and foreign governments pressured the U.S. authorities to increase competition and privatize control over the DNS. After requesting comments, the National Telecommunications and Information Administration (NTIA), an agency of the U.S. Department of Commerce, released a Statement of Policy in June 1998, which called upon the Internet community to form a private not-for-profit corporation to manage the DNS.[8] This resulted in the formation of a new corporation under California law, ICANN.[9] ICANN is characterized by a multi-stakeholder governance model and bottom-up decision-making processes: its policies are initiated and developed within supporting organizations whose members represent both commercial and non-commercial interests of the DNS. Final decisions are taken by ICANN's Board of Directors. Advisory committees complete this complex structure to give an opportunity to governments, among others, to make their voices heard within ICANN.[10]

6 Until 30 September 2016, ICANN's authority over the DNS derived from a crucial contract with the U.S. government – acting through the NTIA – regarding the so-called IANA functions.[11] The IANA contract, which was initially signed in 2000 and renewed several times,[12] made ICANN responsible for coordinating the Internet unique identifiers (domain names, IP addresses, and protocol parameters). The U.S. government retained oversight over ICANN through this contractual relationship, notably by its ability to impose new contractual terms during renewal rounds.[13] The U.S. government oversight was highly controversial, not only because the privatization of the DNS management was incomplete, but also because other governments did not have similar powers and only played an advisory role within ICANN. Following years of criticism, the U.S. government announced in March 2014 its intention to relinquish its remaining oversight role and to transition that responsibility to the global multi-stakeholder community, excluding a government-led or an inter-governmental replacement.[14] ICANN was designated as the convener of the process to develop a transition proposal with all stakeholders across the global Internet community. In March 2016, after two years of intense discussions, this process culminated in the submission of a transition proposal to the NTIA.[15] Notably, the text proposed to transfer

8 U.S. Department of Commerce, NTIA, Management of Internet Names and Addresses, Statement of policy, *Federal Register*, vol. 63, nr. 111, 10 June 1998, p. 31741.

9 For a detailed account of ICANN's inception, see M. Mueller, *Ruling the root: Internet governance and the taming of cyberspace* (Cambridge, MA: MIT Press, 2002); M. Froomkin, 'Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution' (2000) 50(1) *Duke Law Journal* pp. 17-184 and J. Weinberg, 'ICANN and the Problem of Legitimacy' (2000) 50(1) *Duke Law Journal* pp. 187-260.

10 On the role of governments within ICANN, see J. Weinberg, 'Governments, Privatization, and "Privatization": ICANN and the GAC' (2011) 18 *Michigan Telecommunications and Technology Law Review* pp. 189-218.

11 IANA stands for the Internet Assigned Numbers Authority.

12 The latest version of the IANA contract was awarded in July 2012 (IANA Functions Contract, 2 July 2012, <www.ntia.doc.gov/page/iana-functions-purchase-order>). This contract was originally set to expire on the 30th of September 2015 and was extended to the 30th of September 2016 to leave time to complete the transition process initiated in March 2014 (L. E. Strickling, An Update on the IANA Transition, 17 August 2015, <http://www.ntia.doc.gov/blog/2015/update-iana-transition>).

13 See K. McGillivray, 'Give it away now? Renewal of the IANA functions contract and its role in internet governance' (2014) 22(1) *International Journal of Law and Information Technology* pp. 3-26.

14 U.S. Department of Commerce, NTIA, NTIA Announces Intent to Transition Key Internet Domain Name Functions, 14 March 2014, <www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

15 IANA Stewardship Transition Coordination Group, Proposal to Transition the Stewardship of the IANA Functions from the U.S. Commerce Department's NTIA to the Global Multistakeholder Community, 10 March 2016, <http://www.icann.org/en/system/files/files/iana-stewardship-

the performance of the IANA functions to a new, separate legal entity, which would be formed as an affiliate of ICANN. This new entity would become the IANA functions operator, while ICANN would assume the role played until then by the NTIA. In addition, ICANN's actions would be subject to strengthened accountability mechanisms. The transition had indeed prompted a parallel discussion on ICANN's accountability, as the U.S. government oversight was seen as a tool to keep ICANN accountable to its stakeholders.[16] The NTIA accepted the proposal in August 2016[17] and the IANA contract was allowed to expire in October 2016.[18] Since then, the IANA functions have been performed by a new affiliate of ICANN, called Public Technical Identifiers.[19]

7 As part of its DNS managing duties, ICANN contracts with registries[20] and accredits registrars with whom the registries deal. These constitute the lower levels of the DNS administrative hierarchy. Domain name registries are in charge of maintaining and coordinating the database of all the SLD registered within a TLD. There can be only one registry per TLD to ensure coherence and consistency of the database. Registrars offer domain name registration services to the general public (registrants) and collects clients' information and payment in order to make a unique SLD entry into the registry.

8 The addition of new gTLDs to the global namespace had been on the forefront of ICANN's agenda since 1998. Back then only seven gTLDs created in the 1980s were available: *.com, .edu, .gov, .int, .mil, .net* and *.org*. Adding new gTLDs became crucial in the 1990s to improve competition in the registration market. Since 1993 the management of the domain name registration services (both registry and registrar functions) for *.com, .net* and *.org* had been performed by a sole company – Network Solutions Inc. (NSI) – under a cooperative agreement with the National Science Foundation (NSF).[21] At that time, registration of a SLD was subsidized by the NSF and free of charge for the end user. This practice changed with the transformation of the Internet into a commercial platform in the mid-1990s. Demand for domain names was rocketing and costs to support them became unsustainable given the NSF's budget constraints.[22] Therefore, in 1995 NSF amended the cooperative agreement with NSI to allow the company to charge an annual fee of $50 per domain name registered.[23] This was the start of a very lucrative business for NSI, with hundreds of millions dollars at stake in the *.com* domain. Inevitably, this government-blessed monopoly generated a high level of controversy and was one of the driving forces behind the reform of the DNS management and the creation of ICANN. The U.S. government favored two ways to open up the domain name market to competition.[24] First, registry and registrar functions were separated: NSI had to agree to design a shared registry system that would allow competing registrars to market domain name registrations in *.com, .net* and *.org*, while retaining its monopoly on the registry function.[25] Second, the addition of new gTLDs was encouraged to provide an alternative to *.com* and let new registries enter the registration market.

9 Before the New gTLDs Program, ICANN launched two rounds of domain name expansion for gTLDs, which resulted in the delegation of fifteen new gTLDs between 2001 and 2011. The first expansion round took place in 2000 and was designed to evaluate the policy and practical issues associated with the addition of new gTLDs. Rather than choosing new gTLDs and assigning them to new operators, ICANN decided to call for proposals from prospective registries. 47 applications were received and the ICANN Board selected seven new gTLDs (*.aero, .biz, .coop, .info, .museum, .name, .pro*).[26] Interestingly, the Board refused to choose any of the proposals for a *.kids* gTLD, fearing that approving such a domain would bring it uncomfortably close to the business of content regulation.[27] One applicant, ICM Registry,

transition-proposal-10mar16-en.pdf>.

16 Cross Community Working Group on Accountability, Supplemental Final Proposal on Work Stream 1 Recommendations, 23 February 2016, <http://www.icann.org/en/system/files/files/ccwg-accountability-supp-proposal-work-stream-1-recs-23feb16-en.pdf>.

17 U.S. Department of Commerce, NTIA, Update on the IANA Transition, 16 August 2016, <http://www.ntia.doc.gov/blog/2016/update-iana-transition>.

18 U.S. Department of Commerce, NTIA, Statement of Assistant Secretary Strickling on IANA Functions Contract, 1 October 2016, <http://www.ntia.doc.gov/press-release/2016/statement-assistant-secretary-strickling-iana-functions-contract>.

19 ICANN, ICANN Announces Incorporation of Public Technical Identifiers (PTI), 11 August 2016, <http://www.icann.org/news/announcement-2-2016-08-11-en>.

20 For historical reasons ICANN does not have a contract with all the ccTLD registries.

21 Cooperative Agreement Between NSI and U.S. Government, 1 January 1993, <http://archive.icann.org/en/nsi/coopagmt-01jan93.htm>.

22 J.B. Beyster and M.A. Daniels, *Names, Numbers, and Network Solutions. The Monetization of the Internet* (La Jolla: The Foundation for Enterprise Development, 2013), p. 73.

23 Amendment 4 to Cooperative Agreement between NSI and U.S. Government, 13 September 1995, <http://archive.icann.org/en/nsi/coopagmt-amend4-13sep95.htm>).

24 U.S. Department of Commerce, NTIA, Management of Internet Names and Addresses, Statement of policy, Federal Register, vol. 63, nr. 111, 10 June 1998, pp. 31745-31746.

25 Amendement 11 to the DOC/NSI Cooperative Agreement, 6 October 1998, <http://www.ntia.doc.gov/legacy/ntiahome/domainname/agreements/Amend11_052206.pdf>.

26 ICANN, Second Annual Meeting of the ICANN Board, 16 November 2000, <http://www.icann.org/resources/board-material/minutes-annual-meeting-2000-11-16-en>.

27 ICANN, Report on New TLD Applications, III.B.1.c

was even applying for both *.kids* and *.xxx*, arguing that, together, these new gTLDs would enhance online child safety by clearly delineating child-friendly and adult-only content areas.[28] According to M. Mueller, ICANN did not want to take the responsibility for certifying the appropriateness of the material posted in a *.kids* domain.[29] The *.xxx* application was also rejected,[30] but it was resubmitted during the second round of new gTLD applications launched in 2003. This second round called for proposals for sponsored new gTLDs[31], i.e. specialized gTLDs that serve the needs of a defined community not otherwise adequately represented in the DNS.[32] Ten proposals were received and the ICANN Board ultimately selected *.asia, .cat, .jobs, .mobi, .post, .tel, .travel* and *.xxx* as new sponsored gTLDs.[33]

10 The two rounds of expansion elicited criticism for being "painfully slow, unpredictable and entirely discretionary"[34] and "anything but well-organized".[35] M. Mueller and L. McKnight denounced the lack of uniform selection criteria and the absence of a regular timetable for accepting and deciding upon the applications.[36] ICANN itself acknowledged that similar proposals could be treated differently.[37] Moreover, during the second round of DNS expansion, the *.xxx* proposed by ICM Registry for "the responsible online adult-entertainment community"[38] caused a major controversy within ICANN.[39] This application received preliminary Board approval in June 2005 to begin negotiating the terms of the registry agreement, which would only be formally approved in March 2011. In the meantime, ICANN had experienced pressures from a variety of constituencies against the application. Several members of the Governmental Advisory Committee (GAC) condemned an apparent legitimation of online pornography. There were also concerns regarding the actual community support for *.xxx* after complaints from members of the adult entertainment industry fearing that such a TLD would facilitate filtering and censorship. As a result of these pressures, the Board ended up withdrawing its approval in March 2007.[40] This was an unprecedented victory for the GAC, which encouraged its members to weigh in to exert more influence in the ICANN arena.[41] This success was short-lived however. ICM Registry challenged the Board's reversal through ICANN's Independent Review Process.[42] In 2010 the review panel found that ICANN's volte-face on the *.xxx* application "was not consistent with the application of neutral, objective and fair documented policy" and therefore violated its bylaws.[43] Although the opinion was not binding, the Board decided to re-open negotiations with ICM Registry and finally approved the new *.xxx* TLD in March 2011.[44]

11 The handling of the *.xxx* application was concomitant with heated discussions within ICANN about a New gTLDs Program that would offer a much more ambitious expansion of the DNS. The long policy

("Restricted Content Group"), 9 November 2000, <http://archive.icann.org/en/tlds/report/report-iiib1c-09nov00.htm>.

28 ICANN, Registry Operator's Proposal – Volume 2, 18 September 2000, <http://archive.icann.org/en/tlds/kids3/HTML/Volume_2.html>. See as well Berkman Center for Internet and Society, « Accountability and Transparency at ICANN: An Independent Review », 20 October 2010, <http://www.icann.org/en/reviews/affirmation/atrt-review-berkman-final-report-20oct10-en.pdf>, pp. 94-96.

29 M. Mueller (2002), *supra* note 9, p. 204.

30 ICANN, Report on New TLD Applications, III.B.1.c ("Restricted Content Group"), *supra* note 27.

31 ICANN, Regular Meeting of the Board, 31 October 2003, <http://www.icann.org/news/advisory-2003-10-31-en>.

32 Sponsored gTLDs have a sponsor representing the particular community to carry out a "delegated policy-formulation role" over a variety of matters regarding the TLD. See ICANN, Request for Proposals for new sponsored Top Level Domains (sTLDs), 15 December 2003, <http://archive.icann.org/en/tlds/new-stld-rfp/new-stld-application-parta-15dec03.htm>.

33 ICANN, Status Report on the sTLD Evaluation Process, 19 March 2004 (updated on 3 December 2005), <http://archive.icann.org/en/tlds/stld-apps-19mar04/stld-status-report.pdf>. The archive related to the sponsored gTLDs round can be consulted at <http://archive.icann.org/en/tlds/stld-apps-19mar04>.

34 M. Mueller and L.W. McKnight, 'The post-.COM internet: toward regular and objective procedures for internet governance' (2004) 28 *Telecommunications Policy*, p. 495.

35 J. Weinberg, 'ICANN, "Internet Stability", and New Top-Level Domains' in Cranor, L. and Greenstein, S. (eds.) *Communications Policy and Information Technology: Promises, Problems, Prospects* (Cambridge, MA: MIT Press, 2002), p. 17.

36 M. Mueller and L.W. McKnight (2004), *supra* note 34, p. 495.

37 J. Weinberg (2002), *supra* note 35, pp. 19-20.

38 ICANN, New sTLD RFP Application, *.xxx*, Part B. Application Form, <http://archive.icann.org/en/tlds/stld-apps-19mar04/xxx.htm>.

39 For a detailed account of the *.xxx* case, see Appendix D of Berkman Center for Internet and Society, 'Accountability and Transparency at ICANN: An Independent Review', *supra* note 28, pp. 90-124.

40 ICANN, Board Meeting at ICANN Meeting 28, Resolution 07.18, 26-30 March 2007, <http://www.icann.org/resources/board-material/resolutions-2007-03-30-en>.

41 J. Weinberg (2011), *supra* note 10, p. 203.

42 The Independent Review Process is an accountability mechanism set out in ICANN Bylaws that provides for an independent third-party review of Board actions (or inactions) alleged by an affected party to be inconsistent with ICANN's Articles of Incorporation or Bylaws (ICANN, Bylaws, Article IV, Section 3).

43 International Centre for Dispute Resolution , *ICM Registry v. ICANN*, case no. 50 117 T 00224 08, 19 February 2010, <http://www.icann.org/en/system/files/files/-panel-declaration-19feb10-en.pdf>, §§ 149-152.

44 ICANN, Regular Meeting of the Board, Resolutions 2011.03.18.23-2011.03.18.25, 18 March 2011, <http://www.icann.org/resources/board-material/resolutions-2011-03-18-en>.

development process[45] ultimately favored a new approach: instead of arbitrarily pick a few new gTLDs out of a large pool of applications, ICANN decided to establish transparent and predictable selection criteria in an Applicant Guidebook (AGB)[46] that would be fully available to the applicants prior to the initiation of the process.[47] Any word (in any language or script) could be proposed and all applications that would meet the conditions would be granted without restricting the number of new gTLDs. Since the launch of the Program in 2012, the growth of the DNS has already been quite substantial. As of October 2016 and out of the 1,930 admissible proposals received by ICANN, over 1,100 new gTLDs have been delegated into the DNS.[48] These new gTLDs are very diverse: they represent trademarks and company names (such as *.google, .chanel* or *.bmw*), professions and economic sectors (such as *.lawyer, .pharmacy* or *.bank*), geographical areas (such as *.amsterdam, .tirol* or *.vlaanderen*), religious terms (such as *.bible* or *.church*) or generic terms (such *.global, .cool* or *.fail*).[49] This unleashing of global human imagination did not come without restrictions: next to strict financial[50] and operational criteria, processes were put in place to ensure the consideration of rights, interests and values beyond a mere technical evaluation of the applications.

12 The *.xxx* affair constituted an important precedent for ICANN when discussing the liberalization of the generic top-level domain market; it showed that the addition of new gTLDs is, above all, a complex political question. Prior to the launch of the New gTLDs Program, ICANN had to decide which strings of characters would and would not be acceptable TLDs, but also consider who should manage sensitive identifiers and how to reject undesirable new TLDs. The designers of the DNS wanted to avoid being pulled in such delicate debates by denying any meaning to domain names. According to them, the functions of the DNS were very narrow: it was simply a convention for naming computers attached to the Internet, not a form of directory assistance.[51] Yet domain names changed function with the introduction of the World Wide Web, which integrated them in web addresses or Uniform Resources Locators (URLs) such as *www.ulb.ac.be*. As the term resource locator suggests, URLs were not just mere addresses but locators for content posted on the web.[52] Domain names became signboards – identifiers for the content posted on the website they were directing to. Consequently, people got the natural tendency to attribute social meanings to the TLDs,[53] as is powerfully illustrated in the *.xxx* case. Drawing lessons from that controversial affair, ICANN decided to relieve its Board of the assessment of the social meaning of the strings proposed as gTLDs. Instead, objection procedures were established in the AGB to let independent experts take decisions about TLDs that anyone may find offensive, polarizing, or controversial[54]. I examine these procedures in the following section and argue that they served as a preventive mechanism of content control.

C. Objection Procedures: Ex Ante Control of Content

13 A formal objection procedure was developed in the New gTLDs Program to ensure the consideration of rights, interests and values falling outside the scope of ICANN's assessment of applications.[55] Objectors could file their objection on four enumerated grounds (string confusion, legal rights, limited public interest and community) to an independent dispute resolution service provider (hereinafter, DRSP), which then appointed panels of expert(s) to issue determinations.[56] Two types of review could be performed by the panels, depending on the grounds of objection: in the case of string confusion or legal rights objections, only the applied-for string was examined to determine whether it was confusingly similar to an existing TLD or to another applied-for gTLD string, or whether it would be likely to infringe the objector's trademark. These grounds of objection

45 For a detailed account of ICANN's New gTLDs Policy Development Process see chapter 4 of P. White, *Protocols of Power: Lessons from ICANN For International Regime Theory* (2012) Doctoral thesis, University of Huddersfield, available from: <http://eprints.hud.ac.uk/17496>.

46 ICANN, New gTLD Applicant Guidebook, Version 2012-06-04, <http://newgtlds.icann.org/en/applicants/agb>.

47 For a comprehensive overview of the application process for new gTLDs, see T. Bettinger and M. Rodenbaugh, 'ICANN's New gTLD Program' in Bettinger, T. and Waddel, A. (eds.) *Domain Name Law and Practice: An International Handbook* (Oxford, Oxford University Press, 2015), pp. 65-123.

48 The statistics of the New gTLDs Program can be consulted at: <http://newgtlds.icann.org/en/program-status/statistics>.

49 For a complete and up-to-date list of delegated strings, see <http://newgtlds.icann.org/en/program-status/delegated-strings>.

50 Each applicant had to pay a fee of USD 185,000 in order to have its application considered.

51 M. Mueller (2002), *supra* note 9, pp. 78-81.

52 *Id.*, p. 108.

53 D. Lindsay, *International Domain Name Law. ICANN and the UDRP* (Oxford/Portland: Hart Publishing, 2007), p. 10.

54 M. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010), pp. 201-204.

55 The rules and standards applicable to the objection procedures are set forth in Module 3 of the Applicant Guidebook and in the 'New gTLD Dispute Resolution Procedure' attached thereto.

56 For a comprehensive overview of the objection procedures' rules and outcomes, see T. Bettinger, 'Rights Protection Against Applications for New gTLDs (Pre-Delegation Dispute Resolution)' in Bettinger, T. and Waddel, A. (2015), *supra* note 47, pp. 1077-1163.

do not raise particular concern regarding content control. The same cannot be said about the two other grounds of objection, which I will examine more closely below. Not only the applied-for gTLD, but as also the proposed registry management and commitments made by the applicant, played an important role in the determination on the grounds of limited public interest and community. The experts had to determine whether the application would be contrary to general principles of international law for morality and public order, or would cause detriment to a broadly defined community. The International Center of Expertise of the International Chamber of Commerce (ICC) was designated as a DRSP for the objections filed on the grounds of limited public interest and community. Another distinguishing feature of these two grounds of objection can be found in the role played by a new character in ICANN's complex ecosystem: the independent objector.[57] Acting "solely in the best interests of the public who use the global Internet",[58] the independent objector was designated to file objections against "highly objectionable terms"[59] on the grounds of limited public interest and community. The independent objector was acting independently from ICANN, as neither its staff nor its Board had authority to direct or require the independent objector to file or not file any particular objection.

14 In principle, the Board of ICANN was not supposed to directly deal with conflicts arising from third parties' allegations such as in the *.xxx* case. However, there is room for interpretation regarding the binding nature of expert determinations. No specific appeal process was mentioned to challenge expert determinations; neither did the DRSPs adopt procedures to review the work of the appointed panels, nor to provide a unified interpretation of the dispute resolution standards. The Guidebook tersely provides that the expert determination will be considered as an "advice that ICANN will accept within the dispute resolution process".[60] In the independent objector's view, this wording is unfortunate as it seems to imply that ICANN reserves its right not to follow expert determinations, which could pave the way for allegations of arbitrary decisions.[61] This interpretation is confirmed when looking at Module 5 of the Guidebook (Transition to Delegation), which provides that ICANN's Board of Directors has "ultimate responsibility for the New gTLD Program" and that it reserves its "right to individually consider an application for a new gTLD to determine whether approval would be in the best interest of the Internet community". It adds that "under exceptional circumstances, the Board may individually consider a gTLD application".[62] Upon that argument, the Board decided, in specific cases, either to direct a re-evaluation of the objection proceedings by a new panel (the *.hospital* case), or to overturn a determination (the *.amazon* case).

15 The rest of this section is divided in three parts: I will start by examining the results of the objection procedure on the grounds of limited public interest (I) and community (II). Then I will consider ICANN's role regarding the production and implementation of a global standard for freedom of expression online (III).

I. Limited Public Interest

16 The expert panel hearing a Limited Public Interest objection had to determine whether the applied-for gTLD string was contrary to "general principles of international law for morality and public order".[63] The AGB provided for an illustrative, non-exhaustive list of international instruments where such general principles of international law for morality and public order could allegedly be found.[64] It added that, *a contrario*, national laws not based on principles of international law were not valid grounds for a Limited Public Interest objection. According to ICANN, under these principles, everyone has the right to freedom of expression, but the exercise of this right carries with it special duties and responsibilities. The Guidebook provided four grounds upon which applicants' freedom of expression could be restricted. These standards were developed by ICANN's staff after conducting both a comparative study in nine jurisdictions[65] and

57 ICANN announced in May 2012 that Alain Pellet, a French professor of public international law, would serve as the independent objector.

58 AGB, § 3.2.5.

59 AGB, § 3.2.5.

60 AGB, § 3.4.6.

61 Independent Objector, Final Activity Report, 29 July 2014, <http://www.independent-objector-newgtlds.org/home/final-activity-report>, p. 31.

62 AGB, § 5.1.

63 AGB, § 3.5.3.

64 The AGB mentions the following international instruments: the Universal Declaration of Human Rights (UDHR); the International Covenant on Civil and Political Rights (ICCPR); the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW); the International Convention on the Elimination of All Forms of Racial Discrimination; Declaration on the Elimination of Violence against Women, the International Covenant on Economic, Social, and Cultural Rights; the Convention against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment; the International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families; the Slavery Convention; the Convention on the Prevention and Punishment of the Crime of Genocide and the Convention on the Rights of the Child.

65 The study included the following countries: Brazil,

consultations with international law specialists. This research work concluded that considering the variety of potential gTLD strings that might be at issue in dispute proceedings, "panels should have discretion to apply general principles to individual cases".[66] At the same time, ICANN's staff identified public policy rules considered to be "widely if not universally, accepted as grounds for limiting freedom of expression",[67] to guide the experts in the exercise of their discretion. These rules constituted the first three grounds of restriction, incorporated in the AGB as follows: incitement to or promotion of (1) "violent lawless action"; (2) "discrimination based upon race, colour, gender, ethnicity, religion or national origin, or other similar types of discrimination that violate generally accepted legal norms recognized under principles of international law"; and (3) "child pornography or other sexual abuse of children". The fourth ground expressed the discretion granted to the expert panels, as it enabled them to assess the conformity of applied-for gTLDs with "specific principles of international law as reflected in relevant international instruments of law". In practice, all the Limited Public Interest objections were based upon this broad fourth ground.

17 Anyone could file a Limited Public Interest objection, as the AGB did not impose standing requirements. Limited Public Interest was however the least used ground of the objections procedure: only twenty-three objections were filed against health-related strings (*.health, .healthcare, .med, .medical, .hospital*) and strings linked to the financial sector (*.broker, .ira, .mutualfunds, .retirement*). Few private parties used this opportunity and most of the Limited Public Interest objections were filed by the independent objector. Most of the Limited Public Interest objections were either dismissed by the expert panels or withdrawn before the final determination. Only one objection was upheld – in the *.hospital* case – with a dissenting opinion.[68] However, this similarity in outcome should not conceal that expert panels had very divergent opinions on their scope of examination and the subsequent substantive assessment of the cases, especially regarding objections brought against health-related strings.

18 The independent objector filed several objections against gTLDs related to the health sector, alleging that these strings, viewed in context with the intended purpose stated in the application, would be contrary to the right to health enshrined in Article 25 of the Universal Declaration of Human Rights and in other instruments of international law such as the International Covenant on Economic, Social and Cultural Rights. In the independent objector's view, "any good-faith-interpretation of the meaning of the right to receive or have access to health-related information will conclude that this right implies to receive or have access to *reliable and trustworthy* information".[69] Therefore, the independent objector argued that any applicant for a health-related gTLD should demonstrate that it would effectively and continuously manage the gTLD in such a way that the right to health with all of its implications – including the necessity of reliability and trustworthiness – is fully respected. The independent objector reviewed the health-related applications against this general background and found that none of the applicants met the standards outlined above. One of the independent objector's recurring concerns was that applicants would apply the same operating rules and protection measures for all the gTLDs that they requested, without showing awareness of the specificities of a health-related TLD.

19 The initial question for the experts appointed by the International Centre of Expertise of the ICC was to set their scope of examination and therefore determine whether they should restrict their analysis to the applied-for gTLD or take other elements into account. The answer to this question was not obvious. The Applicant Guidebook states that "the panel will conduct its analysis on the basis of the applied-for gTLD string itself" and that "the panel may, *if needed*, use as additional context the *intended purpose* of the TLD as stated in the application".[70] Experts drew different conclusions from this wording. Most panels followed a broad interpretation of this provision, which was also favored by the independent objector. In the *.healthcare* case for example, the panel found that it should "look at how the TLD will be operated as proposed in the application"[71] and emphasized that the issue at stake was the propriety *and the regulation* of the proposed gTLD.[72] Some experts adopted a stricter interpretation of the AGB standard and, therefore, significantly limited their scope of examination. In the *.medical*

Egypt, France, Hong Kong, Japan, Malaysia, South Africa, Switzerland and the U.S.

66 ICANN, New gTLD Program Explanatory Memorandum: Standards for Morality and Public Order Research, 30 May 2009, <http://www.icann.org/en/topics/new-gtlds/morality-public-order-30may09-en.pdf>.

67 ICANN, New gTLD Program Explanatory Memorandum: Morality and Public Order Objection Considerations in New gTLDs, 29 October 2008, < http://www.icann.org/en/topics/new-gtlds/morality-public-order-draft-29oct08-en.pdf >, p. 4.

68 All the expert determinations rendered on objections filed against new gTLD applications are fully available from: <http://newgtlds.icann.org/en/program-status/odr/determination>.

69 All of the independent objector's objections are available from: <http://www.independent-objector-newgtlds.org/home/the-independent-objector-s-objections>.

70 AGB, § 3.5.3 (emphasis added).

71 ICC, International Centre for Expertise, *Independent Objector vs. Silver Glen LLC*, 26 November 2013, EXP/411/ICANN/28 (.healthcare), § 25.

72 *Id.*, § 35 (emphasis added).

case, the panel considered that the starting point had to be "whether the string .medical is contrary to general principles of international law for morality and public order, *not whether the internet content potentially available under that string conforms to such principles*".[73] In other words, the subject matter for the determination of the Panel was "the applied-for gTLD string *.medical* itself, *not the way Applicant intends to manage that string*".[74] A similar strict interpretation of the AGB standard was adopted by the panel in two consolidated *.health* cases. The panel found that the primary conjecture of the independent objector – *i.e.* that a *.health* registry as operated by the applicant would not be adequately safeguarded or protective enough of human rights to health – changed "nothing to the fact that the word "health" is by no means inherently objectionable".[75]

20 This divergence of opinions was mirrored in the substantive assessment of the objections by the expert panels, which all acknowledged that the right to health is a fundamental right and a specific principle of international law. The expert panels favoring a strict interpretation of their scope of examination quickly dismissed the objections.[76] In the other cases, the panels either examined the independent objector's arguments within the context of the applicants' registration policies and commitments to protect the public interest (such as eligibility requirements or anti-abuse remedies),[77] or they chose to balance the claims related to the right to health with the right to freedom of expression. These latter cases triggered another disagreement among experts. In the *.med* cases, the panel considered that a restriction of free expression cannot be justified solely on the basis of its purported positive consequences on the right to health. Following such a path would, in the view of the panel, result "in endless expansions in the permissible limitations of freedom of expression by reference to consequentialist arguments about the impact that a particular restriction could have on the enjoyment of other rights".[78] According to the panel, the information-related element of the right to health is the right to have access to information that is reliable and trustworthy but does not include the right to be protected from the mere risk of misleading or unreliable information.[79] As the independent objector failed to prove a significant risk of dissemination of misleading or unreliable information, while the applicant provided "various assurances, most notably *in relation to the administration of the gTLD*",[80] the panel dismissed the objections.

21 The expert determination issued in the *.hospital* case adopted a completely different approach regarding the kind of balance to strike between the right to health and freedom of expression. The majority of the panel stated that freedom of expression is connected with special duties and responsibilities and that, in the *.hospital* case, "those duties include an application of very specific protection and an awareness of the importance of the role of hospitals in delivering credible healthcare objectives".[81] The majority found that the applicant "failed to avert its mind to these responsibilities" and as a consequence, the application breached the right to health and fell outside of the scope of freedom of expression.[82] The majority elaborated further that the case was an example of "a hard case which requires not only the simple application of legal rules, but also balancing different values and rules".[83] In that case, freedom of expression and the development of services in the Internet had to be balanced with the right to health and even right to life.[84] According to the majority of the expert panel, there was "no doubt that human health and its safety tips the scale in finding the Objection to be justified".[85] However, one of the panelists presented a dissenting opinion, stating that he was unable to concur with the majority in

73 ICC, International Centre for Expertise, *Independent Objector vs. Steel Hill LLC*, 2 January 2014, EXP/413/ICANN/30 (*.medical*), § 49 (emphasis added).

74 *Id.* (emphasis added).

75 ICC, International Centre for Expertise, *Independent Objector vs. DotHealth LLC*, 16 December 2013, EXP/416/ICANN/33 (*.health*), § 89; *Independent Objector vs. Goose Fest LLC*, 16 December 2013, EXP/417/ICANN/34 (*.health*), § 92.

76 ICC, International Centre for Expertise, *Independent Objector vs. DotHealth LLC*, 16 December 2013, EXP/416/ICANN/33 (*.health*), § 103; *Independent Objector vs. Goose Fest LLC*, 16 December 2013, EXP/417/ICANN/34 (*.health*), § 106; *Independent Objector vs. Steel Hill LLC*, 2 January 2014, EXP/413/ICANN/30 (*.medical*), § 50.

77 ICC, International Centre for Expertise, *Independent Objector vs. Affilias Limited*, 6 November 2013, EXP/409/ICANN/26 (*.health*), §§ 66-77; *Independent Objector vs. Silver Glen LLC*, 26 November 2013, EXP/411/ICANN/28 (*.healthcare*), §§ 47-55.

78 ICC, International Centre for Expertise, *Independent Objector vs. HEXAP SAS*, 19 December 2013, EXP/410/ICANN/27 (*.med*), § 112; I*ndependent Objector vs. Medistry LLC*, 19 December 2013, EXP/414/ICANN/31 (*.med*), § 108; *Independent Objector vs. Charleston Road Registry Inc.*, 19 December 2013, EXP/415/ICANN/32 (*.med*), § 103.

79 *Id.*, EXP/410/ICANN/27 (*.med*), § 113; EXP/414/ICANN/31 (*.med*), § 109; EXP/415/ICANN/32 (*.med*), § 104.

80 *Id.*, EXP/410/ICANN/27 (*.med*), § 120; EXP/414/ICANN/31 (*.med*), § 116; EXP/415/ICANN/32 (*.med*), § 111 (emphasis added).

81 ICC, International Centre for Expertise, *Independent Objector vs. Ruby Pike LLC*, 11 December 2013, EXP/412/ICANN/29 (*.hospital*), Determination of the majority, § 88.

82 *Id.*, §§ 87-88.

83 The panel referred to R. Dworkin, *Taking rights seriously* (1977).

84 ICC, International Centre for Expertise, *Independent Objector vs. Ruby Pike LLC*, 11 December 2013, EXP/412/ICANN/29 (*.hospital*), Determination of the majority, § 89.

85 *Id.*

upholding the objection. In his view, it was "not the task of an expert panel to rewrite the application standards for gTLD strings and to supplement them with higher standards in the public interest".[86] Even if he was sympathetic to the majority's concern about the lack of a specific guarantee to ensure reliability and trustworthiness of the information under the *.hospital* gTLD, he could not "tell from the current ICANN registration prerequisites that such an implied substantive, content-wise check is a precondition for a gTLD string registration".[87]

22 The *.hospital* expert determination rendered in December 2013 clearly stands out from the other eight Limited Public Interest expert determinations on health-related gTLDs. The losing applicant, Ruby Pike LLC – a subsidiary of Donuts Inc., which applied for 307 new gTLDs under various aliases – immediately argued that the panel failed to apply the standards defined by the Guidebook and exceeded its powers. In the absence of a specific appeal mechanism, Ruby Pike LLC resorted to two of ICANN's accountability mechanisms to challenge the determination. First, Ruby Pike LLC submitted a request of reconsideration to the ICANN Board Governance Committee (BGC).[88] Several losing parties turned to the BGC for review of an expert determination – most of the time without success – as the BGC constantly refused to perform a substantive review of the determinations. The BGC's review was limited to whether the panel (or ICANN staff in accepting the determination) violated any established ICANN policy or process.[89] The BGC denied Ruby Pike LLC's request in February 2014, determining that there was no evidence that the panel deviated from the standards set forth in the Guidebook.[90] Second, Ruby Pike LLC initiated a Cooperative Engagement Process[91] regarding the determination. As part of this process, the ICANN Board evaluated Ruby Pike LLC's claims and decided in February 2016 to direct a re-evaluation of the objection proceedings by a new expert panel appointed by the ICC.[92] The Board found that the determination was seemingly inconsistent with the expert determinations resulting from all the other health-related Limited Public Interest objections, thereby rendering it potentially unreasonable. The Board took into consideration, *inter alia*, that the *.hospital* case was one of the four virtually identical Limited Public Interest objections brought against subsidiaries of Donuts, Inc. and that the *.hospital* determination was the only one in favor of the objector. The new expert panel was instructed by the Board to determine whether the original expert panel could have reasonably come to the decision reached in the first expert determination through an appropriate application of the standard of review as set forth in the Guidebook, considering the other eight Limited Public Interest expert determinations on health-related gTLDs.[93]

23 The final expert determination on the objection filed against *.hospital* was rendered in August 2016 and resulted in the reversal of the original determination. The new expert panel favored a strict interpretation of its scope of examination and found the first expert determination to be unreasonable because it placed too much emphasis on the intended purpose of the applied-for gTLD[94] and because it restricted the applicant's freedom of expression in favor of a concern – the access to accurate information concerning health-related issues – which is not a specific principle of international law.[95] In the new panel's view, whether Ruby Pike LLC can adequately manage the use of *.hospital* through the use of safeguards or other measures is a policy matter for ICANN to address at a different stage of the application process.[96]

86 ICC, International Centre for Expertise, *Independent Objector vs. Ruby Pike LLC*, 11 December 2013, EXP/412/ICANN/29 (*.hospital*), Dissenting opinion, § 17.

87 *Id.*, § 29.

88 The reconsideration process enables any person or entity materially affected by an action (or inaction) of ICANN to request review or reconsideration of that action by the BGC (ICANN, Bylaws, Article IV, Section 2).

89 ICANN, BGC, Recommendation on Reconsideration request 13-5, 1 August 2013, <http://www.icann.org/en/groups/board/governance/reconsideration/13-5/recommendation-booking-01aug13-en.pdf>.

90 ICANN, BGC, Determination on Reconsideration request 13-23, 5 February 2014, <http://www.icann.org/en/system/files/files/determination-ruby-pike-05feb14-en.pdf>.

91 The Cooperative Engagement Process is a process voluntarily invoked by a complainant prior to the filing of an Independent Review Process (see supra note 42) for the purpose of resolving or narrowing the issues that are contemplated to be brought to the Independent Review Process (ICANN, Bylaws, Article IV, Section 3, §§ 14-17).

92 The ICANN Board provided for a similar review mechanism to address a perceived inconsistency in two sets of expert determinations rendered on the ground of string confusion (ICANN, Meeting of the Board New gTLD Program Committee, Resolutions 2014.10.12.NG02 – 2014.10.12.NG03, 12 October 2014, <http://www.icann.org/resources/board-material/resolutions-new-gtld-2014-10-12-en>).

93 ICANN, Regular Meeting of the Board, Resolutions 2016.02.03.12- 2016.02.03.13, 3 February 2016, <http://www.icann.org/resources/board-material/resolutions-2016-02-03-en>.

94 ICC, International Centre for ADR, Internet Corporation for Assigned Names and Numbers in relation to the matter EXP/412/ICANN/29 between *Independent Objector vs. Ruby Pike LLC*, 31 August 2016, §§ 64-69.

95 *Id.*, §§ 70-76.

96 *Id.*, §§ 77-79.

II. Community Objections

24 Community objections were intended for the cases of substantial opposition to a gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.[97] Strict standing requirements were imposed on the objectors: next to the independent objector, only "established institutions associated with clearly delineated communities" were eligible to file a community objection.[98] As to the substantive assessment of the cases, the AGB set out four conditions, which had to be met cumulatively for a community objection to prevail. The objector had to prove (1) that the community invoked was a clearly delineated community; (2) that community opposition to the application was substantial; (3) that there was a strong association between the community invoked and the applied-for gTLD string; and finally (4) that the application created a likelihood of material detriment to the rights or legitimate interests of a significant portion of the affected community. For each ground, the Guidebook provided an illustrative list of factors that could be taken into account by the panel while examining the objection. A balancing of the factors, as well as any other relevant information, had to be weighed by the panel in order to draw its conclusions.

25 In contrast to limited public interest, community was the most used ground of objection: 104 objections were filed resulting in seventy-three expert determinations.[99] Out of the 48 cases that passed the standing test, 15 objections were upheld and 33 were dismissed, mainly because the panel did not find a likelihood of material detriment.

26 Just like most objections on the ground of limited public interest, the proposed registration policy was paramount to the assessment of community objections. Panels paid attention to the presence of three types of safeguards: eligibility requirements, *ex post* anti-abuse policies, and commitments to involve the targeted community in the management of the gTLD. First, most of the panels reviewing applications for strings related to regulated sectors considered that eligibility requirements were necessary to preserve consumer trust and the reputation of the community. For example, in the *.architect* case, the panel found that it would be incompatible with the public interests linked to the work of architects (primarily public safety) and with the consumers' legitimate expectations to allow the domain name *.architect* to be used by anyone other than a licensed architect. The panel stated explicitly that free speech was not an unlimited right and could be subject to limitations in the public interest.[100] Most objections regarding gTLDs targeted to regulated sectors (such as *.medical*[101] and *.insurance*[102]) were likewise upheld if the applicant did not plan to restrict registration to members of the targeted sector.

27 Second, *ex post* anti-abuse measures were generally featured in the challenged applications and those measures were well received by the expert panels. For example, the anti-abuse policy proposed by the applicant for *.islam* and *.halal* was an important basis in the panel's finding that there was no likelihood of detriment to the Muslim community.[103] The panel welcomed the applicant's commitment to operate the gTLDs in a manner that would prevent "radical content or criticism of Islam and the Muslim faith" and to "take immediate and severe action against this should it occur".[104] Not only did the applicant propose to implement strict eligibility requirements, but it would also subject all second-level domains to a policy of use and impose penalties and suspensions upon those who violated the user's policy.[105]

28 Third, involvement of the community was another important element in the experts' evaluation of the applications. The expert panels were not unanimous on that question: in cases regarding TLDs targeting regulated sectors[106] and sports,[107] lack of community

97 AGB, § 3.2.1.

98 AGB, § 3.2.2.4.

99 All the expert determinations rendered on objections filed against new gTLD applications are fully available from: <http://newgtlds.icann.org/en/program-status/odr/determination>.

100 ICC, International Centre for Expertise, *The International Union of Architects vs. Spring Frostbite LLC*, 3 September 2013, EXP/384/ICANN/1 (*.architect*), § 129.

101 ICC, International Centre for Expertise, I*ndependent Objector vs. Steel Hill LLC*, 21 November 2013, EXP/407/ICANN/24 (*.medical*), §§ 161-166.

102 ICC, International Centre for Expertise, *The Financial Services Roundtable vs. Auburn Park LLC*, 14 January 2014, EXP/432/ICANN/49 (*.insurance*), §§ 175-178.

103 ICC, International Centre for Expertise, *Telecommunications Regulatory Authority of the United Arab Emirates vs. Asia Green IT System Bilgisayar San. ve Tic. Ltd. Sti.*, 24 October 2013, EXP/430/ICANN/47 (*.islam*), §§ 136-145 & EXP/427/ICANN/44 (*.halal*), §§ 143-152.

104 Id., EXP/430/ICANN/47 (*.islam*), § 142; EXP/427/ICANN/44 (*.halal*), § 149.

105 *Id.*, EXP/430/ICANN/47 (*.islam*), § 144; EXP/427/ICANN/44 (*.halal*), § 151.

106 ICC, International Centre for Expertise, *Independent Objector vs. Charleston Road Registry Inc.*, 30 December 2013, EXP/404/ICANN/21 (*.med*), § 81; *International Banking Federation vs. Dotsecure Inc.*, 26 November 2013, EXP/389/ICANN/6 (*.bank*), §§ 163-166.

107 ICC, International Centre for Expertise, *Sportaccord vs. Dot Sport Limited*, 23 October 2013, EXP/471/ICANN/88 (*.sport*), § 158; *Sportaccord vs. Steel Edge LLC*, 21 January 2014, EXP/486/ICANN/103 (*.sports*), § 43.4; *Fédération Internationale de Ski vs. Wild Lake LLC*, 21 January 2014, EXP/421/ICANN/38 (*.ski*), § 48.4; *International Rugby Board vs. Dot Rugby Limited*, 31 January 2014, EXP/517/ICANN/132 (*.rugby*), § 76; *International Rugby Board vs. Atomic Cross LLC*, 31 January

involvement and unaccountability of the registry to the targeted community was sufficient to create a likelihood of material detriment, whereas in the *.gay* and *.amazon* cases, panels were unimpressed by the claim that the commercial operation of the gTLD would be equivalent to exploitation of the targeted community. In three objections brought against applications for *.gay* made by commercial entities, the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA) claimed that taking a group's name and using it to create a profitable business should be regarded as exploitation, unless it is done for and endorsed by the relevant community. Such an endorsement existed for a fourth applicant for the *.gay* string, Dotgay, which had filed an application supported by ILGA and other LGBTQ organizations.[108] The three other applicants were all planning to operate the *.gay* for profit and in an open manner, allowing anyone to register a *.gay* domain name.[109] In ILGA's view, these applications constituted a major damage for the gay community, insofar as they could deprive the community of the chance to operate its own string. The panel acknowledged that this lost chance might be regarded as detrimental to the legitimate interests of the gay community, but considered that this detriment alone was not sufficient to uphold the objection. In the panel's view, the explicit exclusion in the AGB of "detriment that consists only of the applicant being delegated the string instead of the objector"[110] applied in that case, even if ILGA and Dotgay were separate institutions, because they shared identical interests.[111] Moreover, the panel made it clear that its task was not to determine which applicant would be the best registry for a gTLD sought by different parties.[112]

29 In the *.amazon* case, the panel was similarly not convinced by the arguments brought forward by the independent objector against applications filed by the online retailer Amazon. Amazon wished to use its trademark "amazon" (in English, Japanese, and Chinese) as a closed gTLD, meaning that the only eligible registrants would have been Amazon and its subsidiaries. According to the independent objector, this registration policy entailed a risk of misappropriation, because granting exclusive rights on the strings to a private company would prevent the use of the domains for public interest purposes related to the protection, promotion and awareness-raising on issues related to the Amazon region. The panel did not follow these arguments for two reasons.[113] First, the panel noted that even if the objection was successful, the Amazon community would still not be entitled to use the gTLDs, since it did not apply for them. Therefore the panel found that the use of the strings was not crucial to the protection of the Amazon community's interests. Second, the panel considered that "amazon" had been used as a brand, trademark and domain name for nearly two decades, also in the States forming part of the Amazon community, without any evidence that this has caused harm to the Amazon community's interests. In the panel's view, "it is unlikely that the loss of the ".com" after "Amazon" will change matters".[114] The objection was then rejected and the application process should have continued; however, Amazon's success was short lived. Indeed, the Governmental Advisory Committee reached a consensus against the *.amazon* applications[115] and obtained the rejection of the applications by the Board.[116] Pursuant to the AGB, if the GAC advised that there was a *consensus* among the GAC members that a particular application should not proceed, it would "create a *strong presumption* for the ICANN Board that the application should not be approved".[117] The *.amazon* case was particularly controversial: it took almost a year for the Board to balance the competing interests of governments and of Amazon, and to finally decide in favor of the GAC.

2014, EXP/519/ICANN/134 (*.rugby*), § 90.

108 Dotgay would notably restrict registrations to only *bona fide* members of the community through the use of an authentication system relying on partners from all segments of the LGBTQ community, and work on a non-profit basis, devoting its revenues to fund gay organizations and other initiatives in the community (Application for *.gay* filed by Dotgay, 1-1713-23699, Response to questions 18(b) and 20(e), available from: <http://gtldresult.icann.org/application-result/applicationstatus/applicationdetails/444>).

109 Only one applicant (Top Level Domain Holdings Limited) indicated it would provide for a procedure to report inappropriate, harmful or damaging content.

110 AGB, § 3.5.4.

111 ICC, International Centre for Expertise, *The International Lesbian Gay Bisexual Trans and Intersex Association (ILGA) vs. Top Level Design LLC*, 16 November 2013, EXP/392/ICANN/9 (*.gay*), §§ 22-31; *ILGA vs. Top Level Domain Holdings Limited*, 16 November 2013, EXP/393/ICANN/10 (*.gay*), §§ 21-30; *ILGA vs. United TLD Holdco Ltd.*, 16 November 2013, EXP/394/ICANN/11 (*.gay*), §§ 22-31.

112 String contention (*i.e.* the scenario in which several applications for identical or confusingly similar strings remain after the initial evaluation performed by ICANN and potential objection proceedings) is dealt with in a subsequent procedure (AGB, Module 4).

113 ICC, International Centre for Expertise, *Independent Objector vs. Amazon EU S.à.r.l*, 27 January 2014, Consolidated cases EXP/396/ICANN/13 (*.amazon*), EXP/397/ICANN/14 (.アマゾン) and EXP/398/ICANN/15 (.亚逊), §§ 99-105.

114 *Id.*, § 103.

115 GAC, Durban Communiqué, 18 July 2013, <http://durban47.icann.org/meetings/durban2013/presentation-gac-communique-18jul13-en.pdf>, IV.1.a.i.

116 ICANN, Meeting of the Board New gTLD Program Committee, 14 May 2014, Resolution 2014.05.14.NG03, <http://www.icann.org/resources/board-material/resolutions-new-gtld-2014-05-14-en>.

117 AGB, § 3.1.

III. A global standard for freedom of expression

30 With the New gTLDs Program, ICANN produced and enforced a form of global standard for freedom of expression, more precisely of the grounds that could justify restrictions to the imagination of prospective registries for new gTLDs. It has been without doubt the most delicate policy question facing ICANN since 1998, going far beyond its technical mandate to coordinate the Internet's identifiers. Furthermore, it was indeed a burdensome task, considering the diversity of existing laws governing speech around the globe. This long policy development process resulted in relatively broad standards. Consequently, expert panels appointed by the International Chamber of Commerce adopted different interpretations of the AGB standards, which led to opposite determinations in similar cases. In the Limited Public Interest objection proceedings, the most obvious point of disagreement was the panels' scope of examination, as discussed above. Most of the panels accepted to review the intended purpose of the application even if the applied-for gTLD was not highly objectionable as such, while other panels opting for a stricter interpretation of the AGB easily concluded that words like "health" or "medical" did not violate the right to health. The discretion granted to the expert panels undermined the objectives of predictability and fairness of the new gTLD application process, in the absence of a system of binding precedents or independent review mechanisms to ensure a harmonized interpretation of the AGB standards.[118] The ICANN Board only provided for *ad hoc* review mechanisms in the case of seeming inconsistency, which resulted in particularly lengthy dispute resolution proceedings in those few cases. As seen with the controversial *.hospital* case, it took almost three years to correct the too broad interpretation of the AGB favored by the original expert panel. The independence of the objection process was also undermined by these potential interventions of the ICANN Board.

31 ICANN has engaged in very delicate debates by developing this global standard for freedom of expression and it is not the end of the story. ICANN is now requested by various constituencies (intellectual property interests and some governments) to assume greater responsibilities for policing illegal content on the Internet, by increasing the obligations of domain name registries and registrars confronted with reports of abuse within the domains they administer. In the following section, I will examine this heated debate and examine how these technical operators could be transformed into points of control of online speech.

D. New Contractual Obligations of Domain Names Registries and Registrar

32 Obligations imposed by ICANN on domain name registries were substantially increased with the New gTLD Program. This evolution was not the goal of the program, but rather the consequence of several advices submitted to the ICANN Board by the Governmental Advisory Committee and implemented by ICANN after the publication of the Applicant Guidebook. Indeed, while the AGB left it up to the applicants to decide whether or not they would use eligibility criteria or heightened rights protection mechanisms, the GAC lobbied to impose mandatory safeguards on broad categories of new gTLDs. As a consequence, standards applicable to the registration policies for new gTLDs were amended during the course of the evaluation of the applications.

33 The GAC submitted advice to the ICANN Board on two general issues related to the New gTLD Program: (1) the binding and enforceable nature of the commitments made by the prospective registries in their applications; and (2) the imposition of safeguards for broad categories of strings. The GAC advice was accepted by the Board in both cases, which led to amendments to the Registry Agreement (RA), which is the formal written and binding agreement between the applicant and ICANN that sets forth the rights, duties, liabilities and obligations of the applicant as a registry operator. ICANN uses a standard-format Registry Agreement rather than personalized agreements. A revised standard agreement was developed during the application process, based on a draft agreement annexed to Module 5 of the AGB, and formally adopted in July 2013.[119] As registries cannot offer direct registration services to the public, they enter into agreements (Registry-Registrar Agreement, RRA) with registrars. Registrars are required to obtain accreditation from ICANN (through a Registrar Accreditation Agreement, RAA) to be able to offer registration services to the public and enter into registration agreements with the prospective domain name

118 The ICANN Board acknowledged that establishing a general review mechanism may be appropriate in future rounds of the New gTLDs Program, to promote the goals of predictability and fairness (ICANN, Regular Meeting of the Board, Rationale to Resolutions 2016.02.03.12- 2016.02.03.13, 3 February 2016, <http://www.icann.org/resources/board-material/resolutions-2016-02-03-en>).

119 The Base Registry Agreement and all Registry Agreements are available from: <http://www.icann.org/resources/pages/registries-2012-02-25-en>.

holders.[120]

34 The first GAC advice requested the Board of ICANN to explain how ICANN would ensure that any commitment made by applicants, in their applications or as a result of any subsequent change, would be overseen and enforced by ICANN. Specifically, the GAC advised that these commitments should be transformed into binding contractual commitments, subject to compliance oversight by ICANN.[121] In response to the GAC and as part of the revision of the Base Registry Agreement, the ICANN Board introduced a new schedule (Specification 11) to the agreement: the Public Interest Commitments (PICs).[122] The Public Interest Commitments Specification is a mechanism to allow a registry operator to commit to certain statements made in its application for the gTLD,[123] as well as to specify additional public interest commitments[124]. Pursuant to the terms of the revised Base Registry Agreement, these commitments become part of the agreement[125] and are enforceable by ICANN through a new dispute resolution mechanism.[126] Registries have to agree to implement and adhere to any remedies ICANN imposes, which may include the termination of the Registry Agreement.[127] In February 2013 ICANN requested all applicants to submit a TLD-specific Public Interest Commitments Specification and received a total of 499 PIC Specifications.[128] Until then, the process was voluntary and applicants were free to submit commitments to be incorporated in the Registry Agreement.

35 The second general advice submitted by the GAC called for the adoption of safeguards applicable to broad categories of new gTLDs.[129] Among the six safeguards recommended by the GAC to apply to all new gTLDs, three are particularly interesting in terms of the content control obligations they entail for all new gTLD registries. Under the headline "Mitigating abusive activity", the GAC advised that registry operators should "ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in *activity contrary to applicable law*".[130] Then, the GAC advised that a mechanism to make complaints on these grounds should be adopted by the registry operators,[131] as well as "real and immediate consequences for the demonstration of (...) violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include *suspension of the domain name*".[132]

36 The general safeguards proposed by the GAC were adopted by the ICANN Board and implemented as mandatory PICs in Specification 11 of the Base Registry Agreement.[133] However, because the registry operator does not have a direct contractual relationship with the domain name holders, the Board adopted a PIC Specification that requires the registry operator to "include a provision in its Registry-Registrar Agreement (RRA) that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging *in activity contrary to applicable law*, and providing (consistent with applicable law and any related procedures) consequences for such activities including *suspension* of the domain name".[134] Section 2.8 of the Registry Agreement also provides that a registry "shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD". Additionally, Specification 11(1) of the Registry Agreement requires registries of new gTLDs to use only registrars that are party to the 2013 Registrar Accreditation

120 For a detailed account of the contractual network of the gTLD namespace, see E. Weitzenboeck, 'Hybrid net: the regulatory framework of ICANN and the DNS' (2014) 22(1) *International Journal of Law and Information Technology*, at pp. 54-59.

121 GAC, Toronto Communiqué, 17 October 2012, IV.1, <http://gacweb.icann.org/download/attachments/28278845/FINAL_Toronto_Communique_20121017.pdf>.

122 ICANN, Base Registry Agreement, updated 9 January 2014, Specification 11 <http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.pdf>.

123 Specification 11(2) of the Base Registry Agreement.

124 Specification 11(3) of the Base Registry Agreement.

125 Section 2.17 of the Base Registry Agreement states: "Registry Operator shall comply with the public interest commitments set forth in Specification 11 attached hereto".

126 Public Interest Commitment Dispute Resolution Procedure (PICDRP), 19 December 2013, <http://newgtlds.icann.org/en/applicants/agb/picdrp-19dec13-en.pdf>.

127 Specification 11(3) of the Base Registry Agreement.

128 ICANN, Posting of Public Interest Commitments (PIC) Specifications Completed, 6 March 2013, <http://newgtlds.icann.org/en/announcements-and-media/announcement-06mar13-en>.

129 GAC, Beijing Communiqué, 11 April 2013, <http://gacweb.icann.org/download/attachments/27132037/Beijing%20Communique%20april2013_Final.pdf>.

130 GAC Beijing Communiqué, Safeguard 2, p. 7 (emphasis added).

131 *Id.*, Safeguard 5, p. 8.

132 *Id.*, Safeguard 6, p. 8 (emphasis added).

133 ICANN, Meeting of the Board New gTLD Program Committee, Resolutions 2013.06.25.NG02 and 2013.06.25.NG03, 25 June 2013, <http://www.icann.org/resources/board-material/resolutions-new-gtld-2013-06-25-en>.

134 Specification 11.3(a) of the Base Registry Agreement (emphasis added).

Agreement (RAA).[135] As a result, registrars that wanted to offer registration services for new gTLDs were obliged to sign a new RAA with ICANN, even if their accreditation under the previous agreement had not expired yet. The new version of the RAA, adopted in June 2013, notably includes a new section 3.18 entitled "Registrar's Abuse Contact and Duty to Investigate Reports of Abuse". It provides that registrars must establish a dedicated email address to "receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity". All reports must be investigated by the registrar and responded to "appropriately". Information regarding "procedures for the receipt, handling, and tracking of abuse reports" must be published on the website of the registrar, which must "document its receipt of and response to all such reports". Additional requirements apply if the abuse complaint is filed by "law enforcement, consumer protection, quasi-governmental or other similar authorities": the reports must be reviewed "within 24 hours by an individual who is empowered by Registrar to take *necessary and appropriate actions* in response to the report". The RAA indicates that "in responding to any such reports, Registrar will not be required to take any action in contravention of applicable law".[136]

37 Domain name suspension, which is provided in Specification 11(3)a of the Registry Agreement as a potential consequence to illegal activities of the domain name registrant, is a powerful tool to deny access to online content. The registry, which controls the authoritative record for resolving each SLD within its TLD, has the technical capacity either for deleting the connection between the domain name and the associated IP address in the database, or for diverting a domain name to another IP address, such as one pointing to a law enforcement message (see below). Domain name resolution can also be suspended by the registrar that assigned the domain name.[137] In both cases an Internet user who would type the web address containing the suspended domain name in his web browser would not be able to find the requested website. The DNS would return a non-existent or different domain response. This technique is easy to implement as it is not necessary to locate and confiscate the server hosting the content. Indeed, the content itself is not taken down – it can still be accessed via the IP address but most Internet users would be unable to do so, because they would not know the IP address of a specific website.

38 Using the DNS as a tool for law enforcement is not a new strategy. In 2008 the U.S. Congress enacted a law (the "Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act") to expand the scope of civil forfeiture (the process by which the government can seize property that was used in connection with an illegal activity) to encompass the seizure of property used to facilitate copyright infringement and counterfeiting.[138] Civil forfeiture operates *in rem*: it is brought against the property and not against its owner, based on the legal fiction that the property itself is guilty of wrongdoing.[139] Civil forfeiture has been increasingly used by the U.S. Immigration and Customs Enforcement (ICE), in an initiative called "Operation in Our Sites",[140] to seize thousands of domain names of websites infringing copyright or proposing counterfeited goods. U.S. jurisdiction is asserted on domain names that are administered by a U.S.-based registry (like Verisign for the *.com* TLD) or that were purchased through an U.S.-based registrar, regardless of the location of the activities of the domain name holder. As a consequence, the domain name may be seized, even if U.S. courts would not have personal jurisdiction over the domain name holder.[141] In practical terms, the seizure is accomplished with an *ex parte* court warrant ordering the domain name registry to redirect traffic from the seized domain to a website with a law enforcement message from the U.S. government.

39 With the new mandatory safeguard advised by the GAC, the role of registries and registrars as critical Internet points of control to deal with online illegal activities is reinforced. In the procedure of seizure described above, DNS operators have to comply with decisions made by judicial authorities without having to examine themselves if the content is illegal.[142] By contrast, under the new obligations of the RA and RAA, registries and registrars must

135 Specification 11(1) of the Base Registry Agreement.

136 ICANN, 2013 Registrar Accreditation Agreement, <http://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>, § 3.18 (emphasis added).

137 L. DeNardis (2012), *supra* note 1, p.728.

138 Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, Section 206(a), Pub. L. No. 110-403, 122 Stat. 4256 (codified at 18 U.S. Code § 2323).

139 A. Bridy, 'Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy' (2012) 46 *Arizona State Law Journal*, spec. pp. 688-694.

140 K. Kopel, 'Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice' (2013) 28 *Berkeley Technology Law Journal* pp. 859-900.

141 J. Mellyn, 'Reach Out and Touch Someone: The Growing Use of Domain Name seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law' (2011) 42 *Georgetown Journal of International Law* pp. 1241-1264.

142 Following legal actions that involved seizures and transfers of domain names to dismantle criminal networks, ICANN staff published a "thought paper" to offer guidance for preparing orders that seek to seize or take down domain names (ICANN, "Guidance for Preparing Domain Name Orders, Seizures & Takedowns", 7 March 2012, <http://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf>).

offer a point of contact to receive reports of abuse from law enforcement agencies and must respond "appropriately" to these reports,[143] therefore implying a form of examination of the claim of abuse. Additionally, anyone can report to a registrar an allegedly illegal activity involving a domain name. Nothing prevents registries and registrars from using domain name suspension as a reaction to these reports, even if there is no court order or warrant to support it. And the new contractual obligations of registries and registrars are not limited to issues of copyright infringement and counterfeiting: any activity contrary to applicable law could lead to the suspension of the domain name.

40 It remains to be seen how registries and registrars will apply the new obligations embodied in the RA and RAA and how closely ICANN will control their implementation. But the absence of measures to safeguard registrants' freedom of expression gives cause for concern that the DNS could be used as a tool to censor online content. ICANN has disavowed this worrying interpretation of the new contract terms. As articulated by A. Grogan (ICANN's Chief Compliance Officer), "though the appropriate interpretation of 2013 RAA is the subject of debate, there are clear-cut boundaries between ICANN enforcing its contracts and the enforcement of laws and regulations" by existing institutions like law enforcement authorities, regulatory agencies and the judicial systems. He added that "a blanket rule requiring suspension of any domain name alleged to be involved in illegal activity goes beyond ICANN's remit and would inevitably put ICANN in the position of interpreting and enforcing laws regulating website content. At worst, it would put ICANN squarely in the position of censoring, or requiring others to censor, Internet content".[144] The CEO of ICANN reiterated this strong statement at the 54th General Meeting of ICANN in October 2015.[145] However, the issue is far from going away, as intellectual property groups are still demanding an active cooperation from registrars and registries against illegal online activities. Moreover, ICANN is not in a comfortable position. As pointed out by D. Post, one may wonder about the purpose of inserting these new provisions into the standard agreements if ICANN had no intention of enforcing them.[146] Additionally, these uncertainties could lead to registries and registrars adopting voluntary practices to rapidly suspend domain names that are allegedly being used for unlawful or abusive purposes.[147]

E. Conclusion

41 The New gTLD Program is both a tremendous tool to expand the Internet and a vehicle to set alarming precedents with regard to freedom of expression online. Throughout this paper, my aim has been to show that this program will not only revolutionize the DNS but also formalize the role of domain name registries and registrars as points of control for the content posted under all new gTLDs. The New gTLD Program, which aimed at fostering competition and diversity in the DNS, carries threats of censorship at two levels. First, regarding the top level of the domain, passionate discussions took place regarding the strings of characters that could be delegated as new gTLDs and upon which grounds applicants' freedom of expression could be restricted. Obviously it was not the gTLD *per se* that was targeted by this policy, but the potentially offensive or controversial content that might be published under the new identifiers. Therefore, proposed registration policies were paramount to the determinations of experts appointed by the International Chamber of Commerce. Second and more worryingly, as a result of governmental pressures, registries and registrars are now designated points of contact for dealing with alleged abuse committed in the domain they administer. They are expected to take appropriate measures to respond to reports of abuse and may suspend domain names of websites proposing allegedly illegal content. No process has been put in place to ensure due consideration of the registrants' freedom of expression.

42 Now that the application process for new gTLDs is coming to an end, one should keep an eye on two future developments. First, it will be interesting to follow the compliance of new gTLDs registries with their Public Interest Commitments and the willingness of ICANN to impose remedies on recalcitrant registries and registrars. Second, with regard to "old gTLDs" introduced in the 1980s and during the two rounds of expansion in 2000 and 2004, it will be crucial to follow if the new obligations, particularly the new Specification 11, will apply to them when they will renew their Registry Agreement. Particular attention should be paid to the Registry

143 Section 2.8 of the Base Registry Agreement; Section 3.18 of 2013 Registrar Accreditation.

144 A. Grogan, 'ICANN is not the Internet Content Police', 12 June 2015, <http://www.icann.org/news/blog/icann-is-not-the-internet-content-police>.

145 ICANN, 54th General Meeting in Dublin, Welcome Ceremony & President's Opening Session, 19 October 2015, transcript available from <http://meetings.icann.org/en/dublin54/schedule/mon-welcome/transcript-welcome-19oct15-en>, pp. 29 and seq.

146 D.G. Post, 'Internet Infrastructure and IP Censorship' (2015) *IP Justice Journal*, <http://www.ipjustice.org/digital-rights/internet-infrastructure-and-ip-censorship-by-david-post>.

147 Electronic Frontier Foundation, 'Voluntary Practices and Rights Protection Mechanisms: Whitewashing Censorship at ICANN' (21 October 2015), <http://www.eff.org/deeplinks/2015/10/voluntary-practices-and-rights-protection-mechanisms-whitewashing-censorship-icann>.

Agreement between ICANN and Verisign for *.com*, which is set to expire on 30th November 2024[148].

* *Caroline Bricteux* is a PhD researcher in law at the Perelman Centre for Legal Philosophy, Université libre de Bruxelles. The author warmly thanks the organizers of and all participants in the Third Netherlands Institute for Law and Governance PhD Forum *Law and Governance in the Digital Era* (VU Amsterdam, 20 November 2015), where an earlier version of this work was presented.

148 The current version of the .com RA was initially set to expire on 30 November 2018. In October 2016, the term of the contract was extended to 30 November 2024 to coincide with the term of the Root Zone Maintainer Services Agreement concluded in September 2016 between ICANN and Verisign to transition the NTIA's administrative role regarding root zone management (First Amendment to *.com* Registry Agreement, 20 October 2016, <http://www.icann.org/sites/default/files/tlds/com/com-amend-1-pdf-20oct16-en.pdf>). The amendment was a simple extension of the term of the *.com* RA and did not include the new standard clauses of the New gTLDs RA. Several commenters criticized the absence of the new safeguards and protection mechanisms. Taking note of these comments, the ICANN Board indicated that the amendment includes a provision that commits the parties to cooperate and negotiate in good faith to amend the *.com* RA by the second anniversary date of the amendment in order to preserve and enhance the security of the Internet or the TLD. According to the Board, this language was negotiated to provide an opportunity for longer term discussions and additional community input that may be needed to discuss potential changes to the *.com* RA, such as moving to the form of the New gTLDs RA (ICANN, Regular Meeting of the Board, Resolution 2016.09.15.09, 15 September 2016, <http://www.icann.org/resources/board-material/resolutions-2016-09-15-en>).

An Innovative Legal Approach to Regulating Digital Content Contracts in the EU

by **Joshua M Warburton***

Abstract: Unifying laws between States to better facilitate cross-border transactions is not a new concept. Within the EU, such unification has generally been achieved by harmonising Directives and Regulations. However, legislative techniques to govern digital content transactions are still in their infancy; it is likely that any harmonising instrument would be based upon pre-existing legislation that could be refined to better serve its purpose. States themselves would likely attempt to formulate innovative legislative proposals to give contracts formulated under their jurisdiction a competitive advantage. But, once harmonization occurs, attempts to innovate in contract law for individual gain would cease. Analysing the functionality of mutual learning legislative exercises can lead to the conclusion that allowing experimentation, whilst establishing a separate unified optional framework, may well be the most practical way to continue to develop more efficient contractual rules and obligations, that may eventually be proliferated throughout transnational markets. Separating the legislative efforts between national law and an optional law that governs cross-border contracts, overseen by a centralized body attempting to collate the most beneficial aspects of digital content legislation across the breadth of the EU, would be a more progressive system of digital content contract regulation.

Keywords: Optional Instrument; Digital Content; Harmonisation; E-Commerce; Mutual Learning; Jurisdictional Competition

Recommended citation: Joshua M Warburton, An Innovative Legal Approach to Regulating Digital Content Contracts in the EU, 7 (2016) JIPITEC 246 para 1.

A. Introduction

1 The expansion of cross-border trade of digital content is an unequivocal imperative for the European Commission. However, bringing uniformity across Member States' legislative outputs is no simple task. In a market with constantly evolving technology, it is difficult to legislate adequately without constant adaptation and innovation in the legal fields. As can be demonstrated by investigating mutual learning methods, the "knowledge problem" lends credence to the idea that the best form of regulation is yet to be discovered, and, therefore, transnational jurisdictional competition should be encouraged in order to discern the more favorable legislative techniques and policies to cover digital content transactions. The unfortunate ramification of this is that, whilst this development is occurring, there would be little in the form of legislation to encourage cross-border sales. The Draft Digital Content Directive[1] could fulfil some of the need for legislation, but it is too narrow and restrictive. In this paper it is suggested that a reformulation of the currently retracted[2] Common European Sales Law (CESL)[3] as a digital optional instrument would serve to allow both legal development and mutual learning, whilst creating a parallel system that allows uniformity in cross-border digital transactions.

1 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM(2015) 634(final).

2 European Commission 'Commission Work Programme 2015 – A New Start' (Communication) COM(2014) 910 final Annex 2, item 60.

3 European Commission, 'Proposal for a regulation of the European Parliament and of the Council on a Common European Sales Law (CESL)', COM (2011) 635 final.

2 The view portrayed in this paper is that lessons can be learned from the 'Open Method of Coordination' utilized in the European Union (EU) and the Uniform Commercial Code in the United States of America (USA), as both demonstrate the issues of centralized organizations in mutual learning legislative exercises. The argument is that once harmonization occurs, the experimentation - by necessity - must cease, therefore stifling legal innovation. In such a rapidly developing area as e-commerce, this cannot be a beneficial thing, as many rules in traditional consumer legislation are not applicable for the vast majority of digital content sales. Separating the legislative efforts between national law and an optional law that governs cross-border contracts, overseen by a centralized body attempting to collate the most beneficial aspects of digital content legislation across the breadth of the EU, would be a more progressive system of e-commerce regulation.

B. The Alternatives to the Optional Instrument

3 In light of the Digital Single Market Strategy in May 2015,[4] the EU faces a potential issue from the implementation of the proposed Draft Digital Content Directive.[5] The Directive itself is intended to be a "targeted maximum harmonisation" instrument that would mean that "once in force Member States cannot retain or introduce more consumer-friendly rules within its scope".[6] The issue with this is that the protections introduced by the Draft Directive are vague given the complexities and nuances of the myriad types of digital content types already available. This will only be exacerbated as new digital content types emerge and evolve. The protections needed will naturally shift as technology evolves, and legislative output needs to reflect that. The Draft Directive will not allow a sufficient degree of flexibility for states to adapt, and thus it is contestable that the Directive should either be reconsidered, or allow other legislation to work alongside it.

4 It is argued in this paper that in order to encourage legal innovation and to disincentivize behaviors detrimental to other states, an optional instrument is preferable. In order to make this argument, decentralized and centralized versions of mutual learning methods shall be examined, with the exemplifying versions of such being trans-jurisdictional competition and the Open Method of Coordination (hereinafter: OMC) respectively. As the American Uniform Commercial Code (UCC) system has a great deal in common with the latter, and some common ideals shared with the former, the Code shall then be discussed in some detail. The construction of the UCC acts as a useful exemplar of the amalgamation of both methods and illustrates some key practicalities of any optional instrument. These examinations shall be formulated into insights that are relevant to a restructuring of the CESL as this is the current form an optional instrument in consumer sales law would likely take.[7] A discussion as to whether elements of these methods should be utilized by future unifying instruments is also included.

C. Trans-Jurisdictional Competition and Pure Yardstick methods

5 First, it is prudent to understand what trans-jurisdictional[8] competition entails. The reference is usually made to the manner by which individual jurisdictions attempt to make their legal system more appealing, and thus attract more transnational trade, by providing simpler and more beneficial legislation for traders, or to attract more companies to establish themselves within the State.[9] Constant improvement to Member State jurisdiction with the aim of being more favorable than their counterparts, works in much the same way as competition between companies in free markets, and, in theory, creates an internal market that constantly improves. Successful trans-jurisdictional competition often leads to legal transposition of the best methods of jurisdiction, but it can be difficult to qualify the success of such methods as it is a decentralized system. A centralized system is easier to assess qualitatively, but it is likely that the competitive elements diminish in such a system. Thus, the current functioning of these two methods within the EU is worthy of appraisal.

6 The lauded European Economic and Monetary Union

4 European Commission 'Priority: Digital Single Market' (*Europa*, 21 September 2016) <http://ec.europa.eu/priorities/digital-single-market_en> accessed 21 September 2016.

5 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM(2015) 634(final).

6 Mánko Rafal, 'Contracts for Supply of Digital Content: A Legal Analysis of the Commission's Proposal for a New Directive (2016) EPRS In-depth analysis, PE 582.048.

7 It should be noted that the CESL was withdrawn to unleash the power of e-commerce, which suggests some intention to review it. Should it be reformulated, it is the opinion of this author that lessons taken from these comparable measures should be observed.

8 Sometimes referred to as 'traditional jurisdictional competition'.

9 This is a somewhat more simplistic definition of the theory. For a more complete discussion of the terminology, see William Bratton and Joseph McCahery 'The New Economics of Jurisdictional Competition: Devolutionary Federalism in a Second-Best World' (1997) Faculty Scholarship.Paper 849.

(EMU)[10] - designed to assist in the convergence of EU economies - has unintentionally paved the way for a form of mutual learning. The EMU led to the introduction of the European Employment Strategy[11] and then to the creation of the Open Method of Coordination (OMC).[12] The OMC was formed as a new type of governance with the aim of reforming policies throughout Member States via the use of soft law, intended to encourage the adoption of the best policies within the EU to foster a stronger economic policy base.[13] Although the OMC is a centralized benchmarking system, it is a particularly useful method of jurisdictional competition,[14] without the caveat of being as lax in political persuasion as a method such as *laboratory federalism*,[15] which is an entirely decentralized version of such a method. The intention here is to assess the value of decentralized trans-jurisdictional competition and centralized mutual learning on the basis that the continued development of legislative techniques is beneficial to the market as a whole. The value of such ideas in a general sense is not discussed here, as that is an issue for pure economic theory to address.[16]

7 Three forms of mutual learning through competition exist,[17] and it is important to understand how each affects the legislature. The first method is that of *pure yardstick competition*, a method by which two states observe the policy decisions - and their consequences - with another state; this is best described as a pure mutual learning exercise as there is little competitive element implied here. *Trans-jurisdictional competition* is that where legislative efforts and policy making are continually adapted in the face of market circumstances where it is clear that some jurisdictions have more favorable laws for trading.[18] Finally, *regulatory competition*[19] is the type of laboratory federalism that would be most prevalent should an optional instrument arise; being that it is when those governed by law may choose which regulatory system they are to be governed by due to a free choice of law.

8 The OMC is used here as an example of a centralized legal and policy dissemination technique, most reminiscent of *pure yardstick competition*. Although the OMC is a policy based instrument concerned with culture, it accurately portrays how the EU has become involved with mutual learning and self-coordination in the proliferation of laws;[20] it is particularly useful in demonstrating how such methods are unsuitable in regards to consumer contract law. The OMC is notably different from traditional ideas of harmonization, in that policy making is conducted at a national level. Policies in Member States are evaluated at the central level by the OMC, and the very best policies are identified and potentially spread via policy recommendations. The OMC ensures that experts from various ministries meet frequently to create policy manuals to be spread throughout the EU. The instrument is primarily used to build consensus on issues and increase understanding of commonalities - there is no intention of creating binding harmonizing instruments. The Commission oversees the functioning of the OMC to a very minimal extent, instead relying on national governments to monitor their own input. The production of reports on the progress made by the OMC is carried out by the Commission,[21] which otherwise has little involvement. External evaluation is of the opinion that the "OMC generally functioned well and was relevant to the policy objectives in the Work Plan for Culture. The evaluators pointed out that the OMC adds value primarily through mutual learning and the exchange of best practices".[22]

10 'Economic and Monetary Union' (*European Central Bank*, 2015) <http://www.ecb.europa.eu/ecb/history/emu/html/index.en.html> accessed 4 July 2015.

11 'European Employment Strategy' (*European Commission*) <http://ec.europa.eu/social/main.jsp?catId=101&langId=en> accessed 4 July 2015.

12 Open Method of Coordination. See 'European cooperation: The Open Method of Coordination' (*European Commission*) <http://ec.europa.eu/culture/policy/strategic-framework/european-coop_en.htm> accessed 4 July 2015.

13 Wolfgang Kerber and Martina Eckardt 'Policy Learning in Europe: The "Open Method of Coordination and Laboratory Federalism' [2007] 14(2) Journal of European Public Policy, 227.

14 Adrienne Héritier 'New Modes of Governance in Europe: Policy-Making without Legislating' in Adrienne Héritier *Common Goods: Reinventing European and International Governance* (1st edition, Rowman & Littlefield Publishers, 2002), 5.

15 Wallace Oates, 'An Essay on Fiscal Federalism' [1999] 37(3) J Econ Literature, 1120.

16 For a discussion on the general value of these ideas see Wolfgang Kerber and Martina Eckardt 'Policy Learning in Europe: The "Open Method of Coordination and Laboratory Federalism' [2007] 14(2) Journal of European Public Policy, 227.

17 Wolfgang Kerber and Martina Eckardt 'Policy Learning in Europe: The "Open Method of Coordination and Laboratory Federalism' [2007] 14(2) Journal of European Public Policy, 227, 232.

18 Or similar economic venture.

19 Damien Geradin, Daniel Etsy, *Regulatory Competition and Economic Integration: Comparative Perspectives* (*International Economic Law Series*) (Oxford University Press, Oxford, 2001).

20 GOVECOR 'EU governance by self-coordination? Towards a collective "gouvernement économique"' (August 2004, European Commission). <http://cordis.europa.eu/documents/documentlibrary/100124131EN6.pdf> last accessed 3 August 2015.

21 European Commission 'Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the implementation and relevance of the Work Plan for Culture 2011-2014' COM 2014 0535 final.

22 Quote from - Open Method of Coordination. See 'European cooperation: The Open Method of Coordination' (*European Commission*) <http://ec.europa.eu/culture/policy/strategic-

9 To understand the impact of the OMC as a centralized mutual learning exercise, one must look at the effect of a system devoid of centralization. As previously mentioned, *Laboratory federalism* encompasses a few similar definitions. For the purposes of this research, it is viewed as the diffusion of public policies on the basis of innovation and effectiveness as the key aspect of jurisdictional competition - essentially being trans-jurisdictional competition with a focus on mutual learning rather than the improved economic yield of any one Member State.[23] The theory is that within a unified system of States,[24] the individual States will develop and experiment with different policy ideas, the best of which will proliferate the market. The primary goal is to overcome the concept known as the "*knowledge problem*",[25] which states that, in the majority of fields, the optimal policy has not yet been found, resulting in a suboptimal proliferation of legislation. Many of the ideas of jurisdictional competition and laboratory federalism come from the work of Friedrich Hayek and the concept of competition as a discovery procedure,[26] but the conclusions drawn by Hayek are that people are ultimately limited in their ability to intervene in complex societies, thus ensuring that the best policies and legislative techniques may well never be discovered.

10 Both the OMC and laboratory federalism are faced with the common problem of whether it is possible to assess the benefit of others' experience. A solution applied out of context may be actively detrimental. The idea of a singular method being optimal in all situations is demonstrably incorrect, yet this is of course, no indicator that there is nothing to be gained from the exercise. The crucial role of either method is to ascertain better methods for jurisdictions and specific circumstances, as this leads to greater economic efficiency and, therefore, justifies their existence. This difficulty in utilizing information gathered by others is well documented in the economic literature;[27] the diffusion of ideas is difficult, uncertain and lengthy. Even if positive lessons are consistently difficult to apply, it is easier to assess ideas that should not be diffused, with unsuccessful legislation being less likely to find application in other jurisdictions.[28] Regardless of the positive or negative diffusion of ideas, the result is the same, an attempt to unify jurisdictions with the supposed optimal legislative techniques - irrespective of whether the techniques in question have been adequately judged. The potential for non-optimal legislation to be proliferated throughout the EU is in that respect of little difference to harmonization attempts, so long as it appears beneficial politically and creates a uniform market.

11 Whether the OMC has been effective is contestable, yet it appears as though the consensus is somewhat negative. The issue is that in order for the OMC to be effective, it needs to function properly at both the data collection stage (national) and the EU level, and it appears that the data collection stage is not functioning adequately.[29] Furthermore, the incentives to implement the best practices seem to lack in efficacy.[30] Lessons from the European Employment Strategy (EES) show that, without soft sanctions, parties involved with the implementation of these policies show little desire to do so.[31] Laboratory federalism, however, does not depend on multi-national cooperation, so the difficulties in maintaining functionality on different levels are moot in this regard. Yet in the face of this, such a method of mutual learning is near impossible to evaluate, and, in particular, seeks only to improve the economic position of the individual State, rather than the functioning of the larger body. For that reason, the EU would not seek to rely on laboratory federalism to yield positive results for the internal market; a centralized body is required to ensure that the policies suggested are beneficial for all. This should not be taken as a dismissal of trans-jurisdictional competition, however, as there are significant benefits that are not present in

framework/european-coop_en.htm> accessed 4 July 2015, original text to which it makes reference is currently unavailable.

23 Viktor Vanberg, Wolfgang Kerber, 'Institutional Competition among Jurisdictions: An Evolutionary Approach' [1994] 5(2) Constitutional Political Economy, 193.

24 It should be noted that the theory discusses the idea of a true federal system, whereas the EU is most likely a quasi-federal entity, for a view that it is entirely a federal jurisdiction see Alain Marciano and Jean-Michel Josselin 'How the court made a federation of the EU' [2006] 2(1) The Review of International Organizations 59, but this paper does not share that view, only that the theory of laboratory federalism is applicable to the EU.

25 Wolfgang Kerber and Martina Eckardt 'Policy Learning in Europe: The "Open Method of Coordination and Laboratory Federalism' [2007] 14(2) Journal of European Public Policy, 227, 232.

26 F.A. Hayek *Studies in Philosophy, Politics and Economics*, (New edition, University of Chicago, 1980) 66.

27 Everett Rogers, *Diffusion of Innovations*, (5th revised ed., Simon and Schuster International, 2003).

28 Richard Rose, 'When all other Conditions are not Equal: The Context of Drawing Lessons', in Catherine Jones Finer (ed.), *Social Policy Reform in Socialist Market China: Lessons for and from Abroad*, (Ashgate Pub Ltd, 2003).

29 Caroline de la Porte, and Patrizia Nanz, 'The OMC – A Deliberative-democratic mode of governance? The Cases of Employment and Pensions' [2004] 11(2) Journal of European Public Policy, 267, 278.

30 James Arrowsmith, Keith Sisson and Paul Marginson, 'What can 'Benchmarking' Offer the Open Method of Coordination?', [2004] 11(2) Journal of European Public Policy, 311.

31 Wolfgang Kerber and Martina Eckardt, 'Policy Learning in Europe: The "Open Method of Coordination and Laboratory Federalism' [2007] 14(2) Journal of European Public Policy, 227, 237.

harmonized markets. Most notably, under this type of competitive legislative effort, innovation and progressive policies thrive, bringing about a swifter end to the "knowledge problem". This is particularly beneficial to emerging contract types, such as those involving digital content, as the legislation needs to adapt quickly in order to address new challenges. No other mutual learning method is as quick and efficient as trans-jurisdictional competition; but the issue is that it simply does not create uniformity, which is central to fundamental objectives of the EU.

12 With trans-jurisdictional competition judged as too independently minded, the question is then raised: why, beyond issues of current ineffectiveness, should the centralized OMC method be dismissed? It has been established that the knowledge problem illustrates that the best legal method is likely not discovered, and it is also clear that the development of technology and social progress continually alters what the best method would be. For these reasons, jurisdictions must be responsible for their own legal innovation in order to respond adequately to issues promptly.[32] However, if the OMC proliferated the best innovations to other Member States, this would surely result in consistently adequate protection for consumers and traders, on the condition that the Member States were responsive to such non-binding recommendations.[33] However, the manner of the functioning of the OMC does not encourage the introduction of innovative legal and policy methods, merely the proliferation of perceived successful existing versions of such. This is an issue shared by any benchmarking method of harmonization.[34] Therefore, the OMC is useful in attempts to bring heterogeneity to issues under the exclusive jurisdictions of Member States. However, as a non-binding source of law, which crucially offers no incentive for innovation, it is clearly not ideal as a method to legislate for rapidly developing technology types, and is unlikely to become such without external influence.

13 The conclusion to be drawn here is that transnational jurisdictional competition will not lead to convergence towards a single market, but will encourage innovative legislative methods. Pure yardstick competition based on mutual learning (such as the OMC) will suffer from a lack of innovation as increasingly fewer benefits result from such endeavors, particularly considering the economic risks of modifying policies; yet it will assist with the convergence of the market. A halfway point is possible, as the USA has demonstrated with the Uniform Commercial Code or UCC. The Code is created by a centralized body, and then disseminated to the States who choose whether and which parts to adopt, therefore allowing a State to continue to innovate in regards to legislation, whilst the Code still, *theoretically*, ensures that the best ideas proliferate the market as the centralized organization acts as an external examiner of policies in order to benchmark them. However, whether the two mutual learning techniques function well together is an issue worthy of discussion.

D. The American Experience

14 The EU is not alone in trying to create a single market in unified, yet legally distinct, territories. The systems of market integration in the USA is a useful example as it demonstrates a functioning internal market achieved through optional unification.[35] The USA has drawn interest from scholars in the past for its relevance towards system building within the EU.[36] It has been claimed that it works because the States have different Private Laws but the Federation as a whole provides at least a common legal system[37] (albeit with the exception of Louisiana which has a civil legal system) and a shared legal training method.[38] Legal fragmentation is at a much lower point than in the EU for this reason.[39] This is not to say that the laws of the USA should be transposed into the European legal system; but rather that interpretation of historical data from the federalist system may yield information as to what conditions are conducive to trade within an internal market, particularly given its relevance to mutual

32 GOVECOR 'EU governance by self-coordination? Towards a collective "gouvernement économique"' (*European Commission*, August 2004). <http://cordis.europa.eu/documents/documentlibrary/100124131EN6.pdf> last accessed 3 August 2015.

33 Kerstin Jacobsson, 'Soft Regulation and the Subtle Transformation of States. The Case of EU Employment Policy', [2004] 14 Journal of European Social Policy, 355, 366.

34 James Arrowsmith, Keith Sisson and Paul Marginson, 'What can 'Benchmarking' Offer the Open Method of Coordination?', [2004] 11(2) Journal of European Public Policy, 311.

35 David Leebron, "Claims for harmonization: A theoretical framework", [1996] 27 Canadian Business Law Journal, discusses harmonization from a Canadian viewpoint, however America is more useful as it is a larger economy.

36 Eric Stein, Terence Sandalow, 'On the Two Systems: An Overview' in Eric Stein and Terence Sandalow (eds) *Courts and Free Markets: Bk 2: Perspectives From the United States* (Oxford, Oxford University Press, 1982) 3.

37 Hein Kötz 'Contract Law in Europe and the United States: Legal Unification in the Civil Law and the Common Law' [2012] 27 Tulane European and Civil Law Forum, 1.

38 G. Edward White, *Law in American History: Volume 1* (Oxford University Press, 2012).

39 For a more detailed look at the fragmentation of Europe, see Stefan Vogenauer and Stephen Weatherill, *The European Community's Competence to Pursue the Harmonisation of Contract Law – an empirical contribution to the debate* in *The Harmonisation of European Contract Law* (Oxford, Hart Publishing, 2006) 105.

learning methods. The American method was a primary influence upon the formation of the Vienna Convention on Contracts for the International Sale of Goods (CISG). The fact that the CISG was a primary focus of the Lando Commission in their goal of creating a singular European private law system is an indication of the significance that the American system holds upon global commercial legislation. The CISG, however, is not relevant to this paper as it explicitly excludes consumer transactions from its applicability,[40] making it more prudent to examine its predecessor's commercial law system.

15 The USA comprises of individual States that have their own contract, tort, unjust enrichment, property, family and succession law. Though theoretically possible, uniform federal law has not attempted to legislate to create a singular system in any of these fields. Argument may be made that this is primarily due to issues regarding competency, in that the US Constitution restricts the ability of Congress to legislate in this manner by stating that: "Powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people".[41] However, this is not the exhaustive rationale, as in some areas, power has been delegated to the US central government by the Constitution, meaning Congress has the competence to act but remains inactive. This is particularly true in regards to interstate commerce, which Congress has competency to act upon by virtue of Article 1(8)(3) of the Constitution, wherein they are granted the power to legislate on commerce affecting multiple states, foreign nations or Indian tribes. This is different from the EU, wherein Member States retain their sovereignty and are competent and responsible for their foreign policies.[42] However, the competencies to regulate the internal market are separate and shared with the EU as in Arts.3-4 of the TFEU.[43] The Common Commercial Policy, on the other hand, is under the exclusive competence of the EU.

16 In the USA, the National Conference of Commissioners on Uniform State Law (hereinafter: NCCUSL) has attempted to bring uniformity. The NCCUSL is in many respects similar to the aforementioned OMC, in that they examine the laws of states, and suggest what they deem to be the best policies for adoption. In its current form, from its inception in 1892 to the present, the Conference has constructed over three hundred Acts designed to bring uniformity to States that wish to adopt them. Only a small number of these have been implemented.[44] The Uniform Commercial Code (UCC) is the piece that has been the most influential since the creation of the Conference. The Code, introduced in 1952 after a ten-year drafting period in conjunction with the American Law Institute (hereinafter: ALI), covers the Sales of Goods and many other aspects of private law. Although it falls short of being a complete Commercial Code, remaining silent on a number of Commercial issues, it is wider in scope than the former CESL. The uniformity this Code brings is beneficial but is hampered by the fact that the States are entitled to amend the Code should they so wish. The importance of the Code to the system of the USA is not to be understated as it covers transactions cumulatively worth trillions of dollars.[45]

E. The UCC in Context

17 Throughout its tenure, considerable criticism has been levied against the Code, particularly in regards to Art. 2,[46] which is important for the analysis in this paper. "Where the practitioners wanted problems answered in the statute, the draftsmen were content to leave answers to the judicial process".[47] Perhaps the greatest sustained criticism to the UCC in this respect is in relation to its approach to warranties under contract. All States have supplemented Art. 2 to an extent in order to increase consumer confidence, but these actions were seen by some academics as otiose in nature.[48] Only Maine,[49] Connecticut[50] and Maryland[51] made significant impact in that they prohibit the use of clauses that either remove implied warranties or limit remedies for breach of warranty. However, this clearly demonstrates the need for a strong base level of protection for consumers in any form of unifying instrument.

40 CISG Art 2 (a).

41 U.S. Constitution 10th amendment.

42 Catherine Banyard, Steve Peers *European Union Law* (1st edition, Oxford University Press, 2014), 3.

43 Jukka Snell 'Who's Got the Power? Free Movement and Allocation of Competences in EC Law' [2003] 22 Yearbook of European Law 323.

44 NCCUSL 'Home page' <http://uniformlaws.org/> accessed 4 May 2015.

45 The 2007 economic census estimated the value at approx. $3,917,663,456,000 for retail sales alone. 'QuickFacts United States' (United States Census Bureau, 5 August 2015) <http://quickfacts.census.gov/qfd/states/00000.html> last accessed 15/08/15.

46 Carol Swanson, 'Unconscionable Quandary: UCC Article 2 and the Unconscionability Doctrine', [2001] 31 N.M. L. REV., 359.

47 Homer Kripke, 'The Principles Underlying the Drafting of the Uniform Commercial Code' [1962] University of Illinois Law Forum, 321, 332.

48 Joan Vogel, 'Squeezing Consumers: Lemon Laws, Consumer Warranties, and a Proposal For Reform', [1985] Ariz. St. L.J. 589.

49 § 2-316.

50 § 42a-2-316.

51 § 2-316.1.

18 Proposed amendments to the Code are also difficult to implement as States will often refuse them, such as the amendments to Art. 2 proposed by the NCCUSL in 2003, which were refused by all States. The importance of the Uniform Computer Information Transactions Act (UCITA) is that it was designed to deal with intangible products and licenses, which the Code was ill-formed to deal with. The aforementioned Act has not been well received, only being adopted by Maryland and Virginia, whilst being actively condemned by IT groups.[52] The Act is easily overwritten by a shrink wrap license, yet free software distributors and small software developers with limited legal knowledge would be found liable for faults within the software. This is important to any model legislation in that the addition of important modifications are difficult to implement without significant political lobbying, which costs time and money that most supranational organizations could find better uses for, and may be ultimately fruitless.

19 Additions and amendments have consistently been an issue for the UCC, particularly those concerning consumers. Art. 2 in particular, has been difficult to amend since its inception as the Committee, especially Spiedel,[53] have been aware of.[54] The first reason was that no relevant group of consumers or merchants were asking for a revision of Art. 2; with no demand for the revision, change was unlikely to be welcome. Secondly, some of the amendments in the 1999 drafts were so controversial that the Article appeared unfamiliar. Third, the removal of computer data from the scope of the Article did nothing to remove the controversy about computer data. Fourth, the consumer protection provisions consistently attracted the ire of commercial interests.[55] Finally, and perhaps most importantly, the political aspect was too important in the drafting of the revisions; any revision needed to appeal to State legislatures, who would be lobbied by commercial interests.[56] Too much consumer protection would be politically untenable whereas too little would be almost useless.

20 This issue of the difficulty of making amendments is a key argument against any instrument that relies upon soft law methods to implement changes to the legislation. Much like the *pure yardstick competition* type instrument of the OMC, there is little incentive for States to implement any of the proposed changes unless it brings about an obvious economic advantage over the previous system, and if consumers remain unaware of the areas to which they lack protection due to the advances in technology, there would be no increased trade due to consumer confidence brought about by any changes. Furthermore, it is obvious from the historical aspects of the UCC that these amendments are too time consuming to formulate, but even more so to implement, as the large number of States that must be persuaded to adopt the instrument present far more of a challenge than the more autonomous *trans-jurisdictional competition* method would require.

F. No Need for Digital Legislation?

21 The release of the *Principles*[57] in 2010 gave an impression regarding the issues deemed to be facing US consumers in relation to digital content transactions. The surprising element was that the text addressed very few legal problems that were specific to software transactions, and this is deemed to have been intentional due largely to the strength of the (predominantly) common law system.[58] Of course, the EU is not solely made up of Common Law jurisdictions. It is perhaps an incontrovertible truth that there is little software contract specific case law available in the USA, or the EU for that matter, which will lead some academics to suggest that this confirms the strength of the current system.[59] However, that is not the only conclusion that may be drawn, as an overwhelming majority of digital software that is faulty is of so little value outside of opportunity cost that the majority of claims would be brought about under the relevant small claims procedure.[60] As such, this means that the majority of cases involving digital content would go unreported, and whereas judges may simply be able to apply existing sales law or the relevant parts of the draft

52 Dorte Toft 'Opponents blast proposed U.S. software law' (CNN July 2 1999) <http://www.cnn.com/TECH/computing/9907/12/ucita.idg/index.html>, last accessed 6 May 2015 and Richard Stallman, 'Why we must fight UCITA' (GNU, February 28, 2013) <http://www.gnu.org/philosophy/ucita.html> last accessed 6 May 2014.

53 Chief reporter for the Committee.

54 Richard Spiedel, 'Introduction to Symposium on Proposed Revised Article 2', [2001] 54 SMU L. Rev., 787.

55 For a discussion on the impact of such groups upon Art 2(B) see Bruce Kobayashi, Larry Ribstein 'Uniformity, Choice of Law and Software Sales' [2000] George Mason Law and Economics Paper No. 00-07, 16.

56 Edward Rubin, 'Thinking Like a Lawyer, Acting Like a Lobbyist: Some Notes on the Process of Revising UCC Articles 3 and 4', [1993] 26 Loy. L.A. L. REV. 743, 759.

57 American Law Institute, 'Principles of the Law of Software Contracts' (2010) (ALI PRINCIPLES).

58 Juliet M. Moringiello, William L. Reynolds, 'What's Software got to do with it? The ALI Principles of the Law of Software Contracting', Widener Law School Legal Studies Research Paper Series no. 10-02, 12.

59 *Ibid* specifically '*... there were few serious legal issues for the project to address. We know that because there has been little litigation over software-specific issues*'.

60 In Europe this would be under Regulation (EC) No 861/2007 of the European Parliament and of the Council of 11 July 2007 Establishing a European Small Claims Procedure OJ L 199/1.

Directives[61] to beneficial effect, it does not mean that the rationale is applied correctly, consistently or adequately. With the value of digital content likely to continue to rise, it would be naïve to assume that little case law means that prior law is suitable.

22 This argument of prior law being fit for purpose has frequently been raised in respect to the software regulation in the USA, particularly the unpopular Art. 2B that relied heavily on supposed pre-existing law in regard to license agreements.[62] In fact, even the ALI's *Principles* intended to not to go so far as a restatement of laws, but merely intended to be guidance for courts to consider. The *Principles* do make some bold assertions, such as that federal intellectual property law should harmonize contrary State law.[63] However critically, the *Principles* are very different from EU harmonization methods because of the reliance upon the unconscionability doctrine[64] to ensure fairness, rather than on extensive - and potentially exhaustive - lists of unfair contract terms. This ensures the flexibility of the principles, but, flexibility comes at the cost of certainty. Most strikingly, the *Principles* are not binding in any way, as legislation typically is. It is stated that: "Courts can apply the Principles as definitive rules, as a 'gloss' on the common law, U.C.C. Article 2, or other statutes, or not at all, as they see fit",[65] which is, at best, a wholly non-committal assertion of authority, making the variation in State law regarding software a foregone conclusion. Yet, despite the failure of Art. 2B, UCITA and the arguable failure of the *Principles*, the growth of the digital market in the USA appears unimpeded,[66] as the variation in State law appears to not be concerning consumers.

23 A conclusion can be drawn that soft law and the extension of ideas present in sale of goods and services contracts may be extended successfully to digital content. Nevertheless, as precedence diverges from the wording of the UCC, and the re-evaluation of ideas occurs in cases such as in *Bowers v. Baystate Techs., Inc.*,[67] the actual uniformity between States decreases. The USA's commercial system, will however be far more resilient to such a decrease, as the idea of the perception of uniformity will encourage consumers to treat other States' laws as though they were the same as their own.[68] Resilience is not equal to immunity, and various legal organizations in America seem to be aware of this, hence the repeated attempted revision to unified digital content regulation. If the *Principles* can gain traction in being consistently implemented by States, then they may become a strong and adaptable instrument, but like the UCC before it, it is likely that States will not implement all changes in a uniform fashion. Digital legislation is required, and it would be more beneficial to be in some ways binding, rather than the measures of the *Principles*, UCC or OMC.

G. The Relevance to Optional Law in the EU

24 There are obvious concerns as to why the method of legislating by means of an optional Code (such as the UCC), or by means of a mutual learning instrument such as the OMC on commercial transactions, would not be appropriate for EU consumer law. If a future digital optional instrument for consumers were neither a Directive nor a Regulation, but merely a piece of model legislation that States could adopt and adapt to suit the needs of their consumers, the likelihood of Member States adopting such legislation without significant alteration would be negligible. The system of the USA was politically viable because the nation has always maintained a strong sense of unified identity, meaning that national federal measures are not dealt with the amount of skepticism as supranational measures in the EU. The implementation in the USA has been the cause of the majority of issues with the UCC, as the political nature resulted in the difficulty of establishing UCITA. The lesson to be taken from this is that any potential future digital optional instrument for consumers must take the form of a Regulation, and modifications made should be made at a supranational level. It is preferable that amendments be either adopted by all Member States, or none at all, as this avoids the fragmentation that is present in the US system. In order to do so, amendments must be adopted in the Council as it is acknowledged that timely solutions to minor issues are somewhat impractical at a supranational level.

25 Fragmentation of the law is not the only issue that the drafters of any future optional instrument need

61 The Draft Digital Content Directive in particular.

62 'The law that is already out there' is a key theme in articles such as Jessica Litman 'The Tales that Article 2B Tells', [1998] Berkeley Tech. L.J. 13, 931, 934 and Hannibal Travis, 'The Principles of the Law of Software Contracts: At Odds with Copyright, Consumers, and European Law?' [2010] FIU Legal Studies Research Paper Series Research Paper No. 10 – 01, 3 though it should be noted that neither of these papers agreed that the law already existed.

63 ALI Principles, supra note 5, § 1.09.

64 Loosely defined as 'not right or unreasonable', see Arthur Leff, 'Unconscionability and the Code – The Emperor's New Clause', [1967] 115 U PA L Rev., 485.

65 ALI PRINCIPLES, supra note 5, § 1.12.

66 See 'E-Stats 2013: Measuring the Electronic Economy' (Census, May 28 2015) <http://www.census.gov/econ/estats/e13-estats.pdf> accessed 7 July 2015.

67 *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1337 (Fed. Cir. 2003).

68 Or without notable difference.

to be wary of, however, the matter of evolving transaction types is equally troubling. Anticipating how transactions will evolve is unsurprisingly difficult. In the United Kingdom for example, the provisions laid out in the Sale of Goods Act 1893 were eventually deemed unsuitable and replaced by the Sale of Goods Act 1979. Repeal and amendment of statutes are understandable and expected, but an all too frequent change in commercial law is detrimental from an economic standpoint as it brings uncertainty to a market. More established legal norms and methods are preferable in terms of comprehension for consumers and businesses alike. This is particularly relevant to the different types of digital 'goods' that are becoming available through e-commerce.[69] Although the proposal implies that the initial implementation of a digital optional instrument would involve an element of experimentation, a poor start for the instrument could reduce faith in the instrument to a point where it would not be practical to implement and leave it barely used, sharing a fate with UCITA.

26 If it is accepted that pressure from large corporations and consumer groups has stifled the growth of legislation in new areas in the USA, then the concerns of both groups have to be addressed to ensure less friction when attempting to introduce an optional instrument for consumers. Both types of pressure groups have traditionally had primary concerns: large corporations wish to protect freedom of contract; and consumer groups wish to ensure consumer protection measures are enforceable against abuses.

27 With companies' and consumer groups' primary concerns potentially addressed, the instrument must still hold water politically. The tempering of the UCC to ensure that it is adopted by the individual States is reminiscent of the state of affairs with regard to the original proposal for the CESL. Although the CESL proved popular with the European Parliament, the Council rejected it, as many Member States were simply unwilling to allow it to pass in its current form. Lobbies from consumer groups and technical firms dealing in digital content are cited by many as the reason for the reluctance for the Council to accept the CESL without significant modification.[70] Because of the hostility, the CESL was formally withdrawn, and the Commission appears to be once again moving towards maximum targeted harmonization with the Draft Digital Content Directive.[71] The main concern then is that, should the CESL resurface in another form, the scope and power of the instrument might be significantly reduced, leading to a situation not dissimilar to the UCC, wherein the drafters acknowledge a diluted compromise of an instrument being released due to political pressures.

28 The idea that consumer protection is decreasing in the "electronic age"[72] is no different under the CESL - or other EU harmonization - than it is under the American system. The success of either method of legal unification should only be judged on their actual goals, as comparative data in respect to changes in cross-border transactions is not available for both territories. As a goal, the CESL sought to increase cross-border transactions and commentators have suggested it is also intended to enhance European identity.[73] Cross-border transactions are fairly easy to measure, so it would be possible to determine whether or not any future optional instrument would have been a success by its own standards. As previously mentioned, the UCC was a success by its own standards, as it far surpassed the initial expectations for the Code and has continued to evolve over half a century of use. That being said, much of the success would be based on public perception of the optional instrument, and for that to be positive, a point by Karl Llewellyn in regards to the UCC still rings true: "... even where agreements are to have effect in law, they must show sign[s] of being agreements, not dictation or overreaching".[74] That is to say that if any future optional instrument were perceived as being mandatory in all but name, it would be viewed with disapproval. Regardless of how many transactions are governed by the instrument initially, politically it would draw the ire of both consumers and governments. So it can be said that for the instrument to be viewed as a success initially, it must be applied in a wide number of transactions; but for it to be viewed as successful over a longer time frame, it must not seem to have been forced upon the parties.

H. Conclusions

29 This paper asserts that an optional instrument is

69 Clarice Castro, Chris Reed, & Ruy de Quieroz, 'On the Applicability of the Common European Sales Law to some Models of Cloud Computing Services', (2013) 4(3) European Journal of Law and Technology.

70 'Common European Sales Law faces Rocky Reception' (Euractiv, 24 March 2014) <http://www.euractiv.com/sections/innovation-enterprise/common-european-sales-law-faces-rocky-reception-301090> Last accessed 8 September 2014.

71 *Ibid.*, 5.

72 Robert Hillman, Jeffrey Rachlinski, 'Standard-Form Contracting in the Electronic Age' (2002) 77 NYU L rev., 429, 495.

73 Eric Posner, 'The Questionable Basis of the Common European Sales Law: The Role of an OptionalInstrument in Jurisdictional Competition' [2012] University of Chicago Institute for Law & Economics Olin Research Paper No. 597.

74 Karl Llewellyn, 'On Warranty of Quality, and Society: II', [1937] colum. L Rev. vol 37, 341, 403.

desirable on the basis of its unique functionality. By evaluating the functionality of trans-jurisdictional competition and mutual learning methods, a number of impediments to creating an ideal legislative technique to govern digital content were established. Pure yardstick competition, such as the OMC, demonstrated that having a central authority establish best policies, and disseminating such policies throughout the Union is practical, in that it assists in unification and promotes legislative methods that are functional. However, it is difficult to ascertain whether a legislative method would be equally effective in other territories, leading to sub-optimal policies being disseminated on the basis of a misconception of universal applicability. The primary reason that pure-yardstick competition is not the ideal solution is on the basis of the *knowledge problem*, which demonstrates that the best methods in legislating for a particular issue are likely not currently known, and this method is unlikely to make any progress toward that goal.[75] Without incentive for innovation, this method of unification lacks the ability to create optimal policies. Pure trans-jurisdictional competition is the counterpoint, in that it encourages innovation, but provides no incentive or method of unification.

30 The American UCC offered a method of legislation that has similarities to both pure-yardstick competition and trans-jurisdictional competition. The history of the Code demonstrates a number of issues with non-mandatory legislative techniques, in that it can be difficult and time-consuming to encourage adoption of policies amongst States. If the incentive for adopting amendments to the Code were not sufficient, States tend to legislate separately, forming a type of trans-jurisdictional competition, in the midst of an intended mutual learning method. The UCC demonstrates that mutual learning methods without any form of clear incentive for compliance, or sanction for non-compliance, are often ineffective at unifying markets. Competition between authorities has arguably created better legislative options to govern digital content, but at the cost of variation between State legislative approaches. Furthermore, the development of legislation on such a scale is hampered by commercial lobbying, which is seemingly far more effective on such a large scale. Because the stakes are higher than at State level, political lobbying is more effective, and can force legislatures into inaction. It is important to remember, commercial interests want to defend freedom of contract, and consumer interests look for the greatest protective measures.

31 The solution to these issues appears to be offering incentive to innovate, whilst ensuring some level of unification; respecting freedom of contract, whilst maintaining clearly ascertainable protections for consumers. The optional instrument for consumers would consider all of these concerns, establishing a unified contract type for those that wished it, whilst allowing State legislatures to compete against each other for the best national regulatory methods. Businesses would still retain freedom of contract, and consumers would be given strong protections, as long as they remain in line with the former CESL's aims, and are backed up by less specific protections in harmonizing instruments, such as the proposed Draft Digital Content Directive. The benefit of the optional instrument is that, unlike the OMC or UCC, it would not rely on soft law to function effectively, but it would ensure uniformity as States innovate in order to create the greatest economic benefit for themselves. The evolving consumer contract types would be governed by a legislative method that is equally capable of evolving to suit the market. To avert issues such as those faced by the USA with UCITA, the optional instrument would be a more apt solution to govern the evolving consumer contract.

75 Wolfgang Kerber and Martina Eckardt 'Policy Learning in Europe: The "Open Method of Coordination and Laboratory Federalism' [2007] 14(2) Journal of European Public Policy, 227, 232.

* *Joshua Warburton LLB LLM* is the Research Assistant to the Head of the Law School at the University of Leeds.

Regulating Collective Management Organisations by Competition

An Incomplete Answer to the Licensing Problem?

by **Morten Hviid, Simone Schroff and John Street***

Abstract: While the three functions of Collective Management Organisations - to licence use, monitor use, and to collect and distribute the revenue - have traditionally been accepted as a progression towards a natural (national) monopoly, digital exploitation of music may no longer lead to such a fate. The European Commission has challenged the traditional structures through reforms that increase the degree of competition. This paper asks whether the reforms have had the desired effect and shows, through qualitative research, that at least regarding the streaming of music, competition has not delivered. Part of the reason for this may be that the services required by the now competing CMOs have changed.

Keywords: Collective Management Organisations; competition; licensing; reforms; EC; qualitative research

Recommended citation: Morten Hviid, Simone Schroff, John Street, Regulating Collective Management Organisations by Competition: An Incomplete Answer to the Licensing Problem?, 7 (2016) JIPITEC 256 para 1.

A. Introduction

1 The licensing of copyright protected works has been a feature of the music industry for decades, allowing a large variety of users - bars, broadcasters, concert venues etc. - to play music as part of the services they offer. This system rests on central licensing agencies, most commonly known as Collective Management Organisations (CMOs). These administer the rights of copyright holders from a central point, offering licenses to the users. While the system has been in place for a long time and has worked reasonably well (although not perfectly) for analogue uses, the rise of the internet and digital technology has been a game-changer. By expanding the possibility of, and demand for, cross-border uses, the traditional system has come under considerable strain, and is now reaching breaking point as new types of services such as streaming emerge. These services need to license musical works on an EU or global basis to use the technology's full potential. This is difficult because, until now, the CMOs in the EU have been nationally-based monopolies. To obtain a license that covers Europe, 28 different licenses are, in principle required. Such an arrangement clashes directly with the EU's ambition to create a Digital Single Market (DSM).[1] As a result, the current regulatory regime, particularly as it relates to CMOs, has become a

1 For a discussion of the Digital Single Market, see European Commission, Digital Single Market- Bringing Down Barriers to Unlock Online Opportunities 2015 (available at <http://ec.europa.eu/priorities/digital-single-market/>, last accessed 17/12/15).

prime concern of the EU.

2 The functioning of CMOs in the digital domain is of key importance for the DSM.[2] The single market is, after all, intended to allow for the free movement of goods and services across borders, giving EU citizens access to what they most prefer. The inability of the current copyright system to issue cross-border licenses to all users that require them means that CMOs can provide services only on a member state by member state basis, due to the threat of copyright infringement (and therefore high costs) that any unlicensed cross-border use would entail.[3] The result is geo-blocking: individual users are not able to access services once they enter another member state, even if they have paid for those services. Rather than having a single market, online music continues to operate through multiple separate markets.

3 The EU's response to this situation has been to issue a Directive,[4] which is due to be implemented in 2016. This Directive formalises competition between CMOs[5] and places obligations upon them to serve better the interests of users[6] and right holders. In this paper, we assess the possible outcome of this initiative, and argue that there might be more effective ways to address the problem posed by creating a DSM. We confine our attention to the music market, which is feeling the effects of the digital revolution most acutely, at least among the creative industries. We also focus our attention to the streaming of music. Similar issues arise regarding the sales of digital music, for example through electronic stores.[7]

B. Background: The role of the CMO before digitalisation

4 As Handke and Towse point out, the licensing market for musical works in an analogue world was (and remains) highly complex.[8] A large number of creators and products (typically, artists and songs) have to be matched with a similarly large number of diverse users. Asymmetry of information in such a situation creates prohibitive transaction costs for individual licensing between a copyright owner and a user. In other words, individual licensing represents a case of market failure in which copyright owners and

2 See, for example, Intellectual Property Office, Collective rights management in the digital single market available02015 (at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401225/collective_rights.pdf>, last accessed 15/4/16).

3 There have been agreements in the past that offered MTLs, however, they have either not been renewed (see Santiago Agreement), are limited to specific user groups (Simulcasting Agreement), or have been found to be contrary to competition rules (such as the CISAC Model Agreement). For a detailed description of these agreements, please see: Guibault and Van Gompel, Collective Management in the European Union, in Gervais (ed.), Collective Management of Copyright and Related Rights (Alphen Aan Den Rijn: Wolters Kluwer, 2015, 3rd Ed.), 139- 174.

4 Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (Directive 2014/26/EU) (CMO Directive).

5 Competition between CMOs for the management of rights of rights has been introduced in the case law before. CMOs have to be seen as dominant undertakings and are therefore subject to competition rules (GVL v. Commission (Case 7/82, [1983] ECR 483, [1983] CMLR 645); RT v. SABAM (Case 127/73, Belgische Radio en Televisie v. SV SABAM and NV Fonior, [1974] ECR 313, [1974] 2 CMLR 238). The results are a number of restrictions on CMOs towards their members. For the purpose of this article, the most important are the following. It was held that CMOs cannot refuse the management of rights by foreigners, even if they are not resident in a country. This is especially the case if the CMO has a dominant position and quasi monopoly (Case 7/82, Gesellschaft zur Verwertung von Leistungsschutzrechten mbH (GVL) v. Commission, [1983] ECR 483; [1983] 3 CMLR 645). In addition, right holders cannot be required to assign all of their rights. (Case 127/73, Belgische Radio en Televisie v. SV SABAM and NV Fonior, [1974] ECR 313, [1974] 2 CMLR 238)), in particular their online rights (Daftpunk) (Case C2/37.219, Banghalter et Homem Christo v. SACEM, 6 August 2002). This is limited by economic viability though. A CMO cannot be forced to accept only those rights which are expensive to administer (see for example, Case 127/73, Belgische Radio en Televisie v. SV SABAM and NV Fonior, [1974] ECR 313, [1974] 2 CMLR 238, para. 10, 11 and 15).

6 User interests are only indirectly addressed, for example in the transparency rules which are meant to give users the information they need to choose licenses (see in particular (Directive 2014/26/EU) (CMO Directive), art. 19- 22.).

7 Some of these issues have been addressed, either through coalitions of old structures to create broader organisations which can offer bundled clearing of copyrights; or through new structures such as Merlin- a right clearance organisation which can also offer MTLs. However, not all Copyright Management Societies in the EU are members of such structures. Thus transaction costs are incurred to provide pan-EU availability of digital music. As Gómez and Martens note: "We find that in August 2013 there was still substantial variation in availability in the iTunes country stores across the EU DSM. Less than half of all song tracks and music albums are available in all EU27 country stores. Overall, music availability in the EU DSM is somewhere between 73 and 82 per cent of what it could be in a fully open DSM where all song tracks and albums would be available in all EU27 countries." (Gómez and Martens, Language, Copyright And Geographic Segmentation in the EU Digital Single Market for Music and Film, JRC/IPTS Digital Economy Working Paper 2015, (available at <http://ssrn.Com/Abstract=2603144>, last accessed 15/4/16), 3-4. However, Gómez and Martens do acknowledge that matters are improving. It should also be noted that some right holders' business strategies relies on fragmented markets to maximise profits, as for example in the audio-visual sector. These attitudes may oppose the aims of the Commission but nonetheless also affect the availability of pan- European licenses.

8 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15).

the users would both lose out. The copyright owner would not generate the income they seek while the user is not able to legally play the music they want. The solution to this problem has involved several intermediaries, including CMOs streamlining the financial transaction between the creator and user.

5 CMOs act to reduce the market failure.[9] In general, they have three functions: 1) to license works for specific uses; 2) to monitor the use of works and collect the revenue; and 3) to distribute the revenue to its members.[10] The CMOs collect the revenue for low-value, high volume secondary uses; that is, uses where the individual licensing fee is small but the number of licenses which need to be issued add up to a substantial revenue stream. CMOs manage the rights of its members collectively, providing blanket licenses to users. By managing the rights collectively, they are able to lower the transaction costs as well as provide a stable licensing framework. In economic terms, they enable the market to function by ensuring copyright effectiveness in circumstances where copyright owners cannot contract directly. A blanket license gives users – especially broadcasters – the right to use any music within the CMO's repertoire. The blanket licenses reduce the transaction costs because they do not require negotiations on the price or the exact size of the rights bundle for each individual transaction.[11]

6 CMOs have been a core feature of the licensing market within the EU (and beyond) for more than a century. Based on a system of reciprocal agreements between CMOs, they have been able to license a world-wide repertoire. A user can therefore use any song they want and only pay their local CMO. The transfer of funds across borders is carried out by the CMOs themselves and is of no concern to the user. As a result, CMOs have established a system of national monopolies, which do not compete with each other, but instead operate under a set of agreements which determine the cost of licenses. While this broad coverage in works, the economies of scale, and the resulting monopoly status contribute to efficient licensing in practice, it is also the source of the European Commission's main concern. While the licences are "blanket", their price may well differ according to the type of organisation that requests the blanket licence. No stakeholder is able to judge the price charged and the lack of a viable alternative has meant that a copyright holder has no incentive to defect to a rival CMO, no matter how dissatisfied they are.[12] The CMO's monopoly status has given rise to typical concerns often attributed to monopolies—namely the potential abuse of a dominant position.[13] Market prices cannot be established; neither for the users in terms of how much they should pay for their license, nor for the copyright owners, in relation to the cost of administration that the system entails.[14]

7 EU case law has established that the CMOs are undertakings which hold a dominant position, meaning that they are subject to the full force of competition law, including both article 101 TFEU relating to concerted practices and article 102 TFEU relating to the abuse of a dominant position.[15] This required restrictions on how they operated. However, the CJEU also ruled that CMOs serve the public interest, and that, therefore, competition law was not to be applied rigidly.[16] In other words, while the Court found the monopoly status and reciprocal agreements justifiable in the broader

9 Haunss, The Changing Role of Collecting Societies on the Internet, Internet Policy Review 2013, 1-8, Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15).

10 Andersen, Kozul- Wright, Z. and Kozul- Wright, R, Copyrights, Competition and Development: The Case of the Music Industry, United Nations Conference on Trade and Development. Geneva: United Nations Conference on Trade And Development 2000 (available at: <http://unctad.org/en/docs/dp_145.en.pdf>, last accessed 15/4/16), 21.

11 There is an extensive economics literature on what is often termed "buffet" pricing inspired by the "all-you-can-eat buffets". Much of this literature has focused on behavioural aspects, in particular those which lead to obesity, which does not appear to be particularly relevant in our context. The behavioural literature is summarised in Lambrecht and Skiera, Paying Too Much and Being Happy About It: Existence, Causes, and Consequences of Tariff-Choice Biases, Journal of Marketing Research 2006, 212–223 as well as Just and Wansink, The flat-rate pricing paradox: conflicting effects of "all-you-can-eat" buffet pricing, The Review of Economics and Statistics 2011, 193-200.

12 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15).

13 Assessing such abuses is made complicated by the two-sided nature of the market, where the intermediary can decide from which side of the market, copyright holders or users, to extract rent, either in terms of funds or a "quiet life".

14 Kretschmer, Access and Reward in the Information Society: Regulating the Collective Management of Copyright (Poole: Centre for Intellectual Property Policy & Management, 2005), 7.

15 Graber, Collective Rights Management, Competition Policy and Cultural Diversity: EU Law Making at a Crossroads, I-Call Working Paper 2012 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2161763>, last accessed 15/4/16), 6.

16 See for example: Case C-395/87 Ministère Public v Tournier, [1989] ECR-2521, para. 24; Lucazeau v SACEM ECR 2811; GVL v. Commission (Case 7/82, [1983] ECR 483, [1983] CMLR 645; Case 127/73, Belgische Radio en Televisie v. SV SABAM ECR 51 313. All of these cases involved the application of competition law and recognised that there are legitimate interests that can limit its application in practice. Also discussed in: Graber, Collective Rights Management, Competition Policy and Cultural Diversity: EU Law Making at a Crossroads, I-Call Working Paper 2012 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2161763>, last accessed 15/4/16), 6.

public interest, it also recognised the negative impact the system could have on users and right holders. For this reason, CMOs are required to offer users reasonable licensing terms, while at the same time giving their members as much freedom to administer their rights as independently as possible (as long as this is consistent with the functioning of the CMO as a whole). Copyright owners should be able to administer their rights individually insofar as this does not impose undue costs on the CMO. For example, while withdrawing all one's works or the online rights attached to those works is acceptable, withdrawing the online rights for works A, B and C, but not D, and G, is not, because keeping track would be too expensive for the CMO.[17] In essence, the regulations have attempted to balance the threat of monopolisation against effective rights administration.[18] However, given that there was no viable alternative to the CMO system the Commission tolerated it. The rise of the internet has changed the rules of the game.

8 It should be noted that some authors have questioned the treatment accorded to CMOs in the analogue world. Katz in particular challenges the claim that in the analogue world the CMO is a natural monopoly.[19] He observes that more than one CMO may operate in a single territory. Unlike most other countries, where the CMO is a monopolist, the US has three CMOs managing musical works (ASCAP, BMI and SESAC) of which one (SESAC) is rather smaller than the others (less than 5% in 2000)[20] and has coexisted with ASCAP since 1931 and all three have been in the market since 1941. The traditional argument in favour of natural monopoly — economies of scale — is not compatible with the persistent existence of such a small firm.

9 Katz reminds us that, while the CMOs charge for a blanket licence, they do not charge all users the same price.[21] Thus they use their monopoly power to engage in third degree price discrimination[22], charging different prices to different types of businesses, a practice which has an ambiguous effect on both total and consumer surplus. Katz also points out that the existence of different licences for performance of the work adds an extra tool to the CMO to practice successful price discrimination because it enables the CMO to identify the nature of each user.[23]

10 In a supplementary article, Katz explores how his argument would apply in the digital world. Given his conclusion for the analogue world, it is hardly a surprise that he is sceptical about the monopoly argument.[24] However, given when it was written, his paper has to engage in speculation. While it undoubtedly was ahead of its time in 2006, and many of the speculations have come to pass, it adds little to the current debate. However, it does help us understand why the Commission viewed the digital world differently when it comes to competition.

C. The Digital Challenge

11 As digital technology, and especially the internet, rose in importance, the needs of users changed dramatically. A new breed of services came to the fore, most notably, the streaming platforms (Spotify, Deezer, Amazon Music, etc.). They differ from analogue users in the kind of licenses they require. Analogue users only require territorial licenses; their services do not cross national borders[25] and therefore they do not require licenses that extend further. However, the internet (and digitalisation) creates the possibility of easy access to music irrespective of tariff barriers or broadcasting regulations. Any legal service seeking to exploit these possibilities requires multi-territorial licenses. To cater to this need, CMOs reacted first by offering Simulcasting agreements, providing cross-border licenses to internet radio. The Commission accepted this solution as a

17 Kretschmer, Access and Reward in the Information Society: Regulating the Collective Management of Copyright (Poole: Centre for Intellectual Property Policy & Management, 2005), 5.

18 Dietz, Legal Regulation of Collective Management of Copyright (Collecting Societies Law) in Western and Eastern Europe, Journal of the Copyright Society of the USA 2002, 908.

19 Katz, The potential demise of another natural monopoly: Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 541-593.

20 Katz, The potential demise of another natural monopoly: Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 554.

21 Katz, The potential demise of another natural monopoly: Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 541-593.

22 Firms engaging in third degree price discrimination offer different prices to different identifiable groups of buyers – a classic example is different prices for different age groups.

23 Katz, The potential demise of another natural monopoly: Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 550.

24 Katz, The potential demise of another natural monopoly: New technologies and the administration of performing rights. Journal of Competition Law and Economics 2006, 245-284.

25 While strictly speaking not true, this is the assumption which has been made in the industry, motivated by a view that Broadcasters are (supposed to) focus on their national audience, not least because of language barriers. The exception is broadcasting with the Simulcasting Agreement which resolves the issue by treating broadcasters as geographically limited users and therefore as essentially the same as analogue users.

permissible exception under article 101(3) TFEU (which began in 2004).[26] However, it remained the exception, even as the Commission came to realise that digital technology was not only changing user requirements but the system as a whole.

12 The driver of change was not just user demand, but the very nature of licensing itself. Handke and Towse have argued that primarily, digital technology makes the gathering and processing of information much easier. Secondly, they argue that it enhances market signalling: on one hand, the use of individual works can now be assessed with more precision than before; on the other hand, there is potential for price discrimination and charging every user what they are willing to pay. Finally, as a result of these factors, CMOs are able to reduce their costs.[27] New technologies such as Digital Rights Management (DRM)[28], which enable rights to be administered individually,[29] can enhance efficiency. This of course undermines the CMO's justification for their monopoly status,[30] as there are now real alternatives to them.

D. A new regulatory regime

13 The change in the Commission's attitude first became clear when it refused to accept the Santiago and Barcelona Agreements, which aimed to extend the analogue licensing system to the digital domain.[31] The Commission's attitude was made even clearer when it rejected CISAC's model contracts. CISAC, the world-wide umbrella organisation for CMOs, devised model contracts to allow its members to offer multi-repertoire, multi-territorial licenses. The contracts had three core features: a national allocation clause, an exclusivity clause, and a non-intervention clause. Combined, the latter two had the effect of maintaining the national delineation of CMOs, guaranteeing their monopolies. While these clauses were not new, the Commission now considered them unjustified— digital technology meant that a local presence was not required to ensure efficient enforcement.[32] The Commission argued that digitalisation enabled CMOs to compete with each other in the field of digital exploitation, meaning online use in practice. Overall, it found the model contract contrary to competition rules under article 101 TFEU,[33] although this decision was overturned by the General Court in 2013.[34] Instead, CMOs should, the Commission believed, compete with each other to attract members and users. This in turn should lead to increased efficiency in the rights administration, aiding the emergence of new markets.[35] The Commission shifted from viewing the CMO as a necessary evil for ensuring the effective licensing of works, to seeing it an as unnecessary anti-competitive undertaking which harmed both right holders and users. This stance was to become clear Commission policy.

14 While Katz's analysis casts doubt on the survival of the past monopolising elements of collective rights management, the move to digital exploitation could, at least in theory, give rise to a new monopoly element.[36] This has so far attracted

26 Guibault and Van Gompel, Collective Management in the European Union, in Gervais (ed.), Collective Management of Copyright and Related Rights (Alphen Aan Den Rijn: Wolters Kluwer, 2015, 3rd Ed.), 160-161. Other agreements such as the CISAC model contract (leading to the cases European Commission, Commission Decision of 16/07/2008 relating to a proceeding under Article 81 of the EC Treaty and Article 53 of the EEA Agreement (Case COMP/C2/38.698 – CISAC) (available at <http://ec.europa.eu/competition/antitrust/cases/dec_docs/38698/38698_4567_1.pdf>, last accessed 17/12/15) and the CJEU decision CISAC v. European Commission (Case T-442/08)) and the Santiago Agreement (Notification of cooperation agreements (Case COMP/C2/38.126 – BUMA, GEMA, PRS, SACEM),O.J. C. 145/2 of 17.05.2001) as well as the Barcelona Agreement (Notification of cooperation agreements (Case COMP/C-2/38.377 – BIEM Barcelona Agree-ments), O.J. C. 132/18 of 4.06.2002) were found anti-competitive.

27 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15), 13.

28 In this context, DRM is a tool to control the type of access one has to digital music. It controls both access and usage. For a discussion of the merits of DRM, see e.g. Doctorow, What happens with digital rights management in the real world?, *Guardian*, 5 February 2014 (available at: <https://www.theguardian.com/technology/blog/2014/feb/05/digital-rights-management>, last accessed 15/4/16).

29 Kretschmer, Access and Reward in the Information Society: Regulating the Collective Management of Copyright (Poole: Centre for Intellectual Property Policy & Management, 2005), 17.

30 Ficsor, Collective Management of Copyright and Related Rights, WIPO 2002 (available at: <http://www.wipo.int/edocs/pubdocs/en/copyright/855/wipo_pub_855.pdf>, last accessed 15/4/16), 98.

31 Frabboni, Collective Management of Copyright and Related Rights: achievements and problems of institutional efforts towards harmonization, in: Derclaye (ed.), Research Handbook in the Future of EU Copyright (Cheltenham: Edward Elgar, 2009), 373-400.

32 Guibault and Van Gompel, Collective Management in the European Union, in Gervais (ed.), Collective Management of Copyright and Related Rights (Alphen Aan Den Rijn: Wolters Kluwer, 2015, 3rd Ed.), 162.

33 European Commission, Commission Decision of 16/07/2008 relating to a proceeding under Article 81 of the EC Treaty and Article 53 of the EEA Agreement (Case COMP/C2/38.698 – CISAC) (available at <http://ec.europa.eu/competition/antitrust/cases/dec_docs/38698/38698_4567_1.pdf>, last accessed 17/12/15), 220-223.

34 CISAC v. European Commission (Case T-442/08).

35 Sparrow, Music Distribution and the Internet: A Legal Guide for the Music Business (Aldershot: Gower, 2006), 1.

36 Katz, The potential demise of another natural monopoly:

little commentary. With more data available electronically, a comprehensive database of all right holders and associated material would not only be essential, but also display increasing return to scale both in its creation and maintenance. For full functionality it is important that the database is comprehensive. Given the cost of establishment and maintenance, it would be inefficient to have two parallel fully comprehensive databases. By contrast, the other elements - such as monitoring and collecting money - seem to have less of a claim to monopoly status once services become digital. Given the international nature of such a database, there is a serious issue as to who regulates the terms of access and how the database is to be funded. Building on existing databases held by CMOs, one possibility would be for these to set up an institution to hold, transform and maintain these databases. This has to some extent already happened. Most CMO databases (and all of the ones examined here) are part of CIS-Net, the most comprehensive database for musical works and their corresponding rights. It is owned by FastTrack, which, in turn, is owned by the CMOs. The question is whether competition among the CMOs (in the EU) is sufficient to generate a comprehensive database, whilst at the same time engendering a meaningful and valuable choice.

15 In 2005, the Commission reported on the lack of cross-border licenses for users in the online market. It proposed that rights holders should be free to choose their CMO, the rights that they assign to it and their associated territorial reach.[37] The underlying rationale is a typical competition remedy: by giving the individual the choice over the provider, they can choose the service that most closely matches their preferences. In other words, by allowing right holders to vote with their feet, CMOs would be bound to become more efficient in an effort to not lose members. Furthermore, CMOs would issue pan-European licenses, and by choosing their CMO carefully, rights holders would be able to ensure that each CMO would be able to offer coherent bundles.[38] The Commission's recommendation rejected the analogue services' use of reciprocal licence agreements and full harmonisation.[39] Their approach became law in the 2014 CMO Directive 2014/26/EU. The Directive focused on more competition rather than on harmonisation or an extension of the traditional system of reciprocal agreements. The Directive aims at providing an environment in which competition can be fully effective. It sets minimum standards for the transparency and supervision of CMOs by their members and therefore the right holders.[40] Both of these are typical competition remedies, which have been applied to areas such as the energy market. In the case of the music industry, EU policy is based on the distinction between the analogue and the digital licensing market for musical works, and the need to alter the role played by CMOs in the latter. However, the major CMOs are already meeting the Directive's demands,[41] so the question is whether the legislative intervention will have its intended effect. After all, if the database existed and access was regulated/mandated, then the right holder would genuinely have choice based on the quality of service.[42] To answer our question, we investigated the problems that actually affect users in the digital realm.

E. Methodology

16 To understand the current state of licensing in the EU, we compared the experience of an analogue user with that of one who seeks a license for online exploitation. We simulated the path a potential broadcaster or web-streaming service would follow in acquiring a license, starting with the first search to identify CMOs all the way to the final license. It is assumed that the broadcaster seeks a multi-repertoire, single-territory license because they want to be able to use all kinds of music in their programming which, by the nature of the broadcasting sector, is assumed to reach a national audience. By contrast, a web-streaming service would also want to offer all kinds of music but on a multi-territorial basis, making its programmes accessible around the world, or at least within Europe to fully exploit the potential of the Single European Market.

Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 541-593, Katz, The potential demise of another natural monopoly: New technologies and the administration of performing rights. Journal of Competition Law and Economics 2006, 245-284.

37 European Commission, Commission Recommendation of 18 May 2005 on Collective Cross-Border Management of Copyright and Related Rights for Legitimate Online Music Services (2005/737/EC)" (available at <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005H0737&from=EN>, last accessed 17/12/15).

38 Note that rights holders would have an incentive to seek out CMOs who "managed" material similar to their own to give that CMO more bargaining power vis-à-vis the users.

39 Kretschmer, Access and Reward in the Information Society: Regulating the Collective Management of Copyright (Poole: Centre for Intellectual Property Policy & Management, 2005), 13-14.

40 Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (Directive 2014/26/EU) (CMO Directive), Part III.

41 Schroff and Street, The politics of the digital single market: the case of copyright, competition and collective management organisations (forthcoming).

42 For music, there may be an unnecessary stumbling block as rights can only be assigned on an exclusive basis to a CMO and therefore not to more than one collecting agent at the same time.

We used these two licensing scenarios to explore the practical issues raised by providing multi-repertoire, cross-national content.

17 The empirical research was designed in such a way as to give a realistic picture of the situation and challenges faced by practitioners. For this reason, it was carried out by a research associate who has legal training but is not working in the field of intellectual property or licensing copyright material. In our view, this mimics the experience of those individuals who have to acquire licenses for commercial services. The researcher was asked to keep track of how she identified relevant organisations, noting down the challenges that she encountered. We chose a representative set of European case studies: the UK, France, Germany and Sweden. The findings are striking: while the analogue user finds a system in place to satisfy their licensing needs, the same is not true for those who want to run streaming services.

F. Findings: the problems for online users

18 The main finding is that CMOs are either unable or unwilling to satisfy the demand of online-services. When a broadcaster seeks a license, all of our case studies were able to provide them with a multi-repertoire license for the rights in musical works. This was because of the reciprocal agreements that CMOs have with each other. In this sense, the broadcaster has in this sense access to a one-stop-shop. Table 1 below summarises the steps taken as well as the key difficulties in obtaining the right to make copyrighted content available across borders in the case of broadcasting. It is clear from Table 1 that there are only limited difficulties in obtaining a licence for traditional broadcasting.

19 **Table 1: Broadcasting**

	France	Germany	Sweden	UK
Licenses Required	SACEM (covers other CMOs for musical works) SCPP/ SPFF	GEMA GVL	STIM SAMI IFPI	PRS/ MCPS PPL
Information on Coverage	Yes	Yes	Limited	Yes
Broadcasting Tariff available online	Yes	Yes	No	Yes
Indemnity for Licensees (coverage of non-members)	No	Limited (presumption of management)	No	Limited (presumption of management in some cases)
Information available in English	Partial (does not include substantive licensing information)	Partial (does not include substantive licensing information)	Yes	Yes

20 In contrast, Table 2 below demonstrates the considerably greater difficulties encountered in obtaining licences for web-streaming. The licenses for online uses are a lot more complicated, not least because the descriptions used by the CMOs are very vague. Although some multi-territorial licenses exist, it is not clear which works are covered by them. For example, in the UK it is apparent that PRS, the CMO for songwriters, composers and publishers, is able to license the Anglo-American repertoire of certain publishers on a multi-national basis. However, there is no way to check what is actually included in this description. They are not blanket licenses like the ones available to broadcasters in the analogue system. This means in practice that more than one license is necessary to cover the same category of works, increasing the cost for the user.

21 Secondly, just because the license is described as multi-territorial, it does not follow that this involves EU-wide coverage.[43] For example, the French CMO SACEM is only able to license France, Luxembourg and Monaco — the three countries in which it is the main CMO anyway. It would have always been able to license these even without a change in EU policy.[44] Similarly, the other CMOs only offer licenses that cover a very limited number of countries, but none of them provided clear information as to what countries were included. As a result, not only is there no comparable one-stop shop, the territorial gaps in the license are also unclear, giving rise to major concerns regarding what is allowed. In sum, while a broadcaster is provided with a one-stop-

43 A similar problem was observed for the sale of digital music, see Gómez and Martens, Language, Copyright And Geographic Segmentation in the EU Digital Single Market for Music and Film, JRC/IPTS Digital Economy Working Paper 2015, (available at <http://ssrn.Com/Abstract=2603144>, last accessed 15/4/16).

44 The CMO Directive has been an issue at EU level for a significant amount of time before the Directive was finalised. It is therefore possible that stakeholders anticipate the changes early on knowing that they will have to comply at some point. Having said this, SACEM has been able to issue licenses for these three territories for years. It is therefore unlikely that changes in EU policy had an effect on SACEM in this case.

shop to satisfy their licensing needs, the same route is not available to online services wishing to operate across borders. In fact, they struggle with a more fundamental problem — a lack of information about the coverage of the license.

22 Table 2: Web-streaming

	France	Germany	Sweden	UK
Relevant CMOs	SACEM but does not cover phonograms or performances	GEMA but does not cover phonograms or performances	STIM but does not cover phonograms or performances	PRS but does not cover phonograms or performances
MTL Licenses	Not available. SACEM offers a license limited to specific territories but not truly MTL. No information available from other CMOs	Not available. GEMA offers an online tariff covering Germany and some limited multi-national licenses but not Europe- wide. No online tariff by GVL	Not available. STIM offers some limited MTL, especially for Scandinavia. No information available from other CMOs	Not available. PRS/ MCPS offers a license limited to specific territories but not truly MTL. No information available for PPL
Tariff available online	Only SACEM for limited territories	Only GEMA for limited territories	Only for STIM for limited territories	Only for PRS/ MCPS for limited territories
Indemnity for Licensees (extent to which non-members are covered)	No	Limited (presumption of management)	No	Limited (presumption of management in some cases)
Information available in English	Partial (does not include substantive licensing information)	Partial (does not include substantive licensing information)	Yes	Yes

23 A second notable insight from the two tables is the similarities across the countries and hence the relevant CMOs. If competition was driving new or better licensing services, one would expect to see more variation.

G. The Directive and the limitations of competition

24 It would appear from our research that the Directive not only offers no solution, but in fact worsens the problem in some areas. The reasons can be found in its inadequate conceptualisation of copyright, especially its dynamics and the interests involved. In fact, in its current form, it is likely to make the situation more difficult for the majority of authors and users, only really benefitting a small group of large right holders.

I. The User Lost in the Labyrinth

25 The real losers of the changes are the users in the online environment. Having blanket licenses, as broadcasters do, means that most of the identification costs associated with licensing is carried by the CMO. They have to identify the relevant right holders, and they have to transfer revenues to sister CMOs for the repertoire that is used. In the digital environment, the cost is shifted entirely onto the user. Online users however, have to identify the relevant right holders because CMOs are not able to offer blanket licenses. Instead, the user needs to contact a large number of CMOs, hubs aggregating the repertoire of different CMOs, and even individual right holders.

26 Where the local CMO cannot provide licenses with multi-territorial cover, the user has to contact the CMOs in all member states as well as those right holders that have withdrawn their rights.[45] This poses major problems for all aspects of the licensing process. First, there is the problem of identifying the repertoire which requires an additional license and the right holders associated with it.[46] As we have seen, statements about the scope of the repertoire and rights managed by the CMO can be very vague, rendering it difficult to tell what is and is not included. Databases, such as CIS-Net, are

45 An alternative would be to "boycott" songs which were not obviously covered by readily available licences. This may lead to either pressure from the rights holders of those songs to have them included or to migration of those rights holders to another CMO.

46 How big the problem is depends on the activism of the rights holders. If they are very active users of the services, they will identify which CMO offers the best home in terms of repertoire and shift their licences to that CMO. More generally it is important not to treat the rights holders as passive actors.

not publicly accessible.[47] As a result, the only way[48] a user could guarantee a multi-repertoire, multi-territorial blanket style license would be to contact all CMOs or the necessary combination of hubs and CMOs. This difficulty is exacerbated by the absence of authoritative and complete lists to identify CMOs, especially across borders. Our research revealed (especially the second row of Table 2) that it is difficult to identify all relevant CMOs without resorting to the academic literature — a resource which is not easily accessible to the general public. In fact, determining which CMOs need to be contacted has proved to be yet more complex because the information provided is vague. A potential user has to read around the topic, relying on blogs and similar searches. While this may work in practice, the lack of verifiable information is a source of concern. Furthermore, while CMOs provide significant amounts of information on their homepages, it tends to be in their national language. In cases where sections have been translated into English, they are often significantly smaller. In particular, translations of licensing forms are not available. By comparison (Table 1), broadcasting tariffs are clearly accessible and explained by all the relevant organisations on their websites.

27 Given the complexity of the task, users can never be sure if they have actually covered everything and potentially expensive infringement claims remain a possibility. Given the problem of securing the necessary complete clearance, one might reasonably wonder whether it would be better not just for the user, but possibly also overall, if it was accepted that there might be occasional copyright violations but that these would be resolved through court settlements.[49] The key issues here are: what the costs and fines are in cases of infringement; whether the fine is proportional to the loss suffered by a rights holder; and whether the latter ought to have a duty to make it clear which CMO or other vehicle is used for revenue gathering. The extent of the damages depends too on the type of business requiring the licence. In the case of YouTube-style ones, they will be told to take something down. If they do not comply reasonably fast, then they will be held liable. If the service is a Spotify-style one (i.e. no user uploads), then the service would be liable straight away as licenses have to be sought before the service is made available. One question is whether the strategic re-assigning of rights can be used to deceive or trick users in order to cash in later, essentially by acting in a manner equivalent to patent trolls.

28 There is very little information available on how much licensees have to pay as a result of licensing disputes. Most disputes are settled out of court and the details are kept confidential, even if they involve a large number of plaintiffs complaining against a licensing fee.[50] One of the few exceptions is the example of NSM Music which was ordered to pay £85,000 plus interest and legal costs after it lost a licensing dispute with PRS for Music.[51] However, the claims involved in these cases are substantial. In the long-running dispute between the German GEMA and YouTube, the demands reached €1.6 million for the infringement of 1,000 songs that were uploaded by users without consent.[52] In fact, it demanded 0.37 euro cent for each time a song is played.[53] It is easy to see how this could lead to very high costs once the provider is found liable.[54]

II. Everyone Loses Out: the Income

29 The complexity of the current system is also likely to lead to an overall lower licensing income, simply because users cannot manoeuvre the system efficiently. As a result, they either do not offer a service on the scale they would prefer, or they do not pay all rights holders as they should.

30 Looking at the system in practice clarifies this. Today, those CMOs that are able to offer truly multi-territorial licenses are managing Hubs. Hubs refer to the separate legal entities founded by a (large-

47 An interesting question is whether an exclusion could be challenged on competition grounds as an abuse of dominance. The databases may be seen as essential facilities to which some users might be able to force access in return for a reasonable fee.

48 Given the current set-up. As Katz points out, there are alternative solutions if the rights holders and publishers are ready to embrace them. Inspiration for this could potentially be drawn from the e-book market. (Katz, The potential demise of another natural monopoly: Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 541-593.)

49 See Viacom International, Inc. v. YouTube, Inc., No. 07 Civ. 2103.

50 ITV et al v PRS and MCPS, Consent Order by the Copyright Tribunal (cases CT 117,188, 199) (available at <http://www.bailii.org/uk/cases/UKIntelP/2012/o011911.pdf>, last accessed 15/4/16).

51 PRS for Music, NSM Music ordered to pay PRS for Music license fees 2011 (<http://www.prsformusic.com/aboutus/press/latestpressreleases/pages/nsmmusicorderedtopayprsformusiclicencefees.aspx>, last accessed 15/4/16).

52 LG München I: Keine Haftung des Plattformbetreibers für Urheberrechtsverletzungen, MMR 2015, 831. The revision was also turned down: OLG München: YouTube schuldet GEMA keinen Schadenersatz, MMR-Aktuell 2016, 375539.

53 Schadensersatzprozess: Gericht weist erneut Gema-Klage gegen YouTube ab, Der Spiegel 28 Jan 2016 (<http://www.spiegel.de/netzwelt/netzpolitik/youtube-gema-verliert-vor-olg-muenchen-a-1074418.html>, last accessed 15/4/16).

54 It should also be noted that YouTube was not found liable in this case due to secondary liability issues. The fee demand itself was not determined as unreasonable.

scale) right holder for the purpose of licensing. Most of them cooperate very closely or are even managed by one or more CMOs. As a result, these CMOs are able to license this repertoire in addition to their own repertoire. However, the CMO which had originally held these works will not be able to issue a license anymore.[55] Major publishers have bundled their rights in these Hubs but the repertoire is not universal. Instead, repertoire coverage is divided by publisher or even by sections of a publisher's repertoire (for example, Latin-American or Anglo-American music). The management of Hubs overlaps so that specific CMOs are able to license rights of more than one repertoire. For example, PRS for Music in the UK is involved in "*Peer Music Publishing Anglo-American repertoire, Imagem Anglo-American repertoire, IMPEL Anglo-American repertoire, CELAS and SOLAR*[56] *(EMI and Sony/ ATV Anglo- American repertoire) and Warner Chappell Music Publishing repertoire as a PEDL partner*".[57] However, depending on what type of repertoire the user requires, it is likely that they will have to contact more than one CMO to cover all the required rights. The multi-repertoire license has been sacrificed for multi-territorial coverage as the licenses do not combine both.

31 In addition, these Hubs cover only musical works. All other types of works for which licenses are required cannot be cleared this way. Record labels which own the rights in the performance and phonogram usually manage their rights individually, but on a multi-territorial basis. The exception is Merlin which licenses for a range of Independent labels on a multi-territorial basis.[58] There is also some limited cooperation for cross-border licensing among the CMOs in this area. For example, GVL, the German CMO for performances and phonograms, offers multi-territory licenses, but these cover only 20 member states[59] and is therefore not sufficient for EU-wide clearance, which for example Europeana[60] requires. Europeana only accepts works which will be accessible in all EU member states.[61] As a result, it would be necessary in most cases to contact the record label in order to clear the rights in the records and performances; contacting the CMOs alone would not be sufficient as they cannot provide adequate MTL coverage. Finally, there is still no authoritative list of Hubs and CMOs and of which works and rights are covered, making the process more laborious.[62] As a result, the MTL licensing of musical works is entirely divorced from other related rights, even when they are intrinsically linked - such as musical works and performances.

32 In practice, finding Hubs takes a significant amount of effort in practice. They are not prominently featured or promoted by the CMOs. There is also no database or similar facility to help users determine if there is a Hub able to provide them with the license they seek. Furthermore, even these projects are very limited in scope. In fact, most focus is on the Anglo- American repertoire. These Hubs also do not have separate homepages with licensing facilities that can be contacted directly; they are managed by the CMOs. Thus, the number of potential actors has increased, rather than decreased - another step away from the one-stop-shop that broadcasters enjoy.[63] If musical works cannot be licensed, incomes cannot be generated and therefore the incentivising effect of copyright is itself weakened.

55 Exploitation contracts that CMOs have with the right holder do usually require the exclusive assignment of rights. The Directive does not actually prohibit that. As a result, when the rights are withdrawn, they are usually withdrawn entirely, meaning that the original CMO does not manage them anymore. The right holder is still able to license non-commercial uses directly (article 5(3)) but these are not relevant for this study. It should be noted though that if the MTLs are based on the passport system, meaning that CMO 1 has mandated CMO 2 to manage the online licensing under article 29 of the CMO Directive, then these agreements are not exclusive. However, this is not the case for the HUBs discussed here as these have the rights entrusted to them directly.

56 SOLAR combines the Hubs from PAECOL (GEMA) and CELAS. GEMA, Sony/ ATV Launches Joint Venture with PRS for Music and GEMA (<https://www.gema.de/en/aktuelles/sonyatv_launches_joint_venture_with_prs_for_music_and_gema-1/>, last accessed 14/9/15).

57 PRS for Music. 2015. "Multi-Territorial Licensing" (<https://www.prsformusic.com/users/broadcastandonline/onlinemobile/multiterritorylicensing/Pages/default.aspx>, last accessed 10/9/15).

58 Merlin is a rights clearance organisation that manages the rights on behalf of independent labels. In difference to other organisations in this area, its licenses cover more than one territory. In other words, the user can license the rights held by many different independent labels in a one-stop-shop by contacting Merlin. They do not have to go back to the labels. It is an issue though that the actual membership is not known and therefore may not represent a specific Indie label in question. (<http://www.merlinnetwork.org/>, last accessed 10/9/15).

59 GVL, Länderliste Web_radio (available at <https://www.gvl.de/rechtenutzer/webradio/laenderliste-webradio>, last accessed 10/9/15).

60 Europeana is the common gateway where users can access materials digitised and hosted by European cultural heritage institutions. It can be accessed here: <http://www.europeana.eu/portal/>. The example is used here because it has been actively promoted at EU level.

61 GVL, Länderliste Webradio (available at <https://www.gvl.de/rechtenutzer/webradio/laenderliste-webradio>, last accessed 10/9/15).

62 The CMO Directive does envisage such a list and requires the Commission to make it public. However, this has not happened yet. (Directive 2014/26/EU) (CMO Directive), art. 39.

63 This highlights the fundamental trade-off between the greater convenience of dealing with a single firm, a monopoly, and that with a monopoly where there is no competition. A similar dilemma has in the past arisen in the case of "yellow pages", where both advertisers and consumers would prefer a single provider so long as that provider did not abuse its monopoly position.

33 This is made even worse in practice as the Directive omits a key part of the licensing process. Licensing music is a direct result of copyright law, especially the right to control the public performances of musical works and sound recordings. The Directive only sets licensing standards for the multi-territorial licensing of musical works. However, from a copyright point of view, performing a work in public, such as streaming or broadcasting it, requires a license covering the performance and the recording of the work. These are considered neighbouring rights and administered by a distinct and separate set of CMOs.

34 The clearest indication of this is the lack of streaming tariffs via CMOs for neighbouring rights. For example, in Germany a broadcaster needs a license from GEMA for the musical work and from GVL for the performance and the sound recording. For streaming the situation is more complicated and more fragmented. The GVL, for example, does not offer a streaming tariff on its homepage and in fact also does not mention how to acquire the license in practice. This means that a user has to contact the right holder directly - a very onerous process in practice, given the large number of record labels and other right holders involved. The situation is not any different in the other member states; in all our cases the access to neighbouring rights for online exploitation is limited in comparison to analogue uses (such as broadcasting). In this respect, it is unrealistic to expect users to acquire the correct license in a system that is vague, highly complex and unable to meet the demand. The failure of licensing practices to change quickly enough could actually harm the aim of copyright as a whole.

III. The Freedom of the Right Holder

35 For the user, the fragmentation of the rights is the root of the problem. However, the Directive explicitly allows copyright holders to split their rights into bundles, based on the type of right and the territorial scope. This results in a worsening of the situation: the administration of rights has become increasingly fragmented.[64] In particular publishers and record labels can now administer their rights themselves, having withdrawn them from the CMO system.[65] However, they have not withdrawn the works as a whole, but instead only the online rights. In other words, while the CMO may be able to license the work for broadcasting, it cannot do so for online exploitation. This fragmentation places a substantial burden on CMOs and right holders to keep track of who holds what right to which work. This task should not be underestimated.[66] Some CMOs themselves struggle to identify the specific works and rights that they administer.[67]

36 Secondly, by allowing not only CMOs but also independent rights management organisations (which focus on licensing without the collective component)[68] to administer rights, the Directive has effectively endorsed the licensing Hubs. Given the demand for multi-territorial licenses, CMOs have had to cooperate with each other and with major publishers to offer multi-territorial licenses. While these Hubs are managed by the CMOs, they are distinct from them. This means that rather than competing with each other to offer multi-territorial licenses, CMOs are being hired by right holders to do this via a clearing house system. It also means that the usual social and collective features of the CMO, a key element in the justification of their existence is being marginalised.

37 In sum, the remedy which was supposed to bring about CMOs to provide multi-territorial licenses has instead cemented a fragmented system where it is not clear what a license covers. Right holders have got the power to choose where to register their rights. Their decision will be determined both by the nature and offerings of those who are willing to have the rights registered to them and the users of the services of those organisations, such as the streaming services themselves and their consumers. While it is unhelpful to look at this market through the lens of the theory of two-sided markets, it is important to keep in mind that to achieve the best

64 Cooke, Dissecting the Digital Dollar, Part One: How streaming services are licensed and the challenges artists now face (London: Music Managers Forum., 2015)

65 Arezzo , Competition and Intellectual Property Protection in The Market for the Provision of Multi-Territorial Licensing of Online Rights in Musical Works – Lights And Shadows of The New European Directive 2014/26/EU, International Review Of Intellectual Property And Competition Law 2015, 545, Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (Directive 2014/26/EU) (CMO Directive), Part III.

66 In this respect some may argue that the CMOs are simply left with the wrong "technology", i.e. databases, which may make the intervention by the Commission look harsh. An unresolved question is whether the CMOs have been less innovative than on other sectors because they were part of a set of cosy monopolists or because there are some issues which make it fundamentally harder to bring music into the 21st century.

67 Ranaivoson, Iglesias, and Vondracek, The Costs of Licensing for Online Music Services: An Exploratory Analysis for European States. Michigan State International Law Review 2013, 674.

68 CMOs license works and use some of their income for services to the membership as whole, including social insurances, pensions and cross-subsidising of genres. Rights management organisations license works and distribute the income to the right holders, without providing broader services like CMOs do. As a result, the cross-subsidising from successful to less successful right holders is significantly more limited.

financial outcome for the rights holders, creating appropriate bundles of music is clearly valuable.[69] In other words, there is a natural tendency to have CMOs that cover all works and represent all rights.

IV. Who Benefits?

38 In addition to the problems of rights fragmentation, there are questions concerning the benefit to be derived for the majority of authors. The clear winners of the changes are successful artists and large right holders, such as publishers and labels. They have the resources to administer their rights on their own.[70] This trend has been most recently confirmed by Arezzo who sees the publishers as exploiting the new options.[71] Withdrawal of rights in order to ensure efficient administration is not a realistic option for most right holders, a problem that is compounded by the fact that CMOs are not required to use a common language.

39 In addition to the practical and technical issues not addressed by the Directive, the Commission has a highly simplistic view of author preferences. It does not allow for how interests within the right holder group may differ. Larger right holders have an interest in leaving because, for them, economic performance is key.[72] Successful artists and commercial copyright holders have an interest in generating revenue compared to a less successful artist who may rely on a wider distribution of their works in order to generate a fan base.[73] In terms of rights administration, this translates into the larger owners preferring efficiency above other services that CMOs provide (for example, social insurance).

40 Following the Commission's logic, relying on increased competition protected through competition law can make CMOs focus both on generating faster, more accurate practices, as well as lowering overheads. However, there is no accepted measure for CMO performance[74] and therefore neither for "efficiency". The one figure indicating the cost of rights administration for the copyright owner is the administration rate. It measures the percentage of royalties that are used for administration and indicates its relative cost. This is the only directly comparable figure which the CMO Directive requires to be published.[75] Therefore, for copyright holders focusing on economic value a lower administration rate is more attractive.

41 However, the reliance on administration rates has two major drawbacks. First, in a world where there is a choice between CMOs, this would seem an inadequate measure of performance. Having a measure which focuses solely on the cost side is rather limited, since an artist is interested in the absolute amount of money they receive. To be satisfied with the current measure would mean

69 Arezzo , Competition and Intellectual Property Protection in The Market for the Provision of Multi-Territorial Licensing of Online Rights in Musical Works – Lights And Shadows of The New European Directive 2014/26/EU, International Review Of Intellectual Property And Competition Law 2015, 534-564.

70 Ficsor, Collective Management of Copyright and Related Rights, WIPO 2002 (available at: <http://www.wipo.int/edocs/pubdocs/en/copyright/855/wipo_pub_855.pdf>, last accessed 15/4/16), 97,Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15), 10. They also have more lobbying power and it is important to be alert to the dangers that such lobbying power leads inappropriate regulation and potentially slower convergence.

71 Arezzo , Competition and Intellectual Property Protection in The Market for the Provision of Multi-Territorial Licensing of Online Rights in Musical Works – Lights And Shadows of The New European Directive 2014/26/EU, International Review Of Intellectual Property And Competition Law 2015, 534-564. For early predictions of this phenomenon, see Kretschmer et al, The Changing Location of Intellectual Property Rights in Music: A Study of Music Publishers, Collecting Societies and Media Conglomerates, Prometheus, 1999, 163- 186; the issue raised during the public consultation: Max Planck Institute for Intellectual Property and Competition Law, Comments on the Proposal for a Directive of the European Parliament and of the Council on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online uses in the internal market (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208971&download=yes>, last accessed 13/10/16), especially para. 17; and evidence that this is already happening: 1709 Blog, Is Universal Publishing's exit from collective licensing a step backwards for music industry 'one stop' aspirations? (available at: <http://the1709blog.blogspot.nl/2013/02/is-universal-publishings-exit-from.html>, last accessed 13/1/16).

72 This is a well-known problem for cooperatives – and at least for some aspects of the business model, one can equate a CMO with a marketing cooperative. When cooperatives have members with very diverse interests and aims, the cooperative tends to malfunction and the more powerful members tend to leave as they can do better on their own. See e.g. Henriksen, Ingrid, Morten Hviid and Paul Sharp, 2012, Law and peace: Contracts and the success of the Danish dairy cooperatives. The Journal of Economic History 72, 197-224.

73 Kretschmer, Digital Copyright: the End of an Era. European Intellectual property Review 2003, 333-341.

74 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15), 6.

75 Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (Directive 2014/26/EU) (CMO Directive), art 22 and Annex. All of the other indicators which need to be published are in absolute numbers, making them not directly comparable across CMOs. For example, the collected revenue strongly depends on the membership size, making the absolute value in Euros a relative figure.

always preferring a CMO which had low costs, but which generated very little revenue, to one with high costs but also high revenue.

42 Secondly, if CMOs choose to compete, as the Commission intends, it would be on the basis of the administration rate as an indicator of economic efficiency. This would attract the right holders with the most valuable repertoire. The administration fee is currently the same, irrespective of the actual cost of collection. However, as more successful works are easier to administer in practice, larger right holders are cross-subsiding less successful ones.[76] They therefore have an incentive to leave and as a result, the cross-subsidy is likely to unravel.[77] CMOs seeking to prevent this are more prone to the influence of these larger right holders. As their threat to exit is also the most credible, it will enhance their influence within CMOs.[78] As CMOs have in practice significant leeway in determining both the tariffs as well as the distribution policies,[79] smaller right holders are more likely to be losing out.

43 A possible casualty of a more economic/competition approach in this market is the demise of the social and cultural features of the old CMOs. These required a cross subsidy between artists. With the focus on the economic value of the organisation, the incentive to provide these subsidies will decrease. CMOs with a stronger social component would be left with repertoire of a lower market value, raising the costs per work even more.[80] At the same time, it is hard to see the justification for these services being bundled with the other activities of a CMO and being protected through competition law. Channelling the funds from online exploitation and bypassing the established CMO system is likely to work in the same way.

44 This situation feeds back into one of the main issues raised by the effect of copyright. Copyright protection, and especially its strengthening, is usually linked to the harm it does to creators, rather than to the larger corporations which do not create works, but exploit them. This concern derives from the assumption of "the romantic author": the lone creator who works independently.[81] This paradigm is further reinforced by the language used to describe unauthorised use, most notably the moral condemnation of piracy.[82] A similar argument has been made in relation to the term "extension for performers". Famous artists, such as Sir Cliff Richard, have actively lobbied on this basis.[83] However, as the licensing regime moves away from income from shared performance rights as CMOs guarantee,[84] the benefits to the creator are further undermined. The fear is that the regime is increasingly serving the interests of the large stakeholders, whether corporate or individual.[85]

H. Conclusion

45 Our empirical investigation clearly shows that the current system in place for online music licenses is falling significantly short of the Commission's aims.[86] First, it is nearly impossible to determine who can offer an online license, and which works and territories it covers. The information asymmetry faced by users has been made even more problematic by Hubs with limited coverage because it increases the number of relevant players. (This issue has been

76 Wallis, Kretschmer and Klimis, Contested Collective Administration of Intellectual Property Rights in Music- The Challenge to the Principles of Reciprocity and Solidarity, European Journal of Communication 1999, 14-15.

77 Competition typically leads to an unravelling of cross subsidies.

78 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15), 10.

79 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15), 6.

80 Handke and Towse, Economics of Copyright Collecting Societies, SSRN 2007 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159085>, last accessed 14/12/15), 10.

81 For a more detailed description, see Rose, Authors and Owners (London: Harvard University Publishing, 1993) and Campbell, Authorship, incentives for Creation and Copyright in the 21st Century, Proceedings of the American Society for Information Science and Technology 2006.

82 Ricketson and Ginsburg, International Copyright and Neighbouring Rights- The Berne Convention and Beyond (Oxford: Oxford University Press, 2006), 21.

83 Atkinson, Sir Cliff Richard's victory: an extra 20 years of copyright protection for sound recordings is only weeks away (available at: <http://www.technology-law-blog.co.uk/2013/08/sir-cliff-richards-victory-an-extra-20-years-of-copyright-protection-for-sound-recordings-is-only-we.html>, last accessed 17/12/15).Cliff Richard does not write songs, he only performs them. This makes him a performer but not an author under copyright law. However, it shows how the notion of creativity has expanded over time.

84 Most commonly, the income is divided 1:1:1 between the composer, lyricist and publisher, with payments directly to the right holder.

85 For a detailed empirical analysis of copyright reforms from this angle, see Schroff, The evolution of copyright policies (1880-2010): a comparison between Germany, the UK, the US and the international level. Doctoral thesis at the University of East Anglia 2014 (available at <https://ueaeprints.uea.ac.uk/49708/>, last accessed 15/4/16).

86 The same is true for the sales of digital music, see Gómez and Martens, Language, Copyright And Geographic Segmentation in the EU Digital Single Market for Music and Film, JRC/IPTS Digital Economy Working Paper 2015, (available at <http://ssrn.Com/Abstract=2603144>, last accessed 15/4/16).

known for at least a decade, yet no obvious solution has emerged). Secondly, the price of licenses is also unknown. While a system of tariffs is supposed to reduce the transaction costs by addressing the information asymmetry, this is not the case for online licenses. Standard online licenses are not pan-European. At the same time, there is virtually no information available on the cost of pan-European licenses as granted by Hubs. Thirdly, rather than competing with other CMOs, they are hiring out their administrative capabilities to large scale right holders, in particular publishers. All of the major Hubs are associated and run out of the offices of a major CMO, in particular PRS, GEMA, SACEM and SGAE. Their changes are not aimed at the individual creator but instead large intermediaries. As these Hubs are separated from the CMOs, the revenue they generate is separate too, and may therefore not contribute to the social/cultural aspects of the CMOs' work. In other words, CMOs are helping large right holders to channel income past the established system. As the major CMOs are already complying with the CMO Directive's provisions on multi-territorial licensing, we are left to ask: what is wrong with the EU's attempt to meet the demands of digitalisation?

46 The current insistence on rights being entrusted by the right holder to a single CMO exacerbates the problems. Right holders are unable to create competition through multi-homing. As Katz argues, CMOs were not necessarily natural monopolies under the analogue regime and are even less likely to be so under the new digital regime.[87] Some components, such as the databases of works and right holders may be, but the collection of revenue and the single assignment of rights clearly need not be. Because there is a strong commercial interest on the part of all stakeholders to have a comprehensive CMO — at least within genres — monopolies are likely to emerge naturally. It is difficult to see how competition will remain. Whether this will ultimately lead all to be in the same organisation or bodies organised along the lines of a particular repertoire is difficult to predict. One thing which seems abundantly clear is that national organisations are unlikely to survive. By allowing right holders to assign their rights in any way they want, but not permitting simultaneous assignment,[88] the result is likely to be a new system of monopolies or oligopolies. The only difference will be the basis of the distinction, from national monopolies to repertoire-based ones.

47 Our reading of the Directive and our case studies suggest that:

- By mis-conceptualising CMOs, the remedies to ensure more competition have had unintended effects – for instance, the creation of clearing houses managed by CMOs rather than competition between CMOs;
- The Directive does not go far enough — rights are still assigned on an exclusive basis and therefore cannot be assigned to several agents at the same time;[89]
- In the matter of non-exclusive rights assignment several CMOs can license a work, so the user is not detrimentally affected; at the same time, right holders can exclude some badly managed CMOs, while remaining within the licensing regime.

48 Our research has also enabled us to identify a number of further questions:

- Given that licensing is intimately linked to the copyright system, should the copyright system be reformed to accommodate changes in licensing - in particular, for the protection of consumers and less successful authors?
- Are performing rights and their licensing really different from other works and rights (for example, e-books)?
- What problems should a reformed licensing system address? Is streaming equivalent to other disruptive technologies and/or initiatives in other markets such as Uber and Airbnb?

49 Given the importance of licensing practice to the

87 Katz, The potential demise of another natural monopoly: Rethinking the collective administration of performing rights, Journal of Competition Law and Economics 2015, 541-593, Katz, The potential demise of another natural monopoly: New technologies and the administration of performing rights. Journal of Competition Law and Economics 2006, 245-284.

88 Under article 31 CMO Directive, simultaneous assignment is possible in the very limited circumstances that the CMO which usually administers the online use of works does not offer multi-territorial licenses and has not mandated another CMO to do so under the passport system. However, even in this case the multi-territorial online use cannot only be assigned to one other CMO. It is therefore still a single CMO which can provide the license in practice.

89 It is not required by the Directive that the same right for the same work is assignable to more than one CMO. Indeed, exploitation contracts explicitly prevent this. See for example: BUMA/ STEMRA, Exploitatiecontract A (auteur) (available at: <http://www.bumastemra.nl/wp-content/uploads/2015/05/PV2.BUM_.512.0914.08-A3-SPEC-Exploitatiecontract-A-auteur-def.-d.d.-03.10.2014.pdf>, last accessed 13/10), art 2(3) or GEMA, Berechtigungsvertrag (Fassung April 2016) (available at: <https://www.gema.de/fileadmin/user_upload/Gema/Berechtigungsvertrag.pdf>, last accessed 13/10/16), art. 1 and 1a; PRS for Music, Articles of Association (available at: <https://www.prsformusic.com/SiteCollectionDocuments/About%20MCPS-PRS/prs-memorandum-articles.pdf>, last accessed 13/10/16), art. 7.

legitimacy and effectiveness of copyright more broadly, linking the two directly at EU level is a potential avenue of fruitful reform. Although beyond the scope of this paper, future research should investigate how the effect of copyright is shaped by the licensing process. Key to this is the current absence of copyright contract law rules to cushion the effect of changes in the licensing practices for less successful artists. Furthermore, research should investigate the option of resorting to harmonisation (potentially in combination with a re-adjusted competition approach), as was done in areas of protection to standardise licensing practices and the availability of licenses across borders. Examining the effects of copyright in this context is especially important, given the on-going EU copyright review.

* *Morten Hviid* is the Director of the Centre For Competition Policy, a member of CREATe and UEA Law School, University of East Anglia, Norwich NR7 4TJ, UK. *Simone Schroff* is an associated researcher with CREATe and a member of the Institute for Information Law, University of Amsterdam, Vendelstraat 7, 1012 XX Amsterdam, The Netherlands. *John Street* is a member of CREATe, the Centre for Competition Policy and the School of Politics, Philosophy, Language and Communication Studies, University of East Anglia, Norwich NR7 4TJ, UK.
We would also like to acknowledge RCUK Centre for Copyright and New Business Models in the Creative Economy (CREATe) for funding this project. Any remaining errors are ours.

Liability under EU Data Protection Law

From Directive 95/46 to the General Data Protection Regulation

by **Brendan Van Alsenoy***

Abstract: This article analyses the liability exposure of organisations involved in the processing of personal data under European data protection law. It contends that the liability model of EU data protection law is in line with the Principles of European Tort Law (PETL), provided one takes into account the "strict" nature of controller liability. After analysing the liability regime of Directive 95/46, the article proceeds to highlight the main changes brought about by the General Data Protection Regulation. Throughout the article, special consideration is given to the nature of the liability exposure of controllers and processors, the burden of proof incumbent upon data subjects, as well as the defences available to both controllers and processors.

Keywords: Data protection; controller; processor; Directive 95/46; General Data Protection Regulation; GDPR; Principles of European Tort Law; PETL; liability

Recommended citation: Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 (2016) JIPITEC 271 para 1.

A. Introduction

1 Practically every organisation in the world processes personal data. In fact, it is difficult to imagine a single organisation which does not collect or store information about individuals.[1] European data protection law imposes a series of requirements designed to protect individuals when their data are being processed.[2] European data protection law also distinguishes among different types of actors who may be involved in the processing. As far as liability is concerned, the most important distinction is the distinction between "controllers" and "processors". The controller is defined as the entity who alone, or jointly with others, "determines the purposes and means" of the processing.[3] A "processor", on the other hand, is defined as an entity who processes personal data "on behalf of" a controller.[4] Together, these concepts provide the very basis upon which

1 Under EU data protection law, "personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject') [...]" (see art. 2(a) Directive 95/46; art. 4(1) GDPR). "Processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (art. 2(b) Directive 95/46; art. 4(2) GDPR).

2 P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Claes, Duff and Gutwirth (eds.), *Privacy and the Criminal Law* (Intersentia, 2006), p. 76. See also R. Gellert, "Understanding data protection as risk regulation", *Journal of Internet Law* 2015, p. 3-16.

3 Art. 2(d) Directive 95/46; art. 4(7) GDPR.

4 Art. 2(e) Directive 95/46; art. 4(8) GDPR.

responsibility for compliance is allocated. As a result, both concepts play a decisive role in determining the liability exposure of an organisation under EU data protection law.[5]

2 For almost 15 years, Directive 95/46 stood strong as the central instrument of data protection regulation in the EU.[6] In 2010, however, the Commission announced that the time for revisions had come.[7] The Commission considered that while the objectives and principles underlying Directive 95/46 remained sound, revisions were necessary in order to meet the challenges of technological developments and globalisation.[8] A public consultation conducted in 2009, revealed concerns regarding the impact of new technologies, as well as a desire for a more comprehensive and coherent approach to data protection.[9] During the consultation, several stakeholders also raised concerns regarding the concepts of controller and processor.[10] Various solutions were put forward, ranging from minor revision to outright abolition of the concepts. In the end, the EU legislature opted to retain the existing concepts of controller and processor in the General Data Protection Regulation (GDPR).[11] Notable changes were made however, with regards to the allocation of responsibility and liability among the two types of actors.

3 The aim of this article is two-fold. First, it seeks to clarify the liability exposure of controllers and processors under EU data protection law. Second, it seeks to highlight the main differences between Directive 95/46 and the GDPR regarding liability allocation. The article begins by analysing the liability regime of Directive 95/46. The primary sources of analysis shall be the text of the Directive itself, its preparatory works, and the guidance issued by the Article 29 Working Party. Where appropriate, reference shall also be made to the preparatory works of national implementations of the Directive (e.g. the Netherlands, Belgium), as a means to supplement the insights offered by the primary sources. Last but not least, the Principles of European Tort Law (PETL), as well as national tort law, will be considered for issues not addressed explicitly by Directive 95/46.[12] The second part of this article will analyse the liability regime of the GDPR. Here too, the analysis shall be based primarily on the text of the GDPR itself, its preparatory works, and the Principles of European Tort Law.

B. Directive 95/46: a "strict" liability regime for controllers

4 Under Directive 95/46, a controller is, as a matter of principle, liable for any damages caused by the unlawful processing of personal data. Article 23(1) stipulates that Member States must provide that the controller shall be liable towards data subjects for any damages suffered as a result of an unlawful processing operation. A controller may be exempted from liability, however, in whole or in part, "if he proves that he is not responsible for the event giving rise to the damage" (article 23[2]). Directive 95/46 does not contain any provisions regarding the liability exposure of processors. While article 16 stipulates that processors may only process the data in accordance with the instructions of the controller, the Directive does not explicitly allocate liability in case of a disregard for instructions.

5 Unfortunately, the distinction between controllers and processors is not always easy to apply in practice. For a more detailed discussion see B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *Computer Law & Security Review* 2012, Vol. 28, p. 25-43.

6 The European Commission assessed its implementation in 2003 and 2007, both times concluding there was no need for revisions. See COM (2003) 265, "Report from the Commission - First Report on the implementation of the Data Protection Directive 95/46/EC)", at 7 and COM (2007)87, "Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive", p. 9.

7 COM(2010) 609, "A comprehensive approach on personal data protection in the European Union", p. 2.

8 *Ibid*, p. 3.

9 COM(2010) 609, "A comprehensive approach on personal data protection in the European Union", p. 4.

10 See e.g. Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data" (2009), p. 2-3; International Chamber of Commerce (ICC), ICC Commission on E-business, IT and Telecoms, "ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data" (2009), p. 4; Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data" (2009), at paragraph 19 and European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework" (2009), p. 5.

11 The definitions of controller and processor contained in the GDPR are quasi identical to the definitions contained in Directive 95/46. Only minor linguistic edits were made, none of which brought about a substantive change to the definitions.

12 It should be noted that, as an academic piece, the PETL do not enjoy legal authority as such. Nevertheless, the PETL offer an interesting frame of reference when assessing any regulation of liability at European level, as they reflect what leading scholars have distilled as "common principles" for European tort law liability. For additional information see <http://www.egtl.org>.

I. Controller liability

1. Nature of controller obligations

5 To properly understand the liability exposure of controllers, it is necessary to first understand the nature of controller obligations. Directive 95/46 imposes a variety of obligations upon controllers. In certain instances, the obligations specify a *result* to be achieved (e.g., "personal data must be collected for legitimate purposes and not further processed in a way incompatible with those purposes").[13] In other instances, the obligations are specified as an obligation to make *reasonable efforts* to do something ("obligation of means"). For example, article 6(1)d provides that the controller must take "every reasonable step" to ensure that data which are inaccurate or incomplete shall be erased or rectified. Similarly, article 17(1) requires the controller to implement "appropriate" measures to ensure the confidentiality and security of processing. Finally, it should be noted that certain requirements necessitate a further assessment in light of the specific circumstances of the processing (e.g., whether or not personal data are "excessive" will depend inter alia on the purposes of the processing). The precise nature of the controller's obligations must therefore always be determined in light to the specific wording of each provision.

6 Article 23(1) provides that the controller shall be liable towards data subjects for any damages suffered "as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive". The liability rule of article 23 has been characterised as a form of "strict" (i.e. "no fault") liability.[14] The reason for this characterisation is the finding that the controller cannot escape liability simply by demonstrating the absence of a "personal fault". Likewise, it is not necessary for data subjects to demonstrate that the unlawful act was personally committed by the controller.[15] One should be careful however, to not overstate the "strict" nature of controller liability.[16] Even though the data subject is not required to demonstrate a "personal fault" on the part of the controller, he or she must in principle still succeed in proving the performance of an "unlawful act".[17] Demonstration of an "unlawful act" generally amounts to a demonstration of "fault" for tort law purposes.[18] Conversely, if the controller can establish that the processing complies with the requirements of the Directive, he will effectively exempt himself from liability on data protection grounds.[19] The characterisation of controller liability as "strict" liability (i.e. the notion that a controller may be still be held liable in absence of a personal fault) is therefore mainly relevant in relation to (1) controller obligations which impose an obligation of result; and (2) the liability of a controller for acts committed by his processor.

2. Non-delegable duty of care

7 Under Directive 95/46, the controller has a general duty to ensure compliance. Because the processor is seen as a "mere executor", who simply acts in accordance with the instructions issued by the controller, the Directive maintains that the responsibility for ensuring compliance remains with the controller. The mere fact that the unlawful action was performed by the processor rather than the controller does not diminish the controller's

13 Art. 6(1)b Directive 95/46.

14 Instruments of Parliament (Belgium), Memorie van Toelichting, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer, 1990-1991, 6 May 1991, nr. 1610-1, p. 54 and D. De Bot, *Verwerking van persoonsgegevens* (Kluwer, 2001), p. 241. See also T. Léonard and Y. Poullet, "La protection des données à caractère personnel en pleine (r)évolution", *Journal des Tribunaux* 1999, p. 394 at nr. 65. Certain authors also refer to the "objective liability" of the controller. Although the terms "strict" and "objective" appear to be used interchangeably at times, some authors associate different legal consequences to the respective terms. For purposes of conceptual clarity, only the term "strict liability" shall be used in this article.

15 Instruments of Parliament (Belgium), op. cit. supra note 14 and D. De Bot, op. cit. *supra* note 14.

16 See also E. Reid, "Liability for Dangerous Activities: A Comparative Analysis", *The International and Comparative Law Quarterly* 1999, p. 736-737 (noting that strict liability is not always "stricter "than fault-based liability, particularly in cases where the circumstances giving rise to liability coincide in large measures with those used in negligence analysis) and E. Karner, "The Function of the Burden of Proof in Tort Law", in Koziol and Steininger (eds.), *European Tort Law 2008* (Springer, 2009), p. 76-77 (arguing that in practice "fault-based" liability and "strict" liability are not two clearly distinct categories of liability, but rather two extremes in a continuum, with many variations between them as regards the possibility of exculpation).

17 See also *infra*; section B.I.3. See also Tweede Kamer der Staten-Generaal (Netherlands), Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *Vergaderjaar* 1997-1998, 25 892, nr. 3, p. 176.

18 See art. 4:101 and 4:102(3) of the Principles of European Tort law (PETL): "A person is liable on the basis of fault for intentional or negligent violation of the required standard of conduct" and "Rules which prescribe or forbid certain conduct have to be considered when establishing the required standard of conduct.") See however also V. Ulfbeck and M.-L. Holle, "Tort Law and Burden of Proof – Comparative Aspects. A Special Case for Enterprise Liability?", in H. Koziol and B.C. Steininger (eds.), *European Tort Law 2008* (Springer, 2009), p. 35-36.

19 See also Judgment of 19 June 2003, Kh. Kortrijk, 1st Ch. (Belgium), (2007) *Tijdschrift voor Gentse Rechtspraak*, p. 96.

liability exposure.[20] The controller shall in principle be liable for any violation of the Directive resulting from the operations carried out by a processor acting on its behalf ("as if they were performed by the controller"). In other words, Directive 95/46 imposes upon controllers a "non-delegable duty of care": the duty of care that a controller owes data subjects cannot be transferred to an independent contractor.[21]

8 A controller cannot escape liability for actions undertaken by its processors by demonstrating an absence of fault in either his choice or supervision of the processor.[22] This is a consequence of the strict liability imposed upon controllers: a controller can only escape liability by demonstrating that the processing complies with the requirements of the Directive or by proving an "event beyond his control" (article 23[2]).[23] The EU legislator chose to attach liability to the quality of a person as data controller (*qualitate qua*), without making any reference to possible exemptions other than the one mentioned in article 23(2).[24]

9 The liability of the controller for the actions performed by its processor is similar to the vicarious liability of a principal for the actions undertaken by its auxiliaries, whereby "a person is liable for damage caused by his auxiliaries acting within the scope of their functions provided that they violated the required standard of conduct".[25] In case of processors, however, the relationship with the controller in principle is not hierarchical in nature. While the processor is legally prohibited from processing the data "except on the instructions of the controller", he is not necessarily a "subordinate" of the controller.[26] As a result, the processor will in principle not be formally considered as an "auxiliary" of the controller for tort law purposes, although the outcome may be similar in practice.[27]

3. Burden of proof

10 To hold a controller liable, the data subject must succeed in demonstrating three elements: namely (1) the performance of an "unlawful act" (i.e. an unlawful processing operation or other act incompatible with the national provisions adopted pursuant to the Directive); (2) the existence of damages; and (3) a causal relationship between the unlawful act and the damages incurred.[28] In addition, the data subject

20 See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17 and C. De Terwangne and J.-M. Van Gyseghem, "Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution", in C. De Terwangne (ed.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, p. 125.

21 Compare Reid, op. cit. *supra* note 16, p. 752-753 (explaining that a principal may be liable for the negligence of its contractors in cases where the law imposes a non-delegable duty of care). Liability for breach of non-delegable duty of care is not the same as vicarious liability, although the two can easily be confused. In case of vicarious liability, liability is "substitutional", whereas in case of a non-delegable duty of care, liability is personal (i.e. originates from a duty which is personal to the defendant). For a more detailed discussion see C. Witting, "Breach of the non-delegable duty: defending limited strict liability in tort", 2006 *University of New South Wales Law Journal*, p. 33-60.

22 Contra: U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft, 1997), p. 264 (arguing that the intent of the European legislator was to exempt the controller not only in case of force majeure but also in cases where the controller had taken all the appropriate measures required by art. 17).

23 Cf. *infra*; section B.I.4.

24 The legislative history of 23(2) makes clear that the EU legislator intended to render the controller strictly liable for the actions committed by his processor by removing the reference to "suitable measures" (which had been present in both the initial and amended European Commission proposal) and by limiting the possible defense of the controller to "events beyond his control", such as force majeure. It stands to reason that the EU legislator thus deliberately chose to derogate from the general principle that a person shall not be liable for the actions performed by independent contractors. See also *infra*; note 38. Compare also with art. 7:102 of the Principles of European Tort Law (PETL) ("Strict liability can be excluded or reduced if the injury was caused by an unforeseeable and irresistible (a) force of nature (force majeure), or (b) conduct of a third party.").

25 Art. 6:102 of the Principles of European Tort Law (PETL). See also C. von Bar a.o. (eds.) "Principles, Definitions and Model Rules of European Private Law - Draft Common Frame of Reference (DCFR)", Study Group on a European Civil Code and the Research Group on EC Private Law, 2009, p. 3318 et seq.

26 Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 61. While art. 17(2) Directive suggests that the controller must supervise "the processor's implementation of organisational and security measures (by using the phrasing "and must ensure compliance with those measures"), the Directive does not bestow upon the controller a general power of instruction or supervision.

27 Needless to say, in cases where the processor is a natural person, it may not be excluded that he or she might *de facto* operate in a hierarchical relationship with the controller, despite being labelled as an "independent contractor" in his or her contract with the employer. In cases where the person carrying out the services should legally be qualified as an "employee" rather than an "independent contractor", he or she will of course be treated as an "auxiliary" for tort law purposes.

28 D. De Bot, "Art. 15bis Wet Persoonsgegevens", in X., *Personen- en familierecht. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer* (Kluwer, 2001), looseleaf. See also Raad van State (Belgium), Advies van de Raad van State bij het voorontwerp van wet tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij Verkeer van die gegevens, 2 February 1998, *Parl. St.* Kamer 1997-1998, nr. 1566/1, p. 145. See also U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 264. It should be noted that certain authors consider that it may be sufficient for the data subject

must also establish, as a preliminary matter, that the defendant is (or was) acting as the "controller" of the processing.[29]

11 The burden of proof incumbent upon data subjects can be quite onerous. First, identifying the controller of the processing at issue may be a complicated exercise, especially where more than one party is involved in the processing. Second, demonstrating the performance of an "unlawful act" may also be a challenge, particularly in cases where the Directive specifies an obligation of means (rather than an obligation of result), or requires further interpretation (e.g., an assessment of proportionality).[30] Demonstrating causality can also be difficult especially in cases where a particular outcome may be caused by different factors. For example, it may be difficult to prove that the unlawful collection of information (e.g., information regarding the ethnicity of a loan applicant) actually caused the damages to occur (e.g., the denial of a loan may be attributed to many different factors).[31] Finally, demonstrating recoverable damages (e.g., loss of reputation, emotional distress) can also be a challenge.[32]

12 A major difficulty for data subjects is that the evidence relevant to their case is often only accessible to the controller or its processor. Because personal data processing is generally conducted "behind closed doors", it can be difficult for data subjects to obtain solid evidence substantiating their claims.[33] Depending on the facts at hand however, the data subject may be able to invoke a *presumption* or other *judicial construct* with similar effect to help substantiate its claim. For example, in a case involving the unauthorised disclosure of personal data, the European Union Civil Service Tribunal has considered that the burden of proof incumbent upon the applicant may be relaxed:

> *"in cases where a harmful event may have been the result of a number of different causes and where the [defendant] has adduced no evidence enabling it to be established to which of those causes the event was imputable, although it was best placed to provide evidence in that respect, so that the uncertainty which remains must be construed against it".*[34]

13 The reasoning of the Civil Service Tribunal can be seen as an application of the so-called "proof-proximity principle", which allocates the evidential burden of proof on the party to whom the evidence is available, or whomever is better situated to furnish it easily and promptly.[35] Another judicial construct which may benefit certain data subjects is the adage of "*res ipsa loquitur*" ("*the thing speaks for itself*"), pursuant to which negligence may be inferred in cases where the harm would not ordinarily have occurred in the absence of negligence.[36] It should be

demonstrate the performance of an "unlawful act" and the existence of damages in order to hold the controller liable, without additionally requiring a demonstration of a causal relationship between the unlawful act and the damages suffered. See e.g. C. De Terwangne and J.-M. Van Gyseghem, "Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution", in C. De Terwangne (ed.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, p. 125. In my view, this interpretation runs counter to the literal wording of article 23(1) of the Directive, which stipulates that the controller is obliged to indemnify the data subject for damages suffered "*as a result of*" an unlawful processing operation. As will be discussed later however, there exist certain judicial constructs through which the evidentiary burden of the data subject in this respect may be alleviated.

29 See also C. von Bar a.o. (eds.) op. cit. *supra* note 25, p. 2994, at paragraph 31 ("The axiom [...], as far as tort law is concerned, is as far as tort law is concerned, is that the plaintiff must plead/establish and prove all of the requirements pertaining to his claim, in particular damage, grounds of liability and causation save where express regulations permit departures from this rule, whereas it is incumbent upon the defendant to show and prove certain requirements which give rise to a ground of defence, thereby displacing the claimant's assertions"). See also the Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43, paragraph 161 and the Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254, paragraph 141.

30 T. Léonard and Y. Poullet, op. cit. *supra* note 14, 394 at nr. 65 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf.

31 *Id.* De Bot indicates the doctrine of "loss of a chance" might be useful in this respect: see D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf. For a comparative discussion of the "loss of a chance" doctrine see V. Ulfbeck and M.-L. Holle, op. cit. *supra* note 18, p. 40-43.

32 See also P. Larouche, M. Peitz and N. Purtova, "Consumer privacy in network industries – A CERRE Policy Report, Centre on Regulation in Europe, 25 January 2016, p. 58, available at <http://cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf> (last accessed 6 November 2016).

33 P. De Hert, V. Papakonstantinou, D. Wright and S. Gutwirth, "The proposed Regulation and the construction of a principles-driven system for individual data protection", *The European Journal of Social Science Research* 2013, p. 141.

34 Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43, paragraph 161. See also the Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254, paragraphs 141-142.

35 C. Volpin, "The ball is in your court: Evidential burden of proof and the proof-proximity principle in EU competition law", *Common Market Law Review* 2014, p. 1173-1177. See also E. Karner, "The Function of the Burden of Proof in Tort Law", op. cit. *supra* note 16, p. 72-73.

36 See V. Ulfbeck and M.-L. Holle, op. cit. supra note 18, p. 32-35; F.E. Heckel and F.V. Harper, "Effect of the doctrine of res ipsa loquitur", *22 Illinois Law Review*, p. 724-725 and F. Dewallens and T. Vansweevelt, *Handboek gezondheidsrecht Volume I*, 2014, Intersentia, p. 1329. While the doctrine of *res ipsa loquitur* appears similar to reasoning of Civil Service Tribunal, there is a difference: the presumption of the Civil Service Tribunal pertained to the *attribution* of an act of negligence, whereas *res ipsa loquitur* concerns the *existence* of negligence. In case of *res ipsa loquitur* however, the requirement of attribution shall also be satisfied as one of the conditions for application of the doctrine is that the object which caused harm was under the exclusive control of the defendant *(Id.)*.

noted however, that the ability for the data subject to avail him- or herself of a particular presumption or construct, may vary according to the domestic legal system of each Member State.

4. Defences

14 Article 23(2) stipulates that "the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage". The question inevitably arises as to the nature of the evidentiary burden of proof incumbent upon controllers. Which evidence must controllers offer to successfully exempt themselves from liability, either for their own actions or for the actions performed by their processors or auxiliaries?

15 In order to prove that he is "not responsible for the event giving rise to the damage", the controller must demonstrate three things: (1) the occurrence of an event; (2) which caused the damage; and (3) which cannot be attributed to the controller.[37] In principle, mere demonstration of an absence of fault on the part of the controller is not sufficient.[38] Once it is established that the damage was caused by an unlawful processing operation, the controller can only escape liability by demonstrating that the damages occurred only as the result of an event that cannot be attributed to him.[39]

16 The wording "not responsible for the event giving rise to the damage" recalls the concept of an "external cause" or "event beyond control", which in many jurisdictions is accepted either (1) as a justification ground excluding fault, or (2) as a means to demonstrate the absence of a causal relationship.[40] According to the Draft Common Frame of Reference, an event beyond control is "an abnormal occurrence which cannot be averted by any reasonable measure" and which does not constitute the realisation of a risk for which the person is strictly liable.[41] The aim of the liability exemption is therefore not to reduce the "strict" liability of the controller. Rather, its aim is to keep the strict liability within the borders of the risk for which it exists.[42] Recital (55) provides two examples of events for which the controller cannot be held responsible: namely, (1) an error on the part of the data subject;[43] and (2) a case of force majeure.[44][45]

37 This point was emphasized by the Belgian Council of State during its evaluation of the bill implementing Directive 95/46. See Raad van State (Belgium), op. cit. *supra* note 28, p. 145.

38 *Ibid*, p. 146. During the legislative history of Directive 95/46, the escape clause of art. 23(2) underwent several revisions. In the initial Commission proposal, the escape clause provided that the controller of the file would not be liable for damages resulting from the loss or destruction of data or from unauthorized access if he could prove that he had taken "appropriate measures" to comply with requirements of art. 18 and 22 (security and due diligence). (COM(90) 314, "Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security", p. 40.) The European Parliament amended the text to state that the controller must compensate the data subject for any damage "resulting from storage of his personal data that is incompatible with this directive." (O.J. 1992, C 94/192, "Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992" (First Reading), p. 192. The Parliament's proposed change had the effect of removing the escape clause contained in the initial Commission proposal. The European Commission felt strongly however, that the Member States should be able to exempt controllers from liability, if only in part, for damage resulting from the loss or destruction of data or from unauthorized access "if he proves that he has taken suitable steps to satisfy the requirements of Art. 17 and 24." (O.J. 1992, C 311/54, COM (92) 422, "Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", p. 54. In the end, the issue was settled by the Council, which drafted the final version of 23(2), which provides that: "The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage." The Council clarified the meaning of art. 23(2) by way of a recital which stipulated that "[...] whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he reports an error on the part of the data subject or in a case of force majeure".

39 See in the same vein also M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", (2015) *University of Hong Kong Faculty of Law Research Paper*, No. 2015/45, p. 23-24 (noting that the language of art. 23(2) does not concern itself with the imputation of fault or culpability to the controller, but with the imputation of the facts themselves).

40 See C. von Bar a.o., op. cit. *supra* note 25, p. 3538 et seq. and art. 7:102 of the Principles of European Tort Law (PETL) (defences against strict liability).

41 *Id.*

42 C. von Bar a.o., op. cit. *supra* note 25, p. 3539.

43 The reference to "an error on the part of the data subject" recalls the concept of "contributory negligence" or "contributory fault", whereby a victim whose own faulty behaviour has contributed to the occurrence of his own damage, is not entitled to compensation to the extent that his behaviour contributed to the damage. See von Bar a.o., op. cit. *supra* note 25, p. 3475-3500 and p. 3539. See also H. Cousy and D. Droshout, "Fault under Belgian Law", in P. Widmer (ed.), *Unification of Tort Law: Fault*, Kluwer Law International, 2005, p. 36.

44 "*Force majeure*" or "*Act of God*" can be described as an unforeseeable and unavoidable event which occurs independent of a person's will. For a discussion of the specific requirements for *force majeure* in different Member States see C. von Bar a.o., op. cit. *supra* note 25, p. 3540 et seq.

45 According to the parliamentary works relating to the implementation of Directive 95/46 into Belgian law, other events which cannot be attributed to the controller can

17 Article 23(2) of Directive 95/46 provides the only valid defence for controllers once the data subject has satisfied its burden of proof. In practice, controllers will not wait until the burden of proof shifts to them. Most controllers will try to ward off liability by arguing that the conditions of liability are simply not met, e.g. by demonstrating the absence of illegality in the processing. Again, the nature of the controller obligation at issue will be determinative here. Where an obligation of means is concerned, controllers can effectively avoid liability by demonstrating that they implemented every reasonable measure that might be expected of them. Even where an obligation of result is involved, controllers may seek to avoid liability by reference to the *Google Spain* ruling, where the Court of Justice indicated that there may also be practical considerations which limit the responsibilities of controllers.[46] In particular, when qualifying search engine providers as "controllers", the Court of Justice indicated that there may be practical limits to the scope their obligations:

> *"[...] the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 [...]".*[47]

18 By explicitly referring to the "powers and capabilities" of the search engine operator, the Court of Justice implicitly acknowledged that there may be practical limits to the ability of a search engine operator to meet all the obligations resulting from Directive 95/46.[48] In particular, it can be argued that *Google Spain* does not oblige search engine providers to exercise preventative control over the information it refers to.[49] In fact, the reasoning of the Court of Justice suggests that the obligations of search engine providers concerning third-party data is essentially only "reactive"; only after the provider has been made aware of the fact that the display of specific search results following a name search adversely impacts the data subject, must the provider assess whether or not delisting is necessary.[50]

5. Eligible damages

19 In principle, there is no restriction as to the type or amount of damages that data subjects may claim. Data subjects can claim both material (e.g., loss of a chance) and non-material damages (e.g. loss of reputation, distress).[51] Of course, the general rules on damages shall also apply here (e.g. personal interest, actual loss, etc.).[52]

II. Processor liability

20 Directive 95/46 does not contain any provision regulating the liability of processors. It also does not impose any obligations directly upon processors, with one exception: article 16 of Directive 95/46 requires the processor not to process personal data "except on the instructions from the controller". While Directive 95/46 does foresee additional obligations for processors, it envisages them as being

also be considered as a possible defence (e.g., the act of a third party for which the controller is not accountable). See Instruments of Parliament (Belgium), op. cit. *supra* note 14, p. 54 and D. De Bot, *Verwerking van persoonsgegevens*, op. cit. supra note 14, p. 241. Of course, the presence of a justification ground does not suspend the general duties of care of a controller. If the controller could have foreseen the damages and prevent them by taking anticipatory measures, normal rules of negligence apply. See also C. von Bar a.o., op. cit. *supra* note 25, p. 3538.

46 See also H. Hijmans, "Right to Have Links Removed - Evidence of Effective Data Protection", *Maastricht Journal of European and Comparative Law* 2014, p. 55 and Article 29 Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" (2014), WP 225, p. 6) ("The ruling does not oblige search engines to permanently carry out that assessment in relation to all the information they process, but only when they have to respond to data subjects' requests for the exercise of their rights."). These considerations are particularly relevant as regards the general prohibition to process certain "sensitive" categories of data, which is in principle formulated as an obligation of result.

47 Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 38, emphasis added.

48 For a more narrow reading see M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *supra* note 39, p. 26.

49 See also H. Hijmans, "Right to Have Links Removed - Evidence of Effective Data Protection", Maastricht Journal of European and Comparative Law 2014, p. 559 ("For me, it is obvious that this judgment does not mean that a search engine provider should exercise preventive control over the information it disseminates, nor that it is in any other manner limited in its essential role of ensuring a free internet. In essence, the Court confirms that a search engine – which has as its core activity the processing of large amounts of data with potentially important consequences for the private life of individuals –cannot escape from responsibility for its activities.").

50 See also Article 29 Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" (2014), WP 225, p. 6).

51 U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 263 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf. See also Court of Appeal (Civil Division), *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311 (27 March 2015), at paragraphs 70-79.

52 For a discussion of the general rules of damages under Belgian law see e.g. S. Stijns, *Verbintenissenrecht*, Boek 1bis, Die Keure, 2013, 101-104.

of a contractual nature. In particular, article 17(3) of Directive 95/46 provides that when a controller engages a processor to carry out certain processing operations on his behalf, their relationship must be governed by a contract or other legal act "binding the processor to the controller", which must specify that the processor is obliged (1) to follow the controller's instructions at all times, and (2) to implement appropriate technical and organisational measures to ensure the security of processing.[53] Article 17(3) mentions only the minimum content that should be included in an arrangement between controllers and processors. According to the Working Party, the contract or other legal act should additionally include "a detailed enough description of the mandate of the processor".[54]

21 The absence of a clear liability model for processors under Directive 95/46 begs the question of whether processors may be held liable by data subjects. In answering this question, a distinction should be made between two scenarios. In the first scenario (scenario A), the processor merely fails to give effect to the instructions issued by the controller (e.g., fails to implement the security measures instructed by the controller or fails to update information as instructed by the controller). In the second scenario (scenario B), the processor decides to process personal data for his own purpose(s), beyond the instructions received by the controller (in other words, to act outside the scope of his "processing mandate").

1. Scenario A: processor fails to implement controller instructions

22 In scenario A, the data subject shall in principle only be able to hold the processor liable on the basis of data protection law if this is provided by the national legislation implementing Directive 95/46.[55] Article 49(3) of the Dutch Data Protection Act, for example, provides that the processor can be held liable by data subjects insofar as the damages resulted from his activities.[56] In contrast, the Belgian Data Protection Act does not recognise a right for data subjects to hold processors liable as such. A data subject might nevertheless be able to hold a processor liable if he can demonstrate that the actions of the processor constituted "negligence" or violated another legal provision.[57] The standard of care incumbent upon the processor may, however, be informed by the contract between controller and processor.[58] In any event, the controller who has been held liable by the data subject, should be able to claim back the damages from the processor on the basis of the contract between them.[59]

2. Scenario B: processor acts outside of processing mandate

23 In scenario B, the processor does not merely fail to observe the instructions issued by the controller,

53 Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor'" (2010), WP 169, p. 26.

54 *Id*. See also U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 232 (noting that the contract or legal act should generally address all data protection issues including, for example, how to deal with access requests by governments or other interested third parties). In practice, the legal act binding the processor to the controller shall most often take the form of a contract. The reference to "other" legal acts in art. 17(3) mainly concerns the public sector, where a processor might be appointed either directly by way of legislation or by way of a unilateral decision of a public body. (U. Dammann and S. Simitis, op. cit. *supra* note 22, p. 231).

55 See also Article 29 Data Protection Working Party, op. cit. supra note 53, p. 28. ("*[W]hile the Directive imposes liability on the controller, it does not prevent national data protection laws from providing that, in addition, also the processor should be considered liable in certain cases.*").

56 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), *Staatsblad* 302 (Netherlands). See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 62 and p. 176. Another example of a national law which imposes liability directly upon processors is the Czech Data Protection Act (see art. 8 of Act No. 101/2000 Coll., on the Protection of Personal Data, 4 April 2000, English version accessible at <https://www.uoou.cz/en>).

57 D. De Bot, "Art. 15bis Wet Persoonsgegevens", op. cit. *supra* note 28, looseleaf. Generally speaking, it will be more appealing for the data subject to seek damages from the controller, because (a) the identity of the processor may not be known to the data subject (b) it will generally be more difficult for data subject to establish a violation of general duty of care by processor.

58 See e.g. A. De Boeck, "Aansprakelijkheid voor gebrekkige dienstverlening", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid* (Kluwer, 2008), II.3-84o-p. See also S. Demeyere, I. Samoy and S. Stijns, *Aansprakelijkheid van een contractant jegens derden - De rechtspositie van de nauw betrokken derde*, Die Keure, 2015, p. 37 et seq. The standard of care incumbent upon processor may in principle also be assessed in light of the professional occupation and knowledge of the processor: see e.g. H. Cousy and D. Droshout, "Fault under Belgian Law", op. cit. *supra* note 43, p. 32 and p. 39. In Belgium, plaintiffs may also need to consider the so-called "*rule of the (quasi-)immunity of the contractor's agent*" in cases where there is a contractual relationship between the controller and the data subject. This rule may further limit the data subject's ability to seek redress directly from the processor. If the action by the processor amounts to a crime however, such limitations will not apply. For more information see H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", in J. Spier (ed.), *Unification of Tort Law: Liability for Damage Caused by Others*, Kluwer law International, 2003, p. 50; S. Stijns, op. cit. *supra* note 52, p. 143 et seq.

59 See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 176.

but also decides to process the personal data for his own purposes. In such instances, the processor shall be considered to be acting as a controller in his own right, by virtue of determining his own "purposes and means" of the processing.[60] As a result, the (former) processor can be held liable in any event on the basis of national legislation implementing article 23 of Directive 95/46.[61] In principle, data subjects may also turn to the initial controller (who had entrusted the data to the (former) processor) for compensation. This is a result of the strict liability regime of article 23. The initial controller cannot escape liability by demonstrating an absence of fault in either his choice or supervision of the processor.[62] In practice, this means that the data subject will typically have the choice whether or not to sue both parties and whether or not to do so simultaneously or consecutively (although national tort law may specify otherwise).[63] Again, the initial controller should be able to claim back the awarded damages from the processor for disregarding his instructions on the basis of the contract between them.[64]

III. Multiple controllers

24 Not every collaboration among actors involving the processing of personal data implies the existence of a controller-processor relationship. It is equally possible that each actor processes personal data for its own distinct purposes, in which case each entity is likely to be considered a controller independently of the other ("separate controllers"). It is also possible that the actors jointly exercise decision-making power concerning the purposes and means of the processing, in which case they are considered to act as "joint controllers" or "co-controllers".[65]

1. Separate controllers

25 Separate controllers exchange personal data with one another, but do so without making any joint decisions about the purposes and means of any specific processing operation.[66] In such cases, each party is independently (yet fully) responsible for ensuring compliance of its own processing activities. In principle, the liability exposure of each party is also strictly limited to the processing activities under its own control. In exceptional cases however, liability may nevertheless be shared, particularly where failure to ensure compliance by one controller contributes to the same damages caused by the fault by another controller.

26 In the case of separate controllers, the starting point is that each controller is only responsible for ensuring compliance with its own activities ("*separate control, separate responsibilities*"). As Olsen and Mahler put it:

> *"In this type of multiple data controller relationship, the data controllers separately process personal data, but there is a data flow from one controller to the other. Each controller is responsible for his own processing, and the communication of personal data to the other data controllers is one example of such processing. One controller is not responsible for acts or omissions of the other data controller."*[67]

27 Because each controller is separately responsible for his own processing activities, only one controller shall in principle be liable in case of an unlawful processing operation (scenario A).[68] Liability may nevertheless be shared, however, if the fault of one controller brings about the *same damage* as the fault

60 See also Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 25. A (former) processor shall be (re) qualified as a (co-)controller where he acquires a relevant role in determining either the purpose(s) and/or the essential means of the processing (Id.). See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 62.

61 In principle, the processor may also be held liable on the basis of the national provision implementing art. 16 of Directive 95/46, which specifies that the processor may not process personal data "*except on the instructions of the controller*", which is a requirement directly applicable to processors. Depending on the jurisdiction, a breach of confidentiality by processors may also amount to a crime: see e.g. art. 38 of the Belgian Data Protection Act.

62 This outcome is similar to the liability of principals for torts committed by their auxiliaries "*in the course of the service*" for which they have been enlisted (although results may vary depending on national tort law). See e.g. T. Vansweevelt and B. Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, 2009, Intersentia, p. 416-421 and H. Vandenberghe, "Aansprakelijkheid van de aansteller", *Tijdschrift voor Privaatrecht* (TPR) 2011, p. 604-606.

63 In Belgium, victims of concurrent faults may hold both the tortfeasor and the vicariously liable party liable *in solidum*. See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 33-35. See also art. 9:101 PETL.

64 See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 176.

65 See also B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", op. cit. *supra* note 5, 34 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' –Part II", (2007) *Computer, Law & Security Review*, p. 419.

66 Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 19 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' –Part II", op. cit. *supra* note 65, p. 419.

67 T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", Legal IST project, 2005, p. 41.

68 Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

of another controller (scenario B).

a.) Scenario A

28 A hospital routinely shares information about a patient's treatments with an insurance company in order to obtain payment for the expenses relating to the patient's care. The sharing of personal information takes place with the explicit consent of the data subject and/or pursuant to national legislation. One day, the insurance company suffers a data breach as a result of insufficient security measures. Information about the patient's medical treatment is exposed, leading to considerable emotional harm. In principle, the patient will only be able to obtain compensation from the insurance company for the damages suffered because the hospital is not the controller of the processing operations undertaken by the insurance company.

b.) Scenario B

29 One day a hospital mistakenly transmits information about a patient's treatment to the wrong insurance company. The next day, that same insurance company suffers a data breach as a result of inadequate security measures. In such cases, the patient may be able to obtain compensation from both the hospital and the insurance company for the damages suffered as they each committed a fault contributing to the same damage.

30 Scenario B offers an example of *concurring faults*, whereby several distinct faults may be considered to have caused the same legally relevant damage.[69] What precisely constitutes "*the same damage*" is open to interpretation.[70] In certain jurisdictions, concurring faults lead either to solidary liability or liability *in solidum*.[71] If that is the case, each "concurrent tortfeasor" shall be obliged to indemnify the victim for the entire damage, irrespective of the severity of the fault leading to its liability.[72] The internal allocation of liability between the concurrent tortfeasors may nevertheless take into account the extent or severity of the fault.[73] In the case of scenario B, it would mean that the hospital would be obliged to indemnify the patient for the whole of the damages suffered, even though the hospital was not responsible as a controller for the poor security measures employed by the insurance company.

2. Joint controllers

31 In the case of joint control, several parties jointly determine the purposes and means of one or more processing activities. The distinction between "joint" and "separate" control may be difficult to draw in practice. The decisive factor is whether or not the different parties *jointly* determine the purposes and means of the processing at issue.[74] If the parties do not pursue the *same objectives* ("purpose"), or do not rely upon the *same means* for achieving their respective objectives, their relationship is likely to be one of "separate controllers" rather than "joint controllers". Conversely, if the actors in question do determine the purposes and means of a set of processing operations together, they will be considered to act as "joint controllers" or "co-controllers".[75]

69 See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 29-35; S. Stijns, op. cit. *supra* note 52, p. 110-111 and T. Vansweevelt and B. Weyts, op. cit. *supra* note 62, p. 835-839.

70 *Ibid*, p. 44-45 and S. Guiliams, "Eenzelfde schade of andere schade bij pluraliteit van aansprakelijken", *Nieuw Juridisch Weekblad* (NJW) 2010, afl. 230, p. 699-700 (arguing that different faults will be considered to have contributed to "the same damage" *if it is practically impossible to distinguish* to what extent the damage is attributable to each of the concurring faults).

71 See C. von Bar a.o., op. cit. *supra* note 25, p. 3599 et seq. See also art. 9:101 of the Principles of European Tort Law (PETL).

72 *Id.* The difference between solidary liability and *in solidum* liability is minimal: in both cases, the injured party is able to sue each of the debtors for relief of the whole amount. For more information see H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 29-36.

73 *Id.* In Belgium, the apportionment of liability among the concurrent tortfeasors must in principle be based on the extent to which each concurring fault may be said to have caused the damage, rather than the severity of the fault. (S. Stijns, op. cit. *supra* note 52, 111 and S. Guiliams, "De verdeling van de schadelast bij samenloop van een opzettelijke en een onopzettelijke fout", *Rechtskundig Weekblad* (R.W.) 2010, p. 475.

74 Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 19 ("*joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller*").

75 Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 25. The distinction between joint and separate control was rendered more explicit in the 1984 UK Data Protection Act, which defined a data user as the person that "either alone or jointly or in common with other persons" controls the contents and use of the data (Section 1(5) of the 1984 Data Protection Act). As clarified by the Data Protection Registrar: "The control does not need to be exclusive to one data user. Control may be shared with others. It may be shared jointly or in common. 'Jointly' covers the situation where control is exercised by acting together. Control 'in common" is where each shares a pool of information, changing, adding to or using the information for his own purposes independently of the other". (The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", Office of the Data Protection Registrar, 1989, p. 10-11.) See also the Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and

32 Directive 95/46 EC is essentially silent on how responsibility and liability should be allocated in case of joint control. The only guidance that can be found in the legislative history of Directive 95/46 is the following statement made by the European Commission:

> *"each of the co-controllers must be considered as being constrained by the obligations imposed by the Directive so as to protect the natural persons about whom the data are processed".*[76]

33 The cited passage suggests that each co-controller is individually responsible for ensuring compliance of the processing as a whole and should therefore in principle be liable for any damages resulting from non-compliance ("*joint control, joint responsibilities*"). The liability among joint controllers shall in principle be solidary in nature (i.e. the harmed data subject may bring a claim against any of them for the entire amount of the damage).[77] Of course, the solidary liability of joint controllers only extends to those processing activities for which they in fact exercise joint control. In case of "partial joint control" (whereby certain processing operations are performed under the sole control of one controller),[78] responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities.[79]

34 The solidary liability of joint controllers can be justified on the basis of the "common fault" committed by each controller. A "common fault" arises when multiple parties knowingly and willingly contribute to the same circumstance or event giving rise to the damage.[80] Common faults typically induce solidary liability.[81]

35 If the data subject decides to address only one of the joint controllers for the damages, that controller should be able to obtain redress from his fellow joint controllers for their contribution to the damages.[82] In principle, nothing prevents joint controllers from deciding how to allocate responsibility and liability among each other (e.g., by way of a joint controller contract).[83] The terms of such arrangements shall generally not however be opposable to data subjects, based on the principle of solidary liability for common faults.[84]

36 It should be noted that the Article 29 Working Party has defended an alternative point of view. Specifically, it has argued that joint control should not necessarily entail solidary ("joint and several") liability.[85] Instead, joint and several liability:

> *"should only be considered as a means of eliminating uncertainties, and therefore assumed only insofar as an alternative, clear and equally effective allocation of obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances".*[86]

37 The approach of the Article 29 Working Party seems fair when it comes to the internal allocation of liability among joint controllers, but may potentially be unjust towards the harmed data subject. The approach suggests that a contract between joint controllers may be opposable to data subjects, and that a harmed data subject may carry the burden of deciding which of the joint controllers is "ultimately" responsible for the damages suffered. In my opinion, the viewpoint of the Article 29 Working Party does not find sufficient support in either the text or legislative history of Directive 95/46. In cases where joint control exists, each joint controller should in principle incur solidary liability for damages resulting from the "common" processing. Any arrangements between joint controllers, including those regarding liability, should not be opposable

computer bureaux", Data Protection Registrar, 1985, p. 12.

76 COM (95) 375 final- COD287, "Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data", p. 3. See also Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 17-18.

77 T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", op. cit. *supra* note 67, p. 46-48. See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

78 T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' –Part II", op. cit. *supra* note 65, p. 420.

79 T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", op. cit. *supra* note 67, p. 46-48.

80 See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", op. cit. *supra* note 58, p. 30; T. Vansweevelt and B. Weyts, op. cit. *supra* note 62, p. 839.

81 See art. 9:101 of the Principles of European Tort Law (PETL). See also C. von Bar a.o., op. cit. *supra* note 25, p. 3599 et seq. and E. Karner, "The Function of the Burden of Proof in Tort Law", op. cit. *supra* note 16, p. 74.

82 See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

83 T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", op. cit. *supra* note 67, p. 48.

84 See also Tweede Kamer der Staten-Generaal (Netherlands), op. cit. *supra* note 17, p. 58.

85 Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 22. In this context, the term "solidary liability" is synonymous with the term "joint and several liability".

86 *Ibid*, p. 24.

to data subjects, based on the principle of solidary liability for common faults.[87]

C. The GDPR: a "cumulative" liability regime for controllers and processors

38 The GDPR has introduced several changes to the allocation of responsibility and liability among controllers and processors. While the controller is still the party who carries primary responsibility for compliance, processors have become subject to a host of obligations and are directly liable towards data subjects in case of non-compliance (article 82[2]). In situations involving more than one controller or processor, every controller or processor involved in the processing may in principle be held liable for the entire damage, provided the damage results from its failure to comply with an obligation to which it is subject (article 82[4]). The result is a "cumulative" liability regime, whereby each actor can be held liable in light of its role in the processing.

I. Controller liability

39 The liability model for controllers under the GDPR is essentially the same as under Directive 95/46. Article 82(2) of the GDPR provides that "[a]ny controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation." In other words, the controller remains generally liable for any damages arising from the unlawful processing personal data. The controller may be exempted from liability, in whole or in part, "if it proves that it is not in any way responsible for the event giving rise to the damage" (article 82[3]).

1. Nature of controller obligations

40 As under Directive 95/46, the actual liability exposure of controllers depends on the nature of the obligation in question. Many controller obligations under the GDPR are formulated as an obligation of means. For example, article 17(2) of the GDPR requires controllers who are obliged to erase data pursuant to the right to erasure, to take "reasonable steps" to inform other controllers that the data subject has requested the erasure. Moreover, it is worth noting that many controller obligations make reference to the notion of "risk" (e.g., data protection by design (article 25(1) GDPR), implying that the evaluation of risk may be a determinative factor in liability disputes. Only few controller obligations contained in the GDPR can be qualified as obligations of result. An interesting example is provided by article 13(3) of the GDPR, which concerns the duty to provide information to the data subject in case a controller who collected information from the data subject intends to further process data for a purpose other than that for which the data were collected.[88]

2. Non-delegable duty of care

41 The liability regime for controllers has remained "strict" under the GDPR: once an infringement has been established, the controller cannot escape liability simply by demonstrating the absence of personal fault.[89] The controller shall therefore remain liable for unlawful processing activities undertaken by the processor on its behalf, even if the controller were to demonstrate an absence of fault in either his choice or supervision of the processor. Under the GDPR, a controller may in principle be exempted from liability (in whole or in part) in only two situations: (1) if the controller can prove it is not in any way responsible for the event giving rise to the damage (article 82[3]); and (2) if the controller satisfies the conditions for liability exemption for intermediary service providers contained in Directive 2000/31 (article 2[4]).[90]

3. Burden of proof

42 According to article 5(2) of the GDPR, controllers are under a general obligation to be able to demonstrate their compliance with the basic principles of data protection ("accountability"). Moreover, a number of other provisions additionally stipulate that the controller must be able to demonstrate compliance, such as the provisions regarding the conditions for consent (article 7), processing which does not allow identification (articles 11 and 12[2]), and the general obligation to adopt appropriate technical and organisational measures to ensure compliance (article 24).

43 Strictly speaking, the requirement that the controller should "be able" to demonstrate compliance does

87 Again: in cases of partial joint control, responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities.

88 Interestingly, only in the situation where the personal data have been collected from the data subject is the duty to inform defined as an obligation of result. If the date have been obtained elsewhere, art. 14(5)a GDPR provides an exemption in case of disproportionate effort.

89 Compare *supra*; section B.I.2.

90 See also *infra*; section C.I.4.

not alter the burden of proof incumbent upon data subjects. After all, requiring the *ability* to demonstrate is not the same as requiring *actual* demonstration.[91] Such a formalistic reading would, however, run contrary to the principle of accountability which the GDPR seeks to promote.[92] The EU legislature did not introduce these provisions merely to promote better organisational practices, but also to require controllers to stand ready to demonstrate compliance when called upon to do so. As a result, one could argue that the data subject no longer carries the burden of proof of demonstrating exactly where the processing went wrong.[93] At the very least, the argument can be made that the provisions of the GDPR regarding accountability (which require controllers to "be able to demonstrate compliance") reinforce the notion that the controller is in fact "best placed" to proffer evidence of the measures it has taken to ensure compliance. Even if the legal burden of proof is still borne by the data subject, the evidential burden of proof should *de facto* shift to the controller as soon as the data subject has offered *prima facie* evidence of an unlawful processing activity.[94]

4. Defences

44 Article 82(3) GDPR provides that a controller or processor shall be exempt from liability if it proves that it is "not in any way" responsible for the event giving rise to the damage. Article 82(3) GDPR clearly echoes the escape clause of article 23(2) of Directive 95/46.[95] Interestingly, the GDPR does not contain a recital similar to recital (55) of Directive 95/46, which provides two examples of how a controller might prove that it is "not responsible for the event giving rise to the damage" (i.e., force majeure or error on the part of the data subject). Nevertheless, it is reasonable to assume that the words "not responsible for the event giving rise to the damage" should still be interpreted in the same way. As a result, the escape clause of article 82(3) still refers exclusively to "events beyond control", i.e. an abnormal occurrence which cannot be averted by any reasonable measures and which does not constitute the realisation of the risk for which the person is strictly liable.[96] If anything, the addition of the words "in any way" (in comparison to article 23[2] of Directive 95/46), suggests a desire to tighten the scope of the escape clause even further.[97]

45 A more significant development has been the formal recognition of the liability exemptions for internet intermediaries contained in the E-Commerce Directive. Article 2(4) GDPR specifies that the Regulation "shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive". The clarification provided by article 2(4) GDPR is most welcome, given the uncertain status of these liability exemptions under Directive 95/46. Article 1(5)b of the E-Commerce Directive provides that it does not apply to "questions relating to information society services covered by Directive 95/46 [...]". A literal reading would suggest that the liability exemptions provided in the E-Commerce Directive should not be applied in cases concerning the liability of "controllers", as this is a matter regulated by Directive 95/46.[98]

46 The practical importance of article 2(4) of the GDPR should not be overstated. A reasonable interpretation of controller obligations shall generally not result in the imposition of liability in absence of both knowledge and control. The decision of the Court of Justice in *Google Spain*[99], as well as the decision of the Italian Supreme Court in *Google Video*[100],

91 Only in art. 21 (right to object) does the GDPR specify that it is up to the controller to actually demonstrate the legality of his processing activities.

92 For a detailed discussion regarding the origin and development of the principle of accountability see J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", in D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), *Managing Privacy through Accountability*, 2012, Palgrave Macmillan, p. 49-82.

93 See also P. De Hert, V. Papakonstantinou, D. Wright and S. Gutwirth, op. cit. *supra* note 33, p. 141.

94 Regarding the distinction between *legal* burden of proof and the *evidential* burden of proof see C. Volpin, "The ball is in your court: Evidential burden of proof and the proof-proximity principle in EU competition law", *Common Market Law Review* 2014, p. 1177-1179.

95 Cf. *supra*; section B.I.4.

96 Cf. *supra*; section B.I.4.

97 See also P. Larouche, M. Peitz and N. Purtova, "Consumer privacy in network industries – A CERRE Policy Report", 2016, Centre on Regulation in Europe, p. 58.

98 It should be noted, however, that even in relation to Directive 95/46 certain scholars have argued that controllers should in principle be able to benefit from the liability exemptions contained in the E-Commerce Directive, including in situations where the dispute concerns the unlawful processing of personal data. See e.g. G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *International Data Privacy Law* 2013, p. 5 et seq.; G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *Maastricht Journal of European and Comparative Law* 2014, p. 573 et seq. and M. de Azevedo Cunha, L. Marin and G. Sartor, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *International Data Privacy Law* 2012, p. 57-58.

99 Cf. *supra*; section B.I.4.

100 Sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, Corte di Cassazione, sez. III Penale, n. 5107/14, at paragraph 7.2 ("[...] as long as the offense is unknown to the service provider, it cannot be regarded as the controller of the processing, because it lacks any decision-making power on

clearly support this proposition. Nevertheless, the incorporation of the liability exemptions for internet intermediaries is likely to yield certain benefits. First, it should further the development of a more horizontal and uniform approach to the issue of intermediary liability.[101] In addition, article 15 of the E-Commerce Directive clearly provides that Member States may not impose general monitoring obligations upon internet intermediaries. While most would agree that internet intermediaries should not be expected to proactively monitor whether the personal data disseminated through their platform is being processed lawfully, the formal applicability of article 15 of Directive 2000/31 would offer certain providers greater legal certainty. But article 2(4) of the GDPR is by no means a panacea: the concepts of "hosting, "mere conduit", and "caching" contained in Directive 2000/31 are subjects of continuous debate and have themselves given rise to a fair degree of legal uncertainty.[102] Moreover, the liability exemptions of Directive 2000/31 would only affect the liability exposure of controllers in relation to mere distribution or storage activities. An absence of liability for mere distribution or storage does not however, imply an absence of responsibility with regard to other operations performed on that content. Many service providers perform additional operations which go beyond a purely "intermediary", "passive", or "neutral" capacity.[103] As a result, it may still be necessary to interpret the obligations of internet intermediaries as controllers in light of their "responsibilities, powers and capabilities", as suggested by the Court of Justice in *Google Spain*.[104]

5. Eligible damages

47 Article 82(1) GDPR explicitly recognises that data subjects may seek compensation for both material and non-material damages. The EU legislature has thereby clarified that the right to compensation extends to "non-pecuniary damages". While this was arguably already the case under Directive 95/46, the clarification is nevertheless welcome with a view of removing doubt and ensuring a harmonised approach among EU Member States.

II. Processor liability

48 In contrast to Directive 95/46, the GDPR imposes a range of obligations directly upon processors and renders them liable towards data subjects in the case of non-compliance (article 82[2]).

1. Nature of processor obligations

49 As is the case for controller liability, the liability exposure of processors depends on the nature of the obligation concerned. Many obligations incumbent upon processors are formulated as obligations of means rather than as obligations of result. For example, the obligation to secure the processing of personal data (article 32) is clearly an obligation of means. On the other hand, the obligation not to process personal data except on the instructions of the controller (article 29), has been formulated as an obligation of result. The precise nature of a processor's liability exposure must therefore also be determined in light of the specific wording of each obligation.

50 It should be noted that the GDPR has added considerable detail as regards to the legal binding of processors towards controllers (article 28[3]). Processors must comply not only with requirements that are directly applicable, but also with requirements imposed by way of contract. For example, article 28(3) foresees that the contract or other legal act between the controller and processor shall stipulate that the processor shall assist the controller in the fulfilment of its obligation to respond to requests for exercising the data subject's rights - insofar as this is possible and taking into account the nature of the processing.

51 Other obligations that are directly relevant to processors are the obligation to maintain a record of processing activities (article 30[2]), the obligation to notify data breaches to the controller (article 33[2]), the obligation to appoint a data protection officer (article 37), the adherence to codes of conduct and requirements of certification (articles 41 and 42), and restrictions regarding international transfers (article 44 et seq.).

---

the data itself, and when, instead, the provider is aware of the illegal data and is not active for its immediate removal or makes it inaccessible, however, it takes a full qualification of the data controller".) A special word of thanks is owed to Professor Giovanni Sartor for assisting me with this translation.

101 M. de Azevedo Cunha, L. Marin and G. Sartor, op. cit. *supra* note 98, p. 57-58.

102 See e.g. P. Van Eecke, "Online service providers and liability: a plea for a balanced approach", *Common Market Law Review* 2011, 1481 et seq.; E. Montéro, "Les responsabilités liées au web 2.0", *Revue du Droit des Technologies de l'Information* 2008, p. 364 et seq. and B. Van der Sloot, "Welcome to the Jungle: the Liaiblity of Internet Intermediaries for Privacy Violations in Europe", *JIPITEC* 2015, p. 214-216.

103 B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", 2009 *Identity in the information society*, p. 62.

104 Cf. *supra*; section B.I.4.

2. Proportional liability

52 Despite the increased number of obligations incumbent upon processors, the relationship between controllers and processors has remained largely the same. Like before, the processor is essentially conceived of as an "agent" or "delegate" of the controller, who may only process personal data in accordance with the instructions of the controller (articles 29 and 28[10]). As a result, the liability exposure of processors remains more limited in scope than the liability exposure of controllers. Whereas controllers can in principle be held liable for damages arising from *any* infringement of the GDPR, processors can in principle only be held liable in case of failure to comply with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller (article 82[2]). This is essentially a "proportional" liability model, as the processor can in theory only be held liable in relation "for his segment" in the processing.[105] The processor will be liable for the entire damage however, insofar as it is - at least partially - responsible for the harm suffered (article 82[4]). To properly understand the meaning of article 82(4), it is worth elaborating upon its legislative history.

53 In the initial proposal for the GDPR, the Commission provided that processors would be jointly and severally liable, together with any controller involved in the processing, for the entire amount of the damage.[106] Mere "involvement" in the processing would be sufficient to render the processor liable, unless the processor could prove it was not responsible for the event giving rise to the damage. The Council revised the text to differentiate between the liability exposure of controllers and processors more clearly.[107] The changes introduced by the Council, which were retained in the final version of the GDPR, made clear that a processor would only be liable in case of failure to comply with those obligations of the Regulation which are specifically directed to processors, or if it acted contrary to or outside of the lawful instructions of the controller. As a result, mere "involvement" in the processing is not sufficient to give rise to liability: the liability of the processor is conditional upon a prior finding of responsibility in causing the damage. Only in cases where the processor can be deemed responsible in accordance with paragraphs 2 and 3 of article 82 GDPR can it be held liable for the entire damage. It is important to note however, that there is no threshold regarding the *degree* of responsibility of the processor in contributing to the damage. Even if the processor is only partially responsible, the processor can be held liable for the entire amount of the damage.[108]

54 From the perspective of the data subject, article 82(4) of the GDPR results in a "cumulative" liability regime.[109] The controller carries a general responsibility for the processing and can be held liable for damages in the event of an unlawful processing activity. The data subject additionally has the possibility to sue the processor directly in case he or she has reasons to believe that the processor and not (only) the controller is in fact responsible for the damage.[110] In such cases, the data subject will effectively have a choice whether to sue the controller, the processor, or both.[111] In cases where a controller and processor have been bound to the same judicial proceedings, compensation may be apportioned according to the responsibility of

105 See 2012/0011 (COD), 7586/1/15 REV 1, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 10 April 2015, in particular at p. 11 (Germany); p. 23-24 (France); p. 27 (Croatia) and p. 63 (Portugal). The concept of "proportional liability" is not always neatly defined and can be used to mean different things. See I. Gilead, M.D. Green and B.A. Koch, "General Report – Causal uncertainty and Proportional Liability: Analytical and Comparative Report", in I. Gilead, M.D. Green and B.A. Koch (eds.), *Proportional Liability: Analytical and Comparative Perspectives, Tort and Insurance Law* 2013, Vol 33, p. 1 et seq. Here the term is used to signal that each party's liability exposure is limited to their proportional share in causing the damages. If one party proves insolvent, the loss shall in principle be borne by the data subject. By contrast, in case of joint and several liability, each party can be held liable by data subjects for the full amount. See also J. Boyd and D.E. Ingberman, "The 'Polluter pays principle'": Should Liability be Extended When the Polluter Cannot Pay?", *The Geneva Papers on Risk and Insurance* 1996, Vol. 21, No. 79, p. 184.

106 COM(2012) 11, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 2012/0011 (COD), p. 91.

107 2012/0011 (COD), 9565/15, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", 11 June 2015, p. 185.

108 See also 2012/0011 (COD), 9083/15, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 27 May 2015, p. 3 ("[E]ach non-compliant controller and/or processor involved in the processing are held liable for the entire amount of the damage. However a controller or processor is exempted from this liability if it demonstrates that it is not responsible for the damage (0% responsibility). Thus only controllers or processors that are at least partially responsible for non-compliance (however minor, e.g. 5%) with the Regulation, and/or in case of a processor, with the lawful instructions from the controller, can be held liable for the full amount of the damage.").

109 2012/0011 (COD), 9083/15, "Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII", 27 May 2015, p. 3.

110 *Ibid*, p. 2.

111 *Id*.

each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured.[112] In cases where the processor is not joined to the same proceeding, the controller is entitled to claim back any compensation from the processor that was paid for in damages for which the processor was responsible (article 82[5] GDPR).

55 The cumulative liability regime of article 82(4) of the GDPR reflects the Principles of European Tort Law (PETL) regarding multiple tortfeasors. According to article 9:101 of the PETL, liability is solidary "where the whole or a distinct part of the damage suffered by the victim is attributable to two or more persons".[113] The same provision also stipulates that where persons are subject to solidary liability, the victim may claim full compensation from any one or more of them, provided that the victim may not recover more than the full amount of the damage suffered by him.[114] The main innovation of the GDPR in comparison to Directive 95/46 therefore does not relate to the imposition of cumulative or solidary liability as such (as the GDPR merely codifies general tort law principles), but rather to the fact that the GDPR also imposes an increasing number of obligations directly upon processors.

56 Finally, it is worth noting that article 28(10) explicitly states that if a processor infringes the GDPR by determining the purposes and means of processing, it shall be considered to be a controller in respect of that processing. The rule of article 28(10) applies "without prejudice to articles 82, 83 and 84", meaning that a failure to abide by the controller's instructions could still give rise to liability, even if the processing might theoretically have been legitimate if the processor had obtained the data through other means. It also implies that the initial controller remains liable towards the data subject even in cases where the processor re-purposes the data.[115]

3. Burden of proof

57 To hold a processor liable, the data subject must succeed in demonstrating three elements: namely, (1) the performance of an "unlawful act" (i.e. failure to comply with those obligations of the GDPR which are specifically directly to processors or an act contrary to or outside of the lawful instructions of the controller); (2) the existence of damages; and (3) a causal relationship between the unlawful act and the damages incurred.

58 As indicated earlier, the data subject may be able to invoke one or more presumptions in order to help substantiate its claims.[116] While the GDPR does not impose upon processors a general obligation to "be able to demonstrate" compliance, processors will often still be "best placed" to provide evidence of their efforts to comply with the obligations applicable to processors. As a result, the evidential burden of proof may also shift to the processor as soon as the data subject offers *prima facie* evidence of a failure to comply with those obligations of the GDPR, which are incumbent upon processors.[117] Again, it should be noted that the ability for the data subject to avail him- or herself of such a presumption may vary according to the domestic legal system of each Member State.

4. Defences

59 Processors can in principle benefit from the same liability exemptions as controllers. A processor who is considered (at least partly) responsible for the damage may be exempted from liability - in whole or in part - if it proves that it is not in any way responsible for the event giving rise to the damage (article 82[3]).[118] In addition, processors acting as internet intermediaries within the meaning of article 12 to 15 of the E-Commerce Directive, may also be exempted from liability provided the conditions listed in these articles are met.

5. Sub-processing

60 An interesting issue to consider is the liability of processors in the case of sub-processing. Article 28(4) of the GDPR provides that in the case of subprocessing, the initial processor remains fully liable towards the controller for the performance of the relevant obligations by the subprocessor. The GDPR does not however explicitly state that the initial processor also remains liable towards the data subject. Nevertheless, the argument can easily be made that this should be the case. After all, the GDPR imposes obligations directly upon processors. Every processor involved in the processing must therefore accept personal responsibility for those requirements directed towards processors, even in the case of outsourcing. The formulation of the escape clause of article 82(3) makes clear that the GDPR also imposes a non-delegable duty of care upon

112 Recital (146) GDPR.

113 Art. 9:101(1) PETL.

114 Art. 9:101(2) PETL.

115 See also *supra*; section B.II.2.

116 Compare *supra*; section B.I.2.

117 Compare *supra*; section C.I.2.

118 See also *supra*; section C.I.4.

processors.

6. Eligible damages

61 Under the GDPR, data subjects can claim both material and non-material damages from processors (article 82[1]).

III. Multiple controllers

1. Separate controllers

62 Pursuant to article 82(2) GDPR, any controller involved in the processing can in principle be held liable for the damages suffered. Read in isolation, one might assume that both joint and separate controllers face equal liability exposure. This is not the case however. While joint controllers can theoretically always be held liable for damages caused by processing activities under their joint control, separate controllers can only be held liable if the damage was caused by a processing activity which was under the control of that particular controller (or may otherwise be attributed to him). After all, article 82(4) provides that every controller involved in the processing may only be held liable "for the entire damage" insofar that they can be held responsible in accordance with paragraphs 2 and 3. As a result, separate controllers shall in principle only be liable for the entire damage if they acted as a controller towards the processing activity which gave rise to the damage or in case of "concurring faults".[119]

2. Joint controllers

63 The GDPR introduced a new provision dedicated specifically to situations of joint control. Article 26(1) provides that joint controllers must determine their respective responsibilities for compliance with the GDPR, in particular as regards to the exercise of data subject rights and their respective duties to provide information by means of an "arrangement" between them.[120] The arrangement must duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects (article 26[2]).

64 For the most part, article 26 of the GDPR can be seen as a codification of the earlier guidance provided by the Article 29 Working Party regarding the legal implications of joint control.[121] A notable difference however, is that every joint controller in principle remains liable towards data subjects for the entire damage even if there exists an appropriate arrangement between them (article 82[4]).[122] A joint controller can only escape liability if it succeeds in demonstrating that is not in any way responsible for the event giving rise to the damage (article 82[3]), or that it satisfies the conditions for liability exemption for intermediary service providers contained in Directive 2000/31 (article 2[4]).

D. Assessment

65 The GDPR has not fundamentally altered the basis for apportioning liability among organisations involved in the processing of personal data. The distinction between "controllers" and "processors" is still a decisive factor. Nevertheless, a number of important changes and clarifications have been made. From a liability perspective, the main novelties of the GDPR are:

1. the increased number of obligations directly applicable to processors and the recognition of their liability towards data subjects;
2. the formal recognition of a cumulative liability regime where more than one controller or processor are involved in the processing;
3. the incorporation of the liability exemptions contained in articles 12-15 of Directive 2000/31.

66 The liability model for controllers has essentially remained the same as under Directive 95/46: a

119 Compare supra; section B.III.2.

120 Joint controllers are not obliged to put in place such an arrangement in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

121 Article 29 Data Protection Working Party, op. cit. *supra* note 53, p. 22. See also *supra*; section B.III.2.

122 In its First Reading, the European Parliament had proposed to limit the joint and several liability between controllers and processors in cases where there existed an appropriate written agreement determining their respective responsibilities (P7_TA(2014)0212, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), p. 291. This approach was undesirable however, as it implied that the data subjects would carry the burden of determining which of the joint controllers was ultimately responsible for the damage. The revisions introduced by the Council brought the final text of the GDPR in line with the general principles of European tort law, according to which liability is solidary "*where the whole or a distinct part of the damage suffered by the victim is attributable to two or more persons*". See art. 9:101 of the Principles of European Tort Law (PETL).

controller shall in principle be liable for any damages arising from the unlawful processing personal data. The liability of the controller is also still "strict" in the sense that, once an infringement has been established, the controller cannot escape liability simply by demonstrating the absence of personal fault. Contrary to Directive 95/46, the GDPR also explicitly recognises processor liability. The liability exposure of processors however, remains much more limited in scope than the liability exposure of controllers. Whereas controllers can in principle be held liable for damages arising from any infringement of the GDPR, processors can theoretically only be held liable in case of failure to comply with obligations of the GDPR specifically directed to processors, or where it has acted outside or contrary to lawful instructions of the controller.

67 The cumulative liability regime of article 82(4) of the GDPR reflects the general principles of tort law regarding multiple tortfeasors. The main innovation of the GDPR in comparison to Directive 95/46 therefore does not relate to the imposition of cumulative or solidary liability as such, but rather to the fact that the GDPR also imposes an increasing number of obligations directly upon processors. The incorporation of the liability exemptions contained in Directive 2000/31 is likely to provide greater legal certainty to the providers of certain processing services, but there will still be many grey areas. In those cases, a balanced approach is necessary, which takes into account the "responsibilities, powers and capabilities" of the actor(s) in question.

68 Finally, the GDPR also explicitly recognises the eligibility of non-material damages. While this was arguably already the case under Directive 95/46, the clarification is nevertheless welcome with a view of removing doubt and ensuring a harmonised approach among EU Member States.

E. Conclusion

69 The liability model of EU data protection law is consistent with the Principles of European Tort Law (PETL), provided one takes into account the "general" liability of controllers and the "proportional" liability of processors. In many ways, the changes introduced by the GDPR merely constitute a (further) codification of general tort law principles.

70 The GDPR has retained the general principle that the controller carries "general" (or "primary") liability exposure for any processing activity under its control. It also recognises, in contrast to Directive 95/46, that processors should be directly liable towards data subjects. In addition, by rendering more obligations directly applicable to processors, the enforceability of certain obligations is no longer contingent upon the existence of a "contract or other legal act" between the controller and processor. The result is a cumulative liability regime, in which the data subject has a choice whether to sue the controller, the processor, or both – at least in cases where both controller and processor are at least partially responsible for the damage. In cases where the processor is not in any way responsible for the damage however, the only avenue for remedy shall be against the controller(s) involved in the processing.

71 While the GDPR has provided for greater clarity regarding the liability exposure of actors involved in the processing of personal data, it has not given special consideration to the difficult position that data subjects may find themselves in when trying to substantiate their claims. While certain data subjects may be able to avail themselves of one or more presumptions, the ability to effectively do so will depend on their domestic legal system. Absent the possibility to invoke such presumptions, the burden of proof incumbent upon data subjects remains quite onerous. The question may be asked therefore, whether it would not be desirable to formally recognise a shift in the burden of proof towards controllers and processors as soon as the data subject has offered *prima facie* evidence of an unlawful processing operation. Doing so would likely enhance the accountability of both actors towards data subjects.

* *Brendan Van Alsenoy, PhD.* is a senior affiliated researcher at the KU Leuven Centre for IT & IP Law - imec.

Acknowledgements
I would like to thank Wannes Vandenbussche, Jef Ausloos, Paul De Hert and Joelle Jouret for their valuable input and comments during the writing process. Any errors contained in the article remain my own. The research leading to this paper has received funding from the European Community's Seventh Framework Programme for research, technological development and demonstration in the context of the REVEAL project (revealproject.eu) (grant agreement no: 610928) and from the Flemish research institute imec (previously "iMinds").

jipitec

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu