Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Can Chinese Legislation on Informational Privacy Benefit from European Experience?

dotLegal Publishing dissertation series no. 2014-1

Original and modified cover art and lay-out design by
dotLegal Publishing (Lyx/XeteX/Bibdesk/the Gimp)

ISBN 978-94-92111-00-5

Can Chinese Legislation on Informational Privacy Benefit from European Experience?

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van de Rector Magnificus prof. mr. C.J.J.M. Stolker
volgens besluit van het College van Promoties
te verdedigen op dinsdag 16 September 2014
klokke 13.45 uur
door

Kunbei Zhang

geboren te China in 1983

Promotoren: prof. dr. A.H.J. Schmidt
prof. dr. G.-J. Zwenne
Overige leden: prof. dr. S. van der Hof
prof. dr. B.R. Katzy
prof. dr. R.A. Lawson
prof. dr. J.M. Otto
prof. dr. J.B. Ruhl (Vanderbilt University)
dr. B. W. Schermer

Can Chinese Legislation on Informational Privacy Benefit from European Experience?

张琨蓓

(Kunbei Zhang)

dotLegal publishing
2014
Oegstgeest
consultancy & research
on law & complexity

献给我的父母

Preface

This thesis records the experiences and observations that I collected in the past six years. I spent the most brilliant period of my youth at eLaw, of Leiden University. The interdisciplinary institution helped me find and investigate an interesting field, personal data protection. I selected it as my research subject and will pursue it in my subsequent research efforts (in China).

The conceptions in the thesis are diverse. Part of them is drawn from the legal training I received during the last 12 years. Another part stems from a new interest in the philosophy of science, considering complexity. In this thesis, I weave them together. Indeed, this has seriously challenged my capabilities to cope with creative scientific research, since I needed to describe my arguments and results in a manner understandable to who are strange to this field. The result has been a drastic shift in my research. Readers can find that my research bridges across positivist and realist comparison, law and economics, cultural exploration and complexity theory. Nevertheless, the main purpose of the research remains to improve our comprehension of the law, of data processing and of their interactions.

The book is also an attempt to explain to myself and to my readers how I struggled through the whole journey, with its disappointment and pleasant surprises. Initially, I wrote the thesis in the form of a dialogue to myself. The dialogue I had in mind was a sort of personal testimony, a testimony of how my understandings and misunderstandings unfolded over time, with many detours and shining points hidden in paragraphs, as pleasant surprises. And sometimes I was happy as a playful child when I could change the tune of the story at an unexpected

moment and place. Yet, as a Ph.D student who not only wants to investigate the unexplained, but also wants to graduate, I had to bend this inclination and provided a second version in a more serious tone.

Nevertheless the result still has the traces of a mixed bag that can best be classified as exploratory law research. My research project's structure has (at the level of a single project) become analogous to Kuhn's dynamic scheme for scientific revolutions: normal science within a paradigm, crisis in the paradigm, revolution, the inkling of a new paradigm (Kuhn (1962)). The research was originally triggered by an assumption. Upon its inspection, the research story adapts when anomalies are brought to bare, and finally something new is found, at the point where the initial assumption has itself become an anomaly. Again, the chapters in this thesis follow the logic of exploratory research. Not the "order" of a random walk, but the dynamics of contextually informed search: the conclusion from the current chapter/stage provides the bridge to the questions to be discussed in the following chapters/stages (and then the questions derived thereof become new points for exploration).[1] As a whole, the thesis displays a dynamic scheme because its research path could not be foreseen completely in advance.[2]

One of its most important arguments leads to the conclusion that the community of personal-data users is a complex adaptive system, and that this finding supports and helps further interdisciplinary cooperation for improved information of the legislator. This gives me the courage to follow my intuition in my research to come, to think out my own ideas and to form

[1] I cannot but feel that the legal discipline is currently more in a situation that Kuhn (1962) would qualify as being "in crisis" (also internationally) than in a situation of paradigmatic stability (of "normal science"), when legal data protection arrangements are under consideration.

[2] "The world which we want to explore is a largely unknown entity. We must, therefore, keep our options open and we must not restrict ourselves in advance. Epistemological prescriptions may look splendid when compared with other epistemological prescriptions, or with general principles, but who can guarantee that they are the best ways to discover, not just a few isolated 'facts', but also some deep-lying secrets of nature? (Feyerabend (1975):12)"

my own independent theories, and to investigate them further in diverse scholarly cooperation. I do not have – none of us has – sufficient scientific education to singlehandedly research in an adequate manner the serious and complex problems of our current communities. Personal data protection is central to many of these problems, and that is where my research will remain focused. During my project I have been encouraged by the finding that there are many people around the world, from many disciplines, who agree with me in this. I cannot wait to join forces with them in my future projects.

Leiden, 15 juli 12014, 张琨蓓

Contents

Part I

The Perils of Importing Law

Chapter 1

Introduction

In October 2008 I embarked on a research voyage in order to explore how Chinese legislators, when considering data protection legislation, can benefit from Western experience.[3] My goal is (and was) to find and present well-founded advice for the Chinese legislator on transplantation of European data protection law. By 2014, I had investigated the issue from several perspectives. This book provides the results of the journey.

[3]My voyage was under supervision of dr. Aernout Schmidt (emeritus professor of law and computer science) and dr. Gerrit-Jan Zwenne (professor of data protection law), both at eLaw@Leiden (Center for Law in the Information Society at Leiden University Law School). Both helped me with their scientific guidance and with editing the (imperfect) English language I produce. If you are surprised, here and there, by a long and complex English sentence, it will be the result of a habit in my editors' English that I tolerated to persist. Dr. Schmidt also helped me prepare contributions (that he co-authored in this manner) to (1) the Workshop on Legal Culture, held on May 20-21, 2010 at the Universita ca Vascaria in Venice and to (2) the Eleventh Chinese Internet Research Conference, held on June 15, 2013 at the Internet Institute of the University of Oxford. These two contributions were preliminary versions of my Chapters 3 and 5 respectively. In the beginning of 2014 I was informed that a slightly adapted version of my Chapter 4 was accepted for publication by the peer-review process of the German Law Journal.

Research background

In 2009, a TV program produced by China's national television, CCTV, revealed that a large number of Chinese companies, like mobile Internet advertising companies and telecommunication firms, collected information about their users and sold it to third parties that used the information to conduct fraudulent activities and to commit online crimes. This revelation caught people off guard, and resulted in a significant increase in demands for improving personal data protection in China.[4] It is widely believed that at the root of personal data risks is the lack of comprehensive data protection legislation necessary to enforce data protection. Even today, in China, there is no comprehensive legislation at a national level that deals specifically with the right to the protection of personal data, nor is there any law that provides guidance on how a company can use personal data in a legitimate manner.[5] The traditional legal arrangements for privacy protection are still applied to data protection issues, such as the arrangements for contractual and tort liabilities.[6] Specific rules and provisions governing the use of personal data (e.g., for credit reporting) are scattered over different laws, regulations and local ordinances, and therefore not very effective. This can result in serious problems and surprises (like the one mentioned above), indicating a need to arrange for a more comprehensive and general data protection law.

In order to bring the data protection level to a higher standard on protecting consumers' data rights, proposals regarding the transplantation of Western law arrangements to China have been put on the agenda of the legislative agency in China (Aiming Qi (2007, 2005)). It is unclear why the policymakers prefer to import a law, rather than invent one that fits the specific Chinese context. Supported by my interviewees' opinions (as described in Chapter 2), the legal importation proposal is based on the following two arguments. First, importing a well-established law could save legislators' time and energy. In China, all other adaptation and upgrading of the legal system was suspended, in order to focus on the establishments of the new Civil Code. All capacities of the legislature were reserved for that task, and China's lawmakers may not have had the luxury of time to design a new Chinese personal data protection law. Second, even if a separate and new Chinese data protection law had been drafted, there would have remained a long period of trial and error (and remodeling) to go through. By contrast, importing an established law that has already gone through the process of trial and error in another jurisdiction may be a comparatively fast and efficient solution. Therefore, current Chinese scholarly wisdom suggests that to import (to transplant) a law may satisfy China's needs more rapidly and more effectively (Aiming Qi (2005, 2007), Hanhua Zhou (2006)).

Among the Western arrangements that may be considered candidates for solving the data protection problems in China, many legal scholars, particularly Qi Aimin and Zhou Hanhua who are influential in this field, recommend Europe's current legal arrangement. This is not unexpected.[7] There is almost half a century of data protection in the European legal world. The first general data protection legislation appeared in 1970. The German State of Hessen was first, followed by Sweden, Great Britain and then the rest of the European states gradually followed.[8] In 1981, the Council of Europe established a Convention for the protection of individuals with regard to

[4] See Parsons (2013).

[5] The Decision on Strengthening Protection of Network Information passed by the Standing Committee of the National People's Congress in December 2012 is the first national legislation to squarely address data privacy regulation, albeit only in relation to personal data transmitted via public telecommunications networks and not personal data in general.

[6] In Europe, some scholars suggest following a similar path. For instance, Colette Cuijpers advocates to protect informational privacy by private law, instead of adopting a specialized and comprehensive data protection law (Cuijpers (2004)). Nevertheless, in China, no such advocates exist.

[7] Not all Chinese researchers recommend the transplantation of European legal data-protection arrangements. For example Liu Deliang is strongly against this proposal. However, other researchers whom I interviewed recommend the European model in their papers and/or interviews. (Aiming Qi (2005, 2007),Hanhua Zhou (2006))

[8] Jentzsch (2007):3.

the protection of personal data (Hereafter the Convention).[9] The Convention also regulates cross-border transfers of personal data. In 1995, the enactment of Directive 95/46/EC raised a new playing field at EU level, sustained by harmonized data protection laws. Moreover, as Birnhack said, the global legal network for data protection is mostly driven by the examples of the European legislation (Birnhack (2008)). In 2012, the European Commission proposed a comprehensive reform to update and modernize Directive 95/46/EC. The reform can be seen as another example that Europe leads the way in data protection regulation (Reding (2012)).[10] Many countries enact data protection laws based on the model provided by European law, and multiple studies have buttressed that the right to personal data is protected less in China than in Europe.[11] Moreover, these studies often suggest that the Chinese data protection problems can be addressed by importing a well-written data protection law, and transplantation of European data protection law, as in Directive 95/46/EC, is favorite.

Thus, many Chinese researchers believe that if the legislative agency imports the EU data protection law, the problems related to data protection would be addressed effectively. This expectation in Chinese academia is based on two propositions. First, EU data protection law, especially Directive 95/46/EC, which would be the main object of legal importation, is considered to be complete.[12] This view remains dominant in China's

[9] Council of Europe (1981).

[10] Viviane Reding, the Vice President of the European Commission, submitted that the data protection regulation reform in Europe can build a new gold standard of data protection. The whole contents of her speech can be accessed at http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/20120319speech-data-gold-standard_en.pdf

[11] See for instance Jentzsch (2005), Dehong Ai & Zhigang Cai (2001), Qiong Wang & Zongxian Feng (2006), Xiulan Zhang (2005), Yue Wang & Jian Xiong (2003), Jian Zhou (2001), Qin Xie (2006) , Hailin Hong (2007), Hanhua Zhou (2006), Aiming Qi (2007).

[12] When a law is considered to be complete, it means "obligations can be unambiguously stipulated in the law and the law can be enforced literally provided that evidence is established (Xu & Pistor (2002a):938)."

mainstream legal scholarship.[13] However, as Xu and Pistor suggest, when people promote a law to be complete, their silent assumption is that obligations can be unambiguously stipulated in the law and the law can be enforced literally (Pistor & Xu (2002b): 938). One of the things that I show in this book is that this assumption is invalid for personal data protection in the current era. Second, the Chinese debate on legal transplantation stays predominantly focused on (i) formal legal rules, particularly on the definition/categorization of personal data and on (ii) the nature of the (fundamental? civil?) rights related to personal data. Little attention is paid to the establishment and design of institutions that are responsible for the interpretation and the enforcement of the imported law. Yet I show that ignoring the institutional side can be problematic.

Consequently, the enthusiasm of using EU data protection law to address China's problems related to data protection should be treated with skepticism. I propose a more cautious approach than to unequivocally transplant foreign law, considering that several importation failures happened in practice, including Bankruptcy law (Wu (2009)), Adversary system reforms in Criminal prosecution law (Yin (2002)), Corporate Governance regulations (Shi (2008)), Arrangements on Director Independency (Xie & Zhang (2010)). These law-import projects represent efforts of the Chinese legislators to improve and adapt the Chinese legal system. However, in practice, these transplanted legal systems mostly fail to be accepted by Chinese bodies of legal practice. They have merely become rules in the legal books, and have failed to become integral parts of the Chinese social-economic infrastructure. For instance, the "independent director" has remained an unsuccessful attempt to increase internal supervision of a company (Xie & Zhang (2010)). And bankruptcy law, which was enacted to protect state-owned companies, has become an obstacle to the reform of the corporate system (Wu (2009)). Moreover, intellectual property law, as enacted under the pressure of Western countries, does not feel natural to the Chinese people and is considered to

[13] See, note 4.

be a price to pay for joining the WTO (Wu (2009)). It rather shows China's ambition to gain full integration with the international economic community (Wu (2009)). Yet, the criticisms on China's IP practices are at least as strident as before the law's importation (Wu (2009)). China's IP practices are still re-enforcing a climate of criticism about their legal quality and efficacy (Wu (2009)). Yet, looking at these failures, I am not urging against the data protection laws transplantation plan in China. Rather, it is important to understand that any legal importation attempt does face a non-trivial probability of failure. Thus, China's policymakers will need to be careful when considering plan to transplant European data protection law to China.

Another reason for apprehension about the transplantation plan are the difficulties that data protection law faces in the Europe. The effectiveness of EU data protection law to actually impede inappropriate personal data use, has been hotly disputed.[14] Especially after 9/11, the media exposed serious incidents, displaying the weaknesses of EU data protection law. In 2006, for instance, SWIFT confessed that it had been transferring massive amounts of data on international bank transfers to the US Department of the Treasure, bypassing the European data protection laws and the European data protection regulators supervision (Bignami (2007):616). It was considered to be flawed since the legal system accomplished little more than being a witness to a systematic breach of people's fundamental rights (Rettman (2013)). Arguably, the European data protection law is an institution with strengths and weakness like any other. And even in Europe, it cannot conclusively solve data protection problems for substantial stretches of time, if at all. We witnessed a recent striking example, on April 8th of 2014, when the European Court of Justice declared the EU Telecom Data Retention Directive[15] invalid in a landmark decision.[16] Although these examples can also be interpreted as supporting the contention that the European data protection regime works, they show that there are serious doubts about the effectiveness and completeness of European data protection law in action. Thus, there is an established need to uncover the strengths and weaknesses of EU data protection law, before transplanting it to China. Therefore, my research is motivated by skepticism over China's transplantation plan. I want to challenge the legal transplantation plan and I want to explore what lessons we, Chinese, can learn in a more diligent manner from the European experiences with data protection law. That is what the thesis aims to investigate.

[14] As stated in the "The Future of Privacy", the Directive 95/46/EC has not successfully ensured the translation of data protection requirements into practice (Article 29 Working Party (2009a)). The effectiveness issue has attracted Article 29 Working Party's attentions. Several opinions have been issued to improve this situation, such as Article 29 Working Party (2010a)Article 29 Working Party (2009b)Article 29 Working Party (2012). In 2012, the European Commission submitted the "General Data Protection Regulation" proposal to reform current data protection law which yet failed to bring in real protections. As lawmakers stated in the proposal, the data protection reform is an opportunity to "strengthen the effectiveness of the system by modernizing arrangements in Directive 95/46/EC"(European Commission (2012)).

Research question

Based on the above analysis, my main research question is the following:

> "Is the plan for transplanting European data protection law into China, particularly the Directive 95/46/EC, advisable in view of more adequately protecting personal data?"

More particularly, I try to address the question: If Chinese privacy legislation in the area of data protection is lacking vis-a-vis globally accepted data protection principles, could China benefit from EU experience by transplanting EU data protection legislation to China?

[15] Directive 2006/24/EC.

[16] In Joined Cases C-293/12 and C-594/12.

How can I complete the process?

When I started the research, the first series of questions emerged due to the transplantation plan, and was based on how the European data protection law could improve the quality of data protection in China. As China wants to import the European data protection law, an intuitive argument is that the European law would address the defects of data protection issues in China. In other words, China's policymakers believe European data protection law would improve the current situation, because otherwise these would be no point in importing a foreign law into the Chinese system. Thus, I compare both legal systems to reveal how European data protection law could contribute to China's data protection law.

The second series of questions is related to the question why China failed to generate its own data protection law as early, or as successfully, as in Europe. How does the European cultural background on privacy arguably facilitate, condition and characterize the path to the human rights-based personal data protection in Europe? Is there anything common between the informational privacy patterns in the two regions, or are they fundamentally different? These questions call for an exploration based on an historical and comparative perspective.

The third series of questions arose from the positive reception of the European data protection law in China. As I mentioned above, Chinese policymakers claim that the European data protection law is complete, and stress the reasons why it is so beneficial. However, such a view may contradict the most elementary assumption of legal thinking: neither a rule of law, nor a legal system can be absolutely complete (Hart (1994):128). And European data protection law is no exception. How do European policymakers attempt to compensate for the defects of the incompleteness? If Chinese policymakers still want to import the law, what can they do to adjust their original transplantation plan?

The questions above explore whether the European data protection law can be transplanted. However, the ways in which it is transplanted are equally important. Although transplantation seems a cost effective choice to ameliorate the deficiency of China's data protection law, one important point should be considered when the transplantation strategy is being planned. A law and regulatory system, which seems perfectly suitable to Europe, may yield unexpected negative implications (e.g., corruption or hidden trade barriers) as a result of its being transplanted to a completely different context. Indeed, many problems over data protection issues appear indiscriminately in both China and Europe. Nonetheless, the historical context has much to do with how the solution should be reached. Thus, the possible legal transplantation should be considered in light of local conditions, rather than mechanically reproducing laws from abroad.

Based on the above analysis, my main research question is divided into the following questions:

1. In a comparative perspective, how could the European data protection law improve the quality of data protection in China?

2. How does the historical context shape the data protection law in Europe and China?

3. The European data protection law is not complete as China policymakers' expect. Under this circumstance, how do European policymakers compensate for the defects of the incompleteness?

4. How should China reproduce the EU experiences to achieve a positive impact, more protection for data subjects with respect to their personal data?

Research approach

Multiple methods

In order to answer the above questions, several methods are deployed to advance the analysis. This section briefly describes the application of the analytical framework within each of the six chapters.

Positivist functional comparison

In Chapter 2, I employ an elaborate thought experiment as a heuristic tool, in order to see how the EU data protection law could upgrade China's legal arrangement on data subjects' protection and the protection of their data. In order to demonstrate the gap between the two regions' data-protection laws, I assume that both China and Europe face the same need, to regulate a giant Credit Reporting Database (such as actually exists in China). In this hypothetical way, I investigate how such a giant service, as regulated in China, would be understood in Europe (comparing how the facts would be qualified in two different legal systems). In this way, the differences between the two systems laws are brought into focus from a positivist perspective. This chapter is designed to capture some of the coarse-grained differences that Europe and China have, in this respect. The conclusion of this chapter forms the basis for further comparisons.

My approach is a reformed functional comparison. Conventionally, functional comparisons, as suggested by Zweigert and Kötz, imply that comparisons should assume that different societies have similar needs and that, to survive, any society must have (functionally equivalent) institutions that meet these needs (Michaels (2005): 363). Such conventional approaches seek similarity and have been criticized (Michaels (2005): 363). My approach in Chapter 2 emphasizes the differences between the two regions' legal arrangements on data protection. This reformed approach is greatly influenced by Bignami's work, which explores the solutions to an assumed problem in the two different legal systems under comparison (Bignami (2007): 677). His adapted functional comparison emphasizes on the legal differences between Europe and America over data protection and allows him to propose a number of recommendations for the reform of U.S informational privacy law (Bignami (2007): 677). Similarly, I plan to propose recommendations for upgrading China's data protection law through learning from European experiences.

Cultural comparison

In Chapter 3, I compare the effect of culture on informational privacy in China and Europe through an historical lens. In academia, China's data protection is often compared to its European counterparts. The two data protection regimes are respectively contrasted as cyber surveillance versus freedom in cyberspace, low level of protection as opposed to high level of protection, lack of transparency as opposed to openness. However, even if such a dichotomy may be regarded as a working hypothesis, we may wonder why and how the differences on conception of privacy have emerged in the first place? The national cultural background that lies behind informational privacy may offer an answer to this question. Additionally, the cultural argument may prove useful (in Chapter 5) to convince China's policymakers to pay attention to activities that interfere with personal data protection but that currently lack recognition.

However, I will not delve deep into the cultural explanations, because applying the traditional, detailed approaches to legal-comparative work may lead to "writing an introduction to [...] a broad [...] description of historical events, of examples of legal reasoning, of institutions in a comparative perspective, of a wide variety of sources, including legislation and case law, and ideology" (Otto (2000): 231-232). I am more interested in the legal implications. Therefore, in order to avoid the main argument from becoming diluted and diverted into far too complex a cultural dialogue, I only explore the impact of culture on the two jurisdictions' views on informational privacy. Moreover, I focus particularly on the dissimilarities between the concepts of privacy in China and Europe because the chapter only tries to clarify how the cultural legacies impact on shaping the unique informational privacy legal systems in the two regions.[17]

[17]The two jurisdictions do share similarities. For example, in post 9/11 times, the fear for public insecurity and disorder has substantially increased in Europe, and has reduced the weight of personal data protection in its balance with the weight of public security to a level that reminds me of the balance that has emerged much earlier in China, with its histories of political upheaval, civil wars and long periods of disorder. But these similarities fall outside the scope of this thesis, as it focuses on private law

Incomplete law theory

In Chapter 4, I apply Incomplete Law Theory, a contribution by Chenggang Xu and Katharina Pistor (Xu & Pistor (2002a)). According to Xu and Pistor, the analytical framework of the theory is as follows:

> "We start from the premise that law is intrinsically incomplete, which implies that it is impossible to write a law that can unambiguously specify all potentially harmful actions. Because law is incomplete, law enforcement by courts may not always effectively deter violations. Rather than attempting the impossible task of completing the law, the effectiveness of law enforcement may be enhanced by reallocating lawmaking and law enforcement powers (LMLEP) [...] when law is highly incomplete and violations of the law may result in substantial harm, it is optimal to allocate law enforcement rights to regulators rather than courts" (Pistor & Xu (2004)).

China's policymakers maintain that European data protection law is complete and therefore beneficial (Hanhua Zhou (2006)). Thus, their transplantation plan, based on that assumption, reproduces the contents about data subjects' rights and data controllers' responsibilities in European law. However, formal law must always be expected to be incomplete in the light of changes that may happen due to technological innovations, especially when these changes occur frequently and have considerable impact. There are often obvious gaps between the EU law in the books and the EU law in action. Thus, considering the pros and cons of data protection legislation transplantation without taking these gaps into consideration may not be diligent. Incomplete law theory offers a coherent analytical framework, not only for allowing me to assess the completeness of European data protection law, but also allowing to identify how European policymakers nurse the law (when incomplete) to ensure effective law enforcement (Xu & Pistor (2002a):995).

aspects of privacy and data protection.

Thus, I adopt and apply incomplete law theory in order to propose to China's policymakers an innovative reorientation in their customary ways of thinking and talking about European data protection law.

Realist functional comparison

The purpose of Chapter 5 is to find out what the transplantation to China of the EU laws on data protection would bring about in reality, especially considering the institutional need for law enforcement in an environment that is changing in unpredictable ways at all ends.[18] What would happen if the roles of the European data regulators were transplanted to China? From this realist perspective, the comparison is used as a tool to seek progress through analysis. Through testing how EU data regulators would react to China's Facebook, I try to anticipate the daunting challenges that need to be faced by China's policymakers and the relevant legal agencies in the process. Although Chapter 5 starts (like Chapter 2) with a thought experiment, by imaginatively embedding China's Facebook RenRen into a European member state, the comparison is not for demonstrating the differences in the two regions from a formal-law or positivist perspective, but for explaining that China's legal arrangement over data protection issues might in reality (from a realist perspective) not be equally successful as Europe in creating a sustainable data protection environment, even though it has followed the blueprint of the European model.

Intermediate conclusion

My approach concludes in Chapter 6 that it is not feasible to transplant EU data protection law, unless an equivalent to European data protection regulatory institution is included. And even this is not enough. In Chapter 4, the findings show that the quickened pace of technological changes appear to make the data protection law's subject matter to increasingly behave un-

[18] As, e.g., at the end of technology, the end of mass social media practices, at both ends of economic affairs and at the end of public security.

predictable. The circumstances embedded in the subject matter of the data protection law (i.e., protection of data subjects, regulating data processors and facilitating free flow of data and so on), are affected by technological dynamics, such as the progress in mobile communication and infrastructure (e.g. cloud), as well as the use of personal data by internet services, which generate large personal-data collections. The Incomplete law theory points out the requirements for the law and its institutions to effectively cope with innovations in society. However, even though EU legislators and data regulators continue their struggle with unpredictable problems, they cannot completely accommodate their data protection law to the dynamics that its subject matter exhibits. Yet laws for data protection have been promulgated and continually adapted in the EU for more than 30 years. I do not see many indications of legal activities that will help solve the situations at hand. Traditional legal approaches appear limited when responding to the dynamic characteristics of data protection law's subject matter, because law must be general, certain and predictable, but the data protection law's subject matter is special, dynamic and unpredictable - both technically and socially. Such limits could explain why there are often failures to find stable legal formulas for the effective control of legitimate personal data use. My attempt to further unpack this puzzle is by implementing a non-legal approach.

Complexity theory and its subject matter

Given the findings collected from the previous chapters, the final part of the dissertation provides some policy recommendations to China's policy-makers, based on the Complex Adaptive System theory (CAS-theory). These recommendations are partly founded on my analysis, qualification and identification (in the beginning of Chapter 7) of "the Personal Data Community" as a CAS. The CAS-theory looks at systems

> "in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution" (Mitchell (2009):13).

CAS-theory is the conceptual model built for scientifically understanding these kind of systems. The theory suggests that CASs, regardless of their particular subject matter, exhibit certain universal characteristics, self-organization and emergence being the most critical ones (Tussey (2005): 148).

To adopt CAS theory is innovative and experimental but also challenging, because of its novel scientific formulation. My choice for this theory rests on, what Einstein described as the "sympathetic understanding of experience" (Einstein (1918)). In order to theoretically investigate how the behaviors of dynamic Internet services can be better understood from a non-legal and scientifically oriented perspective, the classics on institutional economics (North (1993)), on complex adaptive systems and on model thinking Page (2008) have been read.[19] These approaches, I believe, could all offer lessons to China's policymakers to enjoy the advantages of European data protection law, from different perspectives.

The reason why I employ the CAS approach is because the subject matter of data protection law, which I identify as Personal Data Community (PDC), as a set of data controllers, data subjects and personal data users, *might be understood as a CAS*. In Chapter 7, I look for evidence that suggests that the PDC is a complex system, where the units collectively exhibit the features of self-organization and emergent system behavior. Because if the PDC is a CAS, the road is cleared for future research that employs CAS-theory to better understand the PDC's dynamics.

In Chapter 7 I show that the PDC is self-organized since various units come to the system voluntarily and even without leaders from inside or outside the system. An instance is the development of Facebook social networking technology by an undergraduate student and then the rapid emergence of the Facebook community as a result of self-organization within the

[19] I also used material presented in an online course on model thinking by Scott Page. See https://www.coursera.org/course/modelthinking

PDC. Although the initial concept of the social network that later became Facebook was designed by only a couple of individuals (particularly Mr Zuckerberg), the appearance of the Facebook community was not designed or commanded. The local, individual actions and communications of technology providers, businessmen, service providers and individual users of social networking produce the patterns that became the Facebook community. The PDC itself is an emergent community, produced by the individual activities of local units without a clue about what their collective behaviors would look like or lead to. The PDC emerged from the local interactions of units, particularly technology providers, service providers, institutional users, consumers, companies and enterprises, and other stakeholders, pursuing their own interests. These interactions produced vast networked communities through which personal data (and much more) may be transmitted fast and easy. This PDC is neither invented nor designed by any individual unit. Rather, it emerged from interactions of a large amount of "constituent" units that reacted to opportunity and need.

Furthermore, I argue that the PDC as a whole is adapting to exogenous changes. Like what I observe in Chapter 4, the most striking constraints for PDC- and PDC-unit behaviors do arise from the dynamics in technology. Units, such as companies, are concerned with technological changes and the changes affect the units' behavior. Indeed, changes in technology have real consequences. Also, in Chapter 3, I observe the changes in social-economic backgrounds which were brought on by the 9/11 tragedy, which brought changes to the behaviors of units in the PDC and led to a tug-of-war of conflicting interests between national security values and privacy values: the protection of national security values implies that advances have to be made into the protection of the right to privacy.

If so, the data protection law system, as a control system of the PDC, may benefit from the insights gained by other CASs. The CAS theory could offer a new lens to look at current data protection laws. Within the complex theory framework, there is ample room for us to integrate human-based activities (lawmaking and law enforcement) with the use of additional instruments.

The integration could assist analysis, understanding, and subsequent strategy formulation regarding opportunities and threats that emerge as the result of the ever-changing PDC.

Positivist and realist perspectives

As mentioned, in order to complete the answers to the research questions in the book both positivist and realist perspectives are used to analyze the effectiveness of the law.[20] These two perspectives are understood as in Marmor:

> "The school of legal realism [...] took up the idea that social forces outside the law are central in determining what the law is. Realists opposed traditional 'formalist' accounts of adjudication, where judges are understood to rely on uniquely and distinctively legal materials in rendering their judgments."
>
> and:
>
> "Positivists, in contrast, have argued that what is law is determined only by the institutional facts internal to a legal system, facts that may or may not meet moral standards [...] According to positivism, law is a matter of what has been posited (ordered, decided, practiced, tolerated, etc.)" (Marmor (2011)).

Although both arguments have long been strongly advocated, often by different and competing schools of legal theory, I adopt the two perspectives jointly. Even though employing both perspectives at the same time may be considered unorthodox, they are both relevant and important to describe and understand Chinese and EU data protection situations. I consider them complementary, the positivist perspective being of dominant importance for legal professionals (e.g., when representing clients in court cases), and the realist perspective for law subjects (e.g.,

[20] Effectiveness here means that data subjects have effective rights rather than to safeguard their personal data.

when estimating the legal risks of behavioral choices). The positivist perspective provides a description of what a legal professional ought to do and the realist perspective of how what Oliver Holmes Jr. called 'a bad man,' will or will not be influenced by the behavior of the law's institutions (See Wendell Holmes Jr. (1897).

This two-perspectives approach is supported by the observation that "an appraisal of Chinese legislative products must invariably deal with two subjects: the lack of clarity, and the lack of consistency" (Otto (2000): 222). The first subject refers to the (positivist) problems of vague and broad provisions and their interpretation, while the second refers to the (realist) problem of poor compliance of lower law institutions with primary legislation (Otto (2000): 222).

This two-prong approach also finds support in the very recent study by Rappaport (Rappaport (2014) - to be published in the California Law Review). An important citation form this work:

> " ... the Court must decide whether to address its decision directly to rank-and-file officers or instead to political policymakers, such as legislators and police administrators, who in turn will regulate officers on the street. In the former, dominant model, termed here first-order regulation, the Court tells officers precisely what they can and cannot do. In the latter model, second-order regulation, the principal objective instead is to enunciate constitutional values and create incentives for political policymakers to write the conduct rules. Framed differently, the Court, as principal, enlists political policymakers as its agents in the regulatory enterprise. This Article is the first to apply an agency framework ... "

This quote shows that Rappaport's conceptualization of first-order and second-order regulation of law enforcement is quite coherent with my two-pronged approach (i) in the sense that the intended audience is important, (ii) in the sense that Rappaport's first-order regulation employs a positivist perspective and Rappaport's second-order regulation is only visible from a realist perspective, and (iii) in the sense that positivist and realist perspectives are not conceptually anomalous – their audiences may exclude each other, but both perspectives may help our understanding concurrently.

As Van Rooij (Van Rooij (2006)) and Li (Li *et al.* (2010)) observe, when violations are not met with sanctions, enforcement gaps' tend to cause legislation to fail to bring the intended effect in practice (Van Rooij (2006): 227). Consequently, any purely positivist assessment of China's data protection law is by no means exhaustive, especially when the comparison is made for measuring the strengths and weaknesses of the laws. The same may well be true for EU data protection laws. Thus, paying attention to both positivist and realist perspectives is crucial for understanding these laws.

The categorization of Chinese law

Investigating China's law from a comparative perspective always entails a latent question: what are the characteristics of the Chinese legal system? How do its civil elements compare with its Communist elements? Much of the comparative law literature focuses on how to categorize and typify different legal systems in legal "families." In the comparative-law literature, multiple efforts have been made to evoke images that typify the Chinese legal system. Three approaches (as identified in Otto (2000)) are mostly significant. The first is by David & Brierley (1968) who argue that:

> "any satisfactory categorization can only be based upon two criteria: legal technique and ideology" (Otto (2000):215)

The second is by Zweigert & Kötz (1998):

> "... focus on the criterion of "style" of a legal system: (a) historical background and development; (b) predominant and characteristic mode of thought

> in legal matters; (c) especially distinctive institutions; (d) the kind of legal sources acknowledged and the way they are handled; and (e) ideology" (Otto (2000):216)

The third is by Mattei (1997):

> "... arrives at a threefold distinction between legal systems: (a) a predominantly professional legal system, such as is found in most Western countries, (b) a predominantly political law, where the legal system is permeated by political interference, and (c) a mainly traditional legal system, found in countries in which religious or customary rules and institutions are predominant in the legal area" (Otto (2000):217)

Based on these three approaches, the Chinese legal system can be labeled in different ways: as a traditional/religious system; as a member system of the Laws of the Far East; as a mixed traditional/political System.

These established criteria for categorizing however, appear too simplified, stressing the similarities, but ignoring the diversity and variation. The categorizing approach may fit easily with a coherently organized legal system, but Chinese law is difficult to characterize, as it gives the impression of being something "esoteric," and a legal system that "absorbs elements from all relevant systems and experiences" (Otto (2000):230). Moreover, China's system is not based upon one coherent systematic model, but instead "consumes all kinds of legal food without a preconceived set of preferences" (Otto (2000): 230). Therefore, in this book, China's legal system is not explicitly and formally categorized into any family.

Terminology

EU jurisdiction

The key question that this thesis seeks to address is whether China can benefit from European experiences on data protection. Consequently, two jurisdictions, namely Europe and China, will be analyzed.

To consider Chinese law as a homogenous jurisdiction is not controversial, as what China is has almost always been derived from the concept of the "Heavenly Mandate," which has as its corollaries a unified political-cultural dynasty jurisdiction based on and supported by a unified written language for civil servants and a general attitude to consider foreigners as barbarians.[21]

On the other hand, arguing for a unified European perspective is considered more problematic, due to the heterogeneity of European political-cultural jurisdictions and languages.

In this book, nevertheless, the EU jurisdiction is taken as a unit of analysis. Indeed, until relatively recent, Europe has had a scattered history of continually changing governance systems and their geographical footholds. After a long history of cultural diversity and a series of full-scale wars, a serious effort started in the early 1950s to unite the European countries through international treaty. There is (and probably will be for the foreseeable future) a lot of debate among member states on the nature of the European Union. Still, one generally accepted objective is to unify these states into a single political-economic area, focusing on the free movement of people, and the free exchange of goods and services. The European legal system demonstrates a complex patchwork of homogeneity and heterogeneity. The rather recent developments of the EU towards a Union in law materially support considering (aspects of) European legal arrangements as a unified jurisdiction.

Cross-national commonalities are evident in the data protection field because of the harmonization efforts. Directive 95/46/EC's binding nature is expressly stated in that "the Member State shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive" (Büllesbach (2010):10). It set a blueprint for member-states to develop their national data protection laws in a manner that would not disturb the EU-level playing field on the market. With such provision, all member states had to converge on

[21] See, for instance, Ter Haar (2009)

the Directive 95/46/EC which represents a clear legal instrument containing principles that constitute high-level data on a union-wide scale (Büllesbach (2010): 13). Thus, for the sake of understanding European privacy issues in general, I adopt Philip Bobbitt's framework, which divides Western history in great wars (Bobbitt (2002)), considering the EU jurisdiction as a unit (and as an emerging part of the West).

Data protection law

Defining the scope of data protection law can be problematic. Data protection law may be referred to with labels as 'Data Protection Law' or the like, such as, for instance, the Directive 95/46/EC. Alternatively, it may be understood functionally, as legal arrangements seeking to influence the behaviors of data users or to protect the data subjects, irrespective of the title of the enactment. Then, the concept of data protection can be found dispersed in several published laws and institutions that uphold them. In this line of thought, the concept of 'consent' for instance, which may be functionally significant for the data subjects' right to participate in a service and that may be significant for a personal data user's legitimate processing, can be found in both EC (1995) and the 'Cookie Rule' (EC (2009)).[22]

Data protection law in this book, nevertheless, refers to the Directive 95/46/EC without any special indication. The

[22]Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users rights relating to electronic communications networks and services OJ L 337, 18.12.2009, at 11 (Nov. 15, 2009). For instance, at Article 5, Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications net work, or as strictly necessary in order for the provider of an information society service explicitly requested by the sub scriber or user to provide the service.'

reasons I focus on this Directive are as follows:

First, the Directive has proven so successful that data protection law has become "predominantly a European phenomenon" (Foutouchos (2005): 45).

Second, the Directive provides a general law that can be applied to any industry and activity related to data protection (Büllesbach (2010): 12). Consequently, in any thought experiment the practice would be covered by the Directive and its analysis would thus provide useful insights.

Third, the Directive 95/46/EC is the object of legislation, which is recommended by the literature to be transplanted to China (Hanhua Zhou (2006)).

Finally, the Directive largely defines the legal regime for data protection at the member-state level. In other words, the Directive takes a central role when looking for a formulation of the current European data protection system. All these considerations lead me to choose the Directive as the basic element for data protection in the European jurisdiction.

Privacy and data protection

Privacy is a conception with a long history, and appears to be widely accepted, if not always explicitly acknowledged (Whitman (2004)). Nevertheless, DeHert & Gutwirth (2006) attribute its legal founding to the publication of 'The right to privacy' in 1890 by Warren & Brandeis (1890). The paper was written to react against American journalism, wherein the authors complained about the journalists' lack of respect for people's "right to be let alone." However, privacy has evolved over the past century and has embraced many types that protect and vindicate individuals with regard to personal activities (Glancy (2000): 358). For instance, the core privacy rights in France are rights to one's image, name, and reputation; the core rights of privacy in Germany relate to the right to informational self-determination (the right to control the disclosure of information about oneself), and the core right to privacy in America is right to freedom from intrusions by the government (Whitman (2004): 1161).

However, data protection is a relatively new concept in the development of contemporary law. Its beginning is marked by the enactment of OECD data protection guidelines in 1980 (Solove (2006): 35). Data protection is a generic term that refers to all aspects of personal data processing, from a legal perspective, whether it is used by individuals or by organizations, and whether such use is with the help of computers, computer systems, computer networks, Internet, storage devices or communication devices. As OECD identified, "'Personal data' means any information relating to an identified or identifiable individual (data subject)" (Organization for Economic Cooperation and Development (2013):art.1(b)). The issues, revolving around data protection, are about collection and use and the protection of them (McFarland (2012)).

These problems related to data protection, which are usually discussed under the rubric of informational privacy, existed before the computer (McFarland (2012)). Or in other words, before the age of computing, the subject matter of data protection law was called informational privacy. According to Rainer Kuhlen, the ethics of informational autonomy is being conceived as "the capacity to choose and use autonomously knowledge and information in an electronic environment" (Kuhlen (2004)Capurro (2005):40). The conception of informational autonomy seems a prerequisite for Alan Westin's (Westin (1968)) description of privacy value, which is "the ability to determine for ourselves when, how, and to what extent information about us is communicated to others" (DeCew (2012)).

Throughout, I treat privacy and informational privacy as synonymous which is the origin of data protection and data protection law.[23] As Directive 95/46/EC claimed, the object

[23]In Gerrit-Jan Zwenne's inaugural lecture, he also used the terms "privacy" and "data protection law" as synonyms (Zwenne (2013):12).

The privacy concept as outlined in Art. 8 of the ECHR refers mainly to "the right to private and family life, respect of private home and private correspondence" (Council of Europe (1950)). However, the scope of Article 8 is continually extended. In 1979 the Case Klass V. Federal Republic of Germany (1979), government surveillance of telephone conversation was included into violation of art. 8 ((Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978). In the case Huvig V France (Application No.11105/84,

of data protection law is to protect the right to privacy, which is recognized in art.8 in the ECHR (EC (1995):2). The OECD guidelines even urged national laws for protecting personal data as part of their "law of privacy" (Organization for Economic Cooperation and Development (2013)). Thus, the two terms "privacy" and "data protection" are used synonymously in this book unless mentioned otherwise.

Data regulator

In this book, the data regulator concept includes several aspects. At the European level, it refers to the "European Data Protection Supervisor" which is set up based on "Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data", and to the "Data Protection Authority," which is set up in "every EU institution and body and works closely with the EDPS to ensure the internal application of the Regulation on the protection of individuals with regard to the processing of personal data by EU institutions".[24] The EDPS "is an independent EU body responsible for monitoring the application of data protection rules within European Institutions and for investigating complaints".[25] Additionally, the art. 29 working party, whose

Judgement of 24 April 1990) policy tapping of an individual business and private telephone lines were involved to be a violation of art. 8. In the case Harford V. United Kingdom, interception of private telephone calls made from business premises on a private telecommunication network was included into art. 8's scope ((20605/92) [1997] ECHR 32 (25 June 1997).). In the case Copland V. United Kingdom ((2007) 45 EHRR 37), monitoring of an employee's telephone calls, Internet usage and email at work constitute a violation of art. 8. The European Charter of Fundamental Rights separated to recognize the right to privacy (art.7) and the right to data protection (art. 8). Nevertheless, as Zwenne said, in his experience, the two terms are well understood and do not need further clarification (Zwenne (2013):12).

[24]The information is cited from the European data protection webpage, http://ec.europa.eu/justice/data-protection/bodies/index_en.htm

[25]Id.

opinions and interventions do not have binding forces but are nonetheless influential, is also considered to be a kind of data regulator. At the national level, the concept of the data regulator refers to the public data authority which is set up based on art. 28 of Directive 95/46/EC. And at the level of corporations, parts of the data regulator function are delegated to a corporate data officer. In each member state, the data authority is responsible for monitoring the applications of the national data protection law (EC (1995): art. 28 (1)) and being endowed with a set of powers and functions, which enable them to supervise (EC (1995): art. 28 (3)). What seems to me to be the most important aspect of the 'data regulator' concept is that parts of the regulatory powers as identified in incomplete law theory are delegated by the legislator and the administration to institutions or roles that have thus gained regulatory agency that allows them to react more adequately, quickly and with expertise, to emerging (mal) practices.[26]

Source of data

I collected data for analysis from the following sources, divided into two categories. The first category is the (published) reports, indicating the formal and informal practices concerning data protection in both China and Europe. Most data in Chapter 2 and Chapter 4 are collected through this channel. The data include reports by Article 29 Working Party, Some European Member States' data protection authorities, China's Ministry of Intellectual and Information, China's Supreme Court's report. I also collected information from some transnational law firms' reports and from international organizations.

The second category is the information collected from interviews. I conducted interviews during the years of 2008-2012. The interviewees include 5 professors in law schools, 10 staff-members in the Chongqing Branches of China's Credit reporting Center and of the Bank of China, 3 IT engineers, 1 lawyer,

[26]See also Rappaport (2014) where he discusses the regulation of the NSA behavior as an example of second order regulation through agency.

1 judge and 3 public servants. The interviews with the law school professors mainly focused on legal comparison and on legal transplantation. The other interviews are mainly for collecting information about practices. Except for Aiming Qi, Zhihai Xiong and Deliang Liu, all of the interviewees preferred to keep their names unpublished. Additionally, I conducted informal interviews with people from different fields, different educational backgrounds and different political backgrounds. The information thus collected helps me, not only evaluate my understanding of data protection situations in different fields, but also shape and update my conception of "privacy" and "personal data" in China.

Structure of the book

The book is organized as follows: in Chapter 2, I ask the question whether or not Chinese privacy legislation is indeed lacking vis-a-vis universally accepted privacy principles? Through comparing the legal arrangements over data protection issues, the answer is positive. The comparison helps to identify which aspects of data protection issues would be affected if China imports the European data protection law. In chapter 3, I adopt an historical and comparative perspective in order to explore the cultural implications behind informational privacy. In Chapter 4, I apply incomplete law theory to the development of data protection regulation in Europe. The evidence suggests that data regulators are efficient to address the incompleteness of data protection law in the European legal system. Subsequently, in Chapter 5, I argue that the incompleteness will be far worse in China since the necessary institutions that help combat incompleteness in Europe are not present. China's transplantation plan may be adjusted in order to respond to the threat of ineffective enforcement of highly incomplete law. Yet, China's policymakers should realize that in the short and medium run of establishing data protection institutions, data regulators might not work as effectively as we expect because of the complexity and dynamic features of the personal data protection issues. Chapter 6 provides conclusions and arguments that, because

EU law is better than no law, it is feasible for China to transplant the EU data protection law. However, transplantation will not be sufficient, because EU law suffers from incompleteness itself and matters will become even worse in China, given the lack of institutions. All in all, I conclude that we need new and additional ways of looking at data protection and perhaps complexity theory is a good starting point. Chapter 7 provides the arguments for qualifying the PDC as a CAS and follows through with a few recommendations, derived from CAS theory, about regulating the dynamical Personal data community. It also proposes ideas for future research.

Chapter 2

A Preliminary Comparison

Introduction

In previous Chapter, I sketch some of the issues that accompany Chinese policymakers' intentions to import European data protection law in order to improve the protection of personal data at home. However, such a sketch does not address the fundamental question of exactly how the Chinese and European data protection legislations are different. Or, in other words, how can the European data protection law improve the quality of data protection in China? Answering these questions requires a comparative examination. This offers the starting point for a more in-depth analysis of China's legal importation plan.

This chapter aims to capture some of the coarse-grained differences between Europe and China in terms of data protection legislation. In order to see how the EU data protection law could upgrade China's legal arrangement, I employ an elaborate thought experiment as a heuristic tool. In particular, I consider a single set of facts and then examine how these facts would transpire in Europe compared to China. My approach follows (but adapts) functional comparison. Traditionally, functional comparisons, as suggested by Zweigert and Kötz (Zweigert & Kötz (1996)), assume that different societies have similar needs

and that to survive any society must have (functionally equivalent) institutions that meet these needs (Michaels (2005):363). Such conventional approaches are predominantly based on similarity and have therefore been criticized (Michaels (2005):363). My approach in this Chapter emphasizes instead the differences between the two regions' legal arrangements on data protection. This adaptation is greatly influenced by Bignami's work, which explores the solutions to a hypothetical problem in two different legal systems under comparison (Bignami (2007): 677). His study focuses on the legal differences, instead of similarities, between Europe and America over data protection and allows him to propose a number of recommendations for the reform of U.S informational privacy law (Bignami (2007): 677). I employ a similar adapted functional comparison approach in order to formulate recommendations for updating China's data protection law through learning from European experiences.

To capture the differences of data protection arrangements between Europe and China, I assume that Europe is required to regulate a hypothetical Credit Reporting Database Center (hereafter the CRC), an actual database in China. In this way, I investigate how such a giant program, as regulated in China, would be understood in Europe.

The CRC is a department/bureau of People's Bank Of China (hereafter PBOC). It is located in Shanghai and was founded in 2006 through legislation. The CRC houses a series of databases, relevant to credit-reporting services. Major databases include the National Database for Consumer Credit Reporting (hereafter the Database) and the National Database for enterprises. I will focus on the first one, since the second database focus on enterprises' information. My study of the database and its use was conducted via literature reviews and interviews during my fieldwork in 2011 and 2012.[27]

Various data furnishers, including creditors and lenders, such as commercial banks and rural credit cooperation; debt collection agencies, such as trust companies, financial companies, automobile financing companies, micro-lending companies; and public utilities, such as the social security department, the public reserve funding, the tax department and courts, provide personal information, financial data and alternative data on individuals to the CRC (Xi Ai (2006); Jentzsch (2005)). The CRC collects these "raw" data and then aggregates them into the database's data "repository". The aggregated data is made available on request mainly for the purpose of credit risk assessment. Until the end of 2013, the database had collected 830 million records with personal information.[28] The CRC claimed that the database is the biggest credit database in the world, with the largest amount of information.[29]

The possibility of data protection issues has become the CRC's center of attention, considering that the collected data is tightly correlated with the data subjects' welfare. This is reflected on the concern for data protection regulation. Multiple regulations, including People's Bank Of China (2005a,b, 2006), have been enacted in order to ensure the adequate protection of personal data. Given the generally high degree of data protection awareness, the regulation on the Database provides a benchmark for China's data protection level. Thus, I "transplant" the CRC from China into a hypothetical European member-state in order to bring into focus the differences between the two regions.

For the comparison, I used a set of indicators, in order to identify the items that China's data protection arrangement is lacking. I adopted these indicators to avoid being hampered by lengthy documents that incorporate an excessive amount of details. Additionally, the indicators work as a common language on the legal arrangements of two different jurisdictions. Out of several data protection standards, I selected the "Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data" (Organization for Economic Cooperation and Development (1980), hereafter OECD 1980), because it is regarded

[27] Interviews are significant to help me get access to the actual performance of the Database which is not open to public. The interviews were kindly supported by Li Jie, Yin Yao, Xiong Jia, and Zhang Yajie.

[28] See the CRC website, http://www.pbccrc.org.cn/zxzx/zxgk/gywm.shtml, from which the information is gained.

[29] Id.

as "the basis of data protection legislation around the world" (Cavoukian (2000):8). The OECD 1980 is one of the earliest attempts to deal with data protection and trans-border data flow, considering that it has the dual aim of achieving acceptance of minimum standards of data protection, as well as reducing the obstacles that may restrict the free flow of data (Kuner (2011):14). Even though it is not legally binding, the OECD 1980 contains a widely accepted set of standards. Even today, its basic privacy principles are still considered to be a relevant general data protection framework (Kuschewsky (2013):2). On September 9, 2013, the OECD 1980 was updated to OECD 2013, due to the clear shift in data-using technology for the past three decades. Early on, the OECD 1980 was established in a time when the technological horizon was determined by databases and "island" computing. Yet, current new technologies have supported "global accessibility and continuous, multipoint data flow" (Organization for Economic Cooperation and Development (1980):20), while "a wide range of analytics has provided comprehensive insights into individuals' movements, interests, and activities" (Organization for Economic Cooperation and Development (1980):20). The OECD concluded that it was an "appropriate time" to adjust the OECD 1980 in order to offer more effective safeguards to protect privacy (Organization for Economic Cooperation and Development (1980): 20). Therefore, in this Chapter, the OECD 2013 is used as the instrument for measuring the differences between European and Chinese legal arrangements over data protection issues.

The Chapter is structured as follows: Section 2 presents the OECD 2013 Guidelines, which I use to identify the differences between the two jurisdictions. Section 3 describes the CRC database in more detail, followed by an assessment of China's applicable laws. Section 4 provides the assessment of European law when measured with the same standards. The final section reveals how the CRC would come into conflict with the European law and explores the consequences of the comparison.

Indicators: OECD Principles

The OECD 2013 has six parts: a. General; b. Basic principles of national application; c. Implementing accountability; d. Basic principles of international application; e. Free flow and legitimate restrictions; f. National implementation and g. International cooperation and interoperability (Organization for Economic Cooperation and Development (2013)). In this book, I focus on the key points and order them into three clusters: 1. Data subjects' rights, 2. Data users' responsibilities and 3. Regulatory guidelines. For each cluster, I identify a list of items for appraisal. The appraisal is done in the positivist[30] manner: I look at how well the text of the laws represents the OECD 2013 principles and other indicators. Since each of the core aspects that are employed, as indicators will be introduced when looking at China's legal arrangements, here they are only mentioned (and the provisions they are collected from):

1. Data subjects' rights: the right to access (Provision 13 (a) (b) (c)), the right to challenge (Provision 13 (d)) (Organization for Economic Cooperation and Development (2013)).

2. Data users' responsibilities: collection limitation principle (provision 7); data quality principle (provision 8); purpose specification principle (provision 9); use limitation (provision 10); security safeguards principle (provision 11); openness principle (provision 12); accountability (provision 14); implementing accountability (provision 15) (Organization for Economic Cooperation and Development (2013)).

3. Implementation: free flow of data (provisions 17, 18, 20, 21, 22); to adopt a privacy law (provision 19-b); national privacy strategy (provision 19-a), privacy enforcement authorities (provision 19-c), encourage self-regulation (19-d), reasonable means for individuals to exercise their rights

[30] For the meaning of "positivist manner," see Section 5 of Chapter 1.

(provision 19-f); adequate sanction (provision 19-f); complementary measures (provision 19-g) and against unfair discrimination (provision 19-i) (Organization for Economic Cooperation and Development (2013)).

Table 2. 1 below lists the three clusters and the relevant items in each category.

Data subjects' rights	**Data users' responsibilities**	**Implementation requirements**
To access	Collect limitation	Free flow of data
To challenge	Data quality	A formal law
	Purpose specification	A national strategy
	Use limitation	Enforcement authority
	Security safeguards	Self-regulation
	Openness	Reasonable means
	Accountability	Adequate sanctions
	Implementing accountability	Complementary measures
		Unfair discrimination

Table 2.1: Inventory of core aspects (the positivist measure sticks)

Thee National Credit Reporting Database

Here I illustrate through a personal narrative how a Chinese data subject can be affected by China's national credit reporting database.

One day, when applying for a new credit card, I found myself in front of a creditor's table in the Bank of China (BOC). I was asked to provide a copy of my financial history (a credit report), which the creditor would use to determine whether to approve my application and what rates to offer. With my authorization, the credit report would be provided by the CRC after the creditor's request. The contract for authorization asked for

my name, date of birth, home address, email address, gender, my ID number and a copy of my identification document, my job details and the address of the company I work for, and my income information. Before signing the contract, I asked what would happen if I did not sign, to which the creditor kindly told me: "Miss Zhang, unfortunately, we cannot issue a credit card to you without the credit report." Therefore, to receive the credit card, I was obliged to sign the contract and accept the automated decision-making.

When the CRC received my creditor's request, the clerk there would search my credit profile. Soon after, the amount of debt I have and how long I tend to take before paying my bills, become tracked and recorded through my credit profile. But individual credit profiles need not be limited to these records. For instance, if I had or am having litigation in any court, if I did not pay any energy bills on time, or if I tried to deceive an insurance company, my credit profile will keep track. The database 'knows' nearly everything about my financial life.

For its database to perform this, CRC employs data resources from the whole financial industry in China (Xi Ai (2006)). In order to collect data, the database cooperates with almost all banks in China, including the four state-owned banks, the joint stock commercial banks and commercial alike (Xi Ai (2006)). These partners hand over their collected information to the database and update their records periodically (Xi Ai (2006)). The database does not record only financial data. For instance, the Social Security Department's database is open to the CRC, which records the information about fraudulent insurance claims (Xi Ai (2006)). Additionally, all the databases in the personal housing accumulation funds, communication firms, water companies, gas companies and judicial system institutions, are open to the CRC (Jentzsch (2005): 21). Among these cooperative databases, most notable is the National Identity Database in the Public Security Department (Jentzsch (2005): 24).[31] The

[31] According to the database's introduction, the National Identity Database was introduced in 2001 and it is the most important system supporting increased social services. The main (not the only) function it performs is to validate the identity of an individual. Moreover, the database is used for co-

National Identity Database and the Database are connected in order to solve the problem of fraudulent personal information (Jentzsch (2005): 24). Customers might be motivated to provide false names, addresses and other personal information for various reasons, which may reduce the efficiency of credit reporting. Thus, the CRC cooperates with the National Identity database for ID verification (Jentzsch (2005): 24).

Once the "raw" data is collected from data furnishers, the CRC "cleans" it, mainly through data archiving, matching, collation and storage, in order to make the data ready for processing. Then, the cleaned data related to a specified consumer are added to his personal credit 'file'. The data file is the 'economic ID' of the subject because it helps trading partners know the credit identity of the ID holder. In my case, the database found my file, which had compiled information on me, and generated a credit report, built on my past financial habits and behavior. It is subsequently used to predict my future behavior. The credit report thus concludes whether to issue a credit card to me and, if so, what rate of credit I can afford. My personal welfare is influenced by the data processing of the database since the creditor makes his decision based on this report.

The adequacy of Chinese data protection legislation

Although China does not have a law labeled as "data protection law", there is a set of rules, tailored to regulate the Database including data protection issues. These rules are the Interim Measures for the Administration of the Basic Data of Individual

ordinating systems across government agencies. In fact enormous amounts of personal information on administrative affairs, like tax payments, are accumulated and then integrated into one database in this way. The Identity Database provides immense benefits and is effectively contributing to cost reduction through increasing operational efficiency as well as systematized operation. Outside the governmental system, the Identity Database is broadly used for private-sector services, for instance when opening a bank account and using credit reporting services. (Information about the National Identity Database is available at http://www.nciic.com.cn).

Credit Information (People's Bank Of China (2005a), hereafter Measure 2005), the Procedures for Searching One's Own Credit Report from the Individual Credit Information (People's Bank Of China (2006)), and Procedures for Handling Disputes about the Individual Credit Information Database (People's Bank Of China (2005b)). All the rules were promulgated by the PBOC. Although the scope of application of the three rules is limited, it is because of their existence that the CRC displays a (relatively) high level of data protection in China (Jia Yao (2008)). Measure 2005 in particular, safeguards the security of individual credit information in the CRC, as well as its legitimate use, covering important aspects of data protection, while the other two focus on procedural issues. An analysis of Measure 2005 may therefore help understand the Chinese policymakers' perceptions of the role of data protection, as it documents their responses to challenges emerging due to massive data mining practices. And the other two rules may be analyzed when procedural issues are involved. In this section, I will use the indicators drawn from the OECD 2013 to evaluate Measure 2005.[32] Through the interpretation of Measure 2005, in light of the indicators, I will show preliminary evidence from a positivist perspective about the qualities and the deficiencies of Measure 2005 as a regulator of data protection issues.[33] My perspective is positivist.[34]

[32]In 2013, the State Council issued the "The Regulation on the Administration of Credit Investigation Industry". The Order is to "regulate credit investigation activities, protect the legal rights and interests of the parties concerned, guide and promote the healthy development of credit investigation industry and enhance the building of the social credit system". (art 1 of the Order). However, the Order is much closer to regulate Credit Reporting market's entry than to manage credit database's practice. Therefore, I will not pay attention to this Order.

[33]Every now and then however, I could not resist inserting comments of a realist nature. These realist comments are between brackets.

[34]The meaning of "positivist" is explained in Chapter 1, Section 5.

Data subjects' rights

The right to access (provision 13 (a) (b) (c)) The right is guaranteed by the Directive in art. 12. Every data subject has the right to get access to his personal data without constraint (EC (1995): art.12). The contents that data subjects could obtain include, at least, the purpose of processing, the categories of the data concerned, the recipients or categories of recipients to whom the data is disclosed, and the logic involved in any automatic processing of data concerning the data subject in the case of automated decision (EC (1995): art.12 (a)).

The right to challenge (provision 13 (d)) Art.12 of the Directive enables the data subjects to rectify inaccurate data and unlawful processing (EC (1995): art.12 (b)). Art. 12 also enables data subjects to delete data if the data processing is unlawful (EC (1995): art.12 (b)). Deletion can be effected either by erasure or by blocking (EC (1995): art.12 (b)). According to the Directive, contacting the third parties to whom the data have been disclosed, for the rectification, deletion or blocking of data, is mandatory, "unless this proves impossible or involves a disproportionate effort" (EC (1995): art.12(c)).

Apart from these basic data subjects' rights, the Directive has a special right granted to data subjects. That is the right to object to the processing of personal data (EC (1995): art.14). Art.14 (a) grants "the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data" Art. 14 (b) identifies a specific right to be informed before any personal data are disclosed to third parties or to be used for direct marketing purposes, and the right to object, free of charge, to such disclosure or use (EC (1995): art.14). These rights are believed to help data subjects have better control over their personal data (Büllesbach (2010): 81-82).

Data users' responsibilities:

Collection limitation requirement (provision 7) As I analyzed above, consent is the key element of the collection limitation requirement. In the European data protection law system, the role of consent is recognized by the EU Charter of Fundamental Rights as an essential aspect of data protection and as a fundamental personal right. Article 8 (2) of the Charter states that personal data can be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law" (European Union (2012)).

In the Directive, consent means, "any freely given specific and informed indication of the data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed (EC (1995):art.2(h)). "Consent" forms a general ground for lawful and fair data processing (EC (1995): art. 6 (1)). In art. 7, consent is the first of the six foundations for legitimate processing of personal data (EC (1995): art.7 (a)). Article 8 provides the possibility of using consent to legitimize the processing of special categories of (sensitive) data, which would be otherwise prohibited (EC (1995): art.8).

In 2011, the art. 29 working party, which is established according to the Directive 95/46/EC, issued "Opinion 15/2011 on the definition of consent" to clarify matters and to ensure a common understanding of the existing legal framework (Article 29 Working Party (2011): 21). According to the Opinion's explanation, for non-sensitive data, the unambiguous consent of the data subject, either explicit or implicit in form, is sufficient to constitute a legal basis for processing personal data (Article 29 Working Party (2011): 21). According to art. 29 working party's Opinion, consent "encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing" (Article 29 Working Party (2011): 25). For sensitive data, art. 8 provides that these special categories of data could not be processed unless the data subject has given explicit consent (EC (1995): art.8 (2)(a)). In this case, consent is usually given

in writing with a hand-written signature (Article 29 Working Party (2011): 25).

Art. 7 starts with consent, and proceeds to list other legitimation grounds for which consent is not required, including processing that is necessary for the vital interests of the data subjects and for the prevailing legitimate interests of the controller or third parties, including the public interest (EC (1995): art. 7 (b)-(f)). The Art. 29 working party's Opinion mentions that consent "does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality"(Article 29 Working Party (2011): 7). Data subjects can withdraw consent if the processing breaches fairness, relevance and proportionality.

Data quality requirement (provision 8) In the Directive 95/46/EC, data quality is reflected on two requirements. One is the relevance of data (art. 6, para 1 (c)), and the other is the accuracy of data (art. 6, para 1 (d)) (the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013): 73). First, data should be processed in a manner "adequate, relevant... to the purpose for which they are collected and/or further processed" (EC (1995): art.6, para 1(c)). This requirement aims to minimize the collection of data in order to avoid data abuse (Büllesbach (2010): 53). Second, art. 6, para. 1 (d) requires data controllers to ensure data accuracy and to keep them up to date. Data controllers must ensure the quality of data, irrespective of whether data subjects demand data corrections (Büllesbach (2010): 53; the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013): 74).

Purpose specification requirement (provision 9) The requirement is identified in art. 6 para. 1 (b) (EC (1995)). The article requires data controllers to process data for specific purposes and to subsequently use or transfer data only where this is compatible with the purpose of collection (EC (1995): art. 6

(1) (b)). According to the Directive, the data processing purpose must be sufficiently specific, explicit and lawful, while the data subject must be informed of the purpose, at latest when the data are collected. Once the purpose of data collection is defined, further use is not legitimate if contrary to the expectations evoked by the information given about the purpose ((Büllesbach (2010): 52).

Use limitation (provision 10) The requirement is clarified in art. 6 (1)(c), which states that data should be processed in a manner "not excessive in relation to the purpose for which they are collected and/or further processed" (EC (1995) :art.6(1)(c)). Excessive use is unlawful unless the processing has a legal basis. Otherwise, data cannot be used even though they have been initially acquired (Büllesbach (2010): 70).

Art. 6 (1) (e) also relates to the use limitation requirement, stating that the time limitation for storing personal data is only "necessary for the purposes for which the data were collected or for which they are further processed"(EC (1995): art.6 (1)(e)). It is the national legislators' duty to make a timeframe and to make sure that personal data are deleted as soon as the time limit for storage has been reached (Büllesbach (2010): 53). (Chapter 3 will discuss the retention issue.)

Security safeguards requirement (provision 11) In art. 17 of the Directive, both data controllers and data processors are required to take necessary measures, either technical or organizational, to keep the data secure (EC (1995)). The Directive recommends hierarchical security mechanisms, based on the risk connected to data processing, as well as the nature of data (Büllesbach (2010): 87). For instance, sensitive data, such as health data, and the CRC large database, require more sophisticated security measures (EC (1995): art. 17-1). Nevertheless, data controllers can decide themselves to choose security measures, which can provide adequate protection after assessing the risks of data processing as well as the costs involved in addressing those risks (Büllesbach (2010): 87).

Openness requirement (provision12) This requirement is clarified by art. 10 and art.11 of the Directive, aiming to ensure that data subjects know how their personal data are used (EC (1995)). The two articles describe the information that must be provided to data subjects, and, in this regard, distinguish between the situations in which the data are obtained directly from the data subjects (obtained data subjects' consent) (art.10) and situations in which the data are obtained from other sources (did not obtain the data subjects' consent) (art.11) (Büllesbach (2010): 66). In the first situation, critical information, including "the identity of the controller and his representative; the purposes of the processing... and further information such as recipients or categories of recipients of data; whether replies are obligatory or mandatory and the existence of rights," should reach the data subjects (EC (1995): art. 10) In the second situation, the data subjects should be notified either at the time of the recording of personal data, or at the first disclosure to a third party (EC (1995):art.10). The contents of the notification should include the same information as mentioned in the first situation.

Accountability (provision 14.15) The Directive mentions in several articles the importance of promoting compliance in order to implement accountability. For instance, art. 20 requires a prior checking mechanism in order to avoid unnecessary processing operations, such as processing sensitive data, data on offense, genetic data, which may present specific risks to the rights and freedoms of the data subjects (Büllesbach (2010):101). The Directive empowers the national data protection supervisory authority to perform such prior checks (EC (1995): art.20 (b)). The role of the personal data protection 'official' appointed by data processors also aims to ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations (EC (1995): art.18 (2)).

Furthermore, in order to clarify the accountability, art. 29 working party enacted "Opinion 3/2010 on the principle of accountability" (Article 29 Working Party (2010a)). The essence

of 'accountability', from the art. 29 Working party's perspective, could be outlined as the controller's obligation to:

> "put in place measures which would – under normal circumstances – guarantee that data protection rules are adhered to in the context of processing operations; and have documentation ready which proves to data subjects and to supervisory authorities what measures have been taken to achieve adherence to the data protection rules" (the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013):79).

Thus, the accountability requirement in the Directive orders data controllers to actively prepare documentation that can, when necessary, show their compliance with the Directive and national laws (in practice), and warns them not to merely wait for data regulators to point out shortcomings (the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013): 79).

Implementation

Free flow of data (provision 17, 18, 20, 21, 22) The Directive has two main objectives, ensuring the free flow of data and protecting data subjects. In art. 1 (2), the Directive establishes a uniform level of data protection within the EU, which allows a free flow of personal data among member states (Büllesbach (2010):113). However, outside of the EU, various interests should be considered. Such onward transfers are only permitted when the receiving countries offer an adequate level of protection, which, according to Article 25 (6) of the directive, is assessed by the European Commission (EC (1995):art. 25). The European Commission's assessment binds member states to take the necessary measures in order to comply. The art.29 Working Party has substantially contributed to this issue. In the working paper, "Transfers of personal data

to third countries: Applying Articles 25 and 26 of the EU data protection directive", the art. 29 working party identified the core aspects and mechanisms for assessment (Article 29 Working Party (1998)). According to the working paper, the core aspects of Directive 95/46/EC include "the purpose limitation principle, the principle of data quality and proportionality, the principle of transparency, the security principle, the rights of access rectification and opposition, the restrictions on onward transfers to other countries, the principle of special protections to sensitive data, direct marking, automatic individual decisions, and enforcement mechanisms" (Article 29 Working Party (1998)). Based on this set of assessment tools, certain countries have been recognized as having an equivalent data protection level.[35] Between Europe and the USA, there is a notable adequacy decision, known as "Safe Harbor Agreement". Companies can voluntarily join the Safe Harbor Agreement (the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013):141), although this bilateral agreement was elaborated mainly for American companies. They are required to declare to be subjected to the supervision of the US Commerce Department and must be documented in a list published by that department (the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013):141).

[35]These tests included New Zealand (Opinion 11/2011 on the level of protection of personal data in New Zealand), the Eastern Republic of Uruguay (Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay.), the Principality of Andorra (Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra 2009), Israel (Opinion 6/2009 on the level of protection of personal data in Israel), Faroer Islands (Opinion 9/2007 on the level of protection of personal data in the Faroe Islands), Jersey (Opinion 8/2007 on the level of protection of personal data in Jersey), the Isle of Man (Opinion 6/2003 on the level of protection of personal data in the Isle of Man), Guernsey (Opinion 5/2003 on the level of protection of personal data in Guernsey), Argentina (Opinion 4/2002 on adequate level of protection of personal data in Argentina), Australia (Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000), Canada (Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act), Hungary (Opinion 6/99 concerning the level of personal data protection in Hungary), Switzerland (Opinion 5/99 on the level of protection of personal data in Switzerland).

Article 26 of the Directive identifies some of the situations that could justify the transfer of personal data to an inadequately protected third country. These situations include: the data subject giving unambiguous consent (EC (1995): art. 26 (a)); performing a contract between data subject and data controller (EC (1995): art. 26 (b)); concluding or performing a contract between a data controller and a third party (EC (1995): art. 26 (c)); public interests (EC (1995):art. 26 (d)); protecting the vital interests of the data subject (EC (1995):art. 26 (e)); and legitimate access to public registers (EC (1995):art. 26 (f)).

To adopt a privacy law (provision 19-b) Europe has a well-established data protection law system. At the European level, two instruments, the European Convention on Human Rights and the Directive 95/46/EC, form a basic legal framework which covers all European member states and all data-using services. At the national level, each member state enacted its own data protection law on the base of Directive 95/46/EC.

National privacy strategy (provision 19-a) It is the responsibility of member states to establish national privacy strategies. In the Directive, no law text on the subject is available.

Privacy enforcement authorities (provision 19-c) Art. 28 require each member state to establish one or more public authorities responsible for data use supervision (EC (1995): art.28). The Directive requires independent supervision as an important mechanism, with its powers and capacities to ensure effective data protection (EC (1995): art. 28).

Encourage self-regulation (19-d) The Directive encourages trade associations and other bodies in each member state to draw up their own codes of conduct (EC (1995): art. 27).

Encouraging self-regulation aims to facilitate the implementation of the national law, taking into account the specific features of the various sectors ((the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013): 105). Self-regulation could concretize the national laws with respect to the experiences, interests, specific circumstances and characteristics of the processing carried out in certain sectors (Büllesbach (2010): 126). In order to make sure that the self-regulation does comply with the national law, the national supervisory authority should evaluate these codes of conduct (EC (1995): art. 27).

Reasonable means for individuals to exercise their rights (provision 19-f); According to the Directive, there are three approaches for data subjects to exercise their rights. The first approach is to request access from the data controller, since data subjects are entitled to the right to access (EC (1995): art. 12(a)). Second, data subjects could lodge a claim with the national data protection supervisory authority concerning the protection of rights and freedom (EC (1995): art. 28(4)). The supervisory authority must keep the data subject informed about the outcomes of the proceeding (EC (1995): art. 28(4)). The supervisory authority is also empowered to intervene by checking the lawfulness of such operations even if no data subject lodged a claim (Büllesbach (2010):136). The third approach is that data subjects are entitled to bring a complaint before a national court (EC (1995): art.28 (3)).

Adequate sanctions (provision 19-f); The Directive requires each member state to provide adequate sanctions for breaches of national data protection law (EC (1995):art.24). It gives member states a wide margin of discretion in choosing the appropriate sanctions and remedies (the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights (2013): 132). In Büllesbach (2010), the authors outlined the sanctions which have appeared in different national

legislations, including administrative fines, criminal fines, imprisonment, informal sanctions and future changes (Büllesbach (2010): 110-112).

Complementary measures (provision 19-g) The complementary measures are not to be found in the Directive.

Discrimination (provision 19-i) The Directive advocates against the discrimination of any data subject. For instance, everybody is entitled to the right to access, not only the data subjects whose data is processed, but also the requesting person who is not processed by the requested party (Büllesbach (2010): 74). Additionally, the right also pertains to non-citizens of member states of the EU (Büllesbach (2010): 74).

Conclusion

This chapter, using documentary evidence and interview results, compares the European general legal system and the Chinese credit reporting legal arrangements over data protection issues, and provides a positivist assessment of the data protection level in the two regions based on a set of indicators, derived from OECD 2013. Gaps between the two regions on data protection issues are marked. The comparison reveals that European data protection laws generally protect the principles of informational privacy, as embedded in OECD 2013, more completely than Chinese laws do (if available at all).

Consequences of the comparison

The analysis in previous sections provides evidence that in Europe the CRC database would be in danger of being deemed illegal, since its operations violate three types of privacy guarantees under European data protection law. Below, I analyze the three types one by one.

A substantive difference concerning data subjects' rights Both regions recognize the rights to access and challenge, as in

the OECD 2013. Yet, the right to object, which can be considered a type of the right to challenge, is specific of European data protection law and is not observed in Chinese laws. The following table illustrates the finding above.

OECD 2013	Access	Object	Challenge
95/46/EC	Complied	Complied	Complied
Measure 2005	Complied	Non-complied	Complied

Table 2.2: Summary of positivist comparison for data subject's rights

Substantive differences concerning data controllers' obligations The Directive recognizes all OECD principles on the data controllers' obligations, while Chinese Credit Reporting Laws lack the collection limitation principle, the use limitation principle, the openness principle and the accountability principle. This finding is illustrated in the following table.

Directive 95/46/EC	OECD 2013	Measure 2005
Complied	Collection Limitation Principle	Non-complied
Complied	Data Quality Principle	Complied
Complied	Purpose Specification Principle	Complied
Complied	Use Limitation Principle	Non-complied
Complied	Security Safeguards principle	Complied
Complied	Openness Principle	Complied
Complied	Accountability	Non-complied

Table 2.3: Summary of positivist comparison of data user's responsibilities

Procedural differences concerning implementation European data protection law, except for the national strategy,

which was only incorporated into the OECD guidelines in 2013, largely recognizes the implementation principles. Yet, Chinese law lacks most of the procedural core issues. Only three principles are found in China's system, including "reasonable means for individual to exercise their rights, adequate sanctions and complementary measures." The following table illustrates the finding concerning implementation.

Directive 95/46/EC	OECD 2013	Measure 2005
Complied	Free flow of data	Non-complied
Complied	To adopt a privacy law	Non-complied
Non-complied	National privacy strategy	Non-complied
Complied	Privacy enforcement authority	Non-complied
Complied	Encourage self-regulation	Non-complied
Complied	Reasonable means	Complied
Complied	Adequate sanction	Complied
Complied	Complementary measures	Complied
Complied	Unfair discrimination	Non-complied

Table 2.4: Summary of positivist comparison for regulatory/enforcement principles

Again, Chinese positive laws on data protection for credit reporting lag seriously behind Directive 95/46/EC when looked at through the lens of OECD 2013. Perhaps, the procedural omissions are, in practice, the worst yet. A particular indicator of the difference in the level of data protection between China and Europe can be found in the absence of a data protection authority in Chinese law. Since the database under scrutiny is authorized by public regulation for national financial ends, it has become an important source for government data mining. Simultaneously, no national supervisory authority needs be consulted, nor is such an authority required to have oversight and enforcement powers over evolving practices. The procedural requirements are to minimize the government's interference with private life. However, these procedures are not only absent in the CRC's laws, they are especially absent in practice.

Can EU law improve Chinese law?

Based on the comparisons conducted above, it is now safe to conclude that if Chinese policymakers introduced the European data protection law, that could largely upgrade Chinese legal arrangements in terms of data subjects and their personal data. In my positivist analysis of European data protection law, I have shown that the law serves data protection better than China's legal arrangements do (when present at all). I propose the following steps as a starting point for such improvement.

First, it is necessary for China to develop a more general data protection law, which can relate to all CRC-like programs that involve large-scale personal data collection and processing. Drawing on European experiences, China's legal arrangement over data protection would only need be modestly changed by adding the right to object, and the principles of collection, use limitation, openness and accountability, on the basis of Measure 2005 (and by making its scope more universal).

Second, an independent data protection authority should be included in the law, while ensuring it does not become an ineffective institution in practice. An independent data protection authority is not irrelevant as China's policymakers thought. It all may depend on whether several important other differences between the two jurisdictions (for instance of a cultural nature) would allow or even support such an institution to succeed.

The conclusion in this Chapter supports the transplantation hypothesis. Nevertheless, it has been pre-mature to support the transplantation proposal, since China has its own pre-existing cultural background on information privacy, which may possibly influence the efficacy of importing law. In the following chapter, I will discuss cultural differences between China and Europe over privacy issues in order to explore whether may make the success of the transplantation disputable.

Chapter 3

Do History and Culture Matter?

Introduction

In the previous Chapter, by comparing them from a positivist position, I discovered that the European data protection law is much more comprehensive than the Chinese one. The subsequent question is: 'why did China fail to generate its own, effective and equally detailed data protection laws as in Europe?' The answer may be provided by exploring the cultural background of privacy in each region. Cultural backgrounds can have long-term impacts that are perpetually experienced (Nunn (2009)). The specific mechanisms underlying culture may help shape different behavioral rules in different cultural traits (Boyd (1988)). Similarly to behavioral rules, law itself is influenced by culture as well (Jolls (1998)).[36] In fact, this claim has been proven by the role of culture in shaping what privacy is and how it should be protected; as Johnson said, 'privacy as a conventional concept is socially or culturally defined' (Johnson (1989)). According to his analysis, the cultural or socially defined nature of privacy is the reason why it varies depending

[36]Law, as a behavioral rule, is about "infusing law...with insights into actual...human behavior when such insights are needed to insure sound predictions or prescriptions about law" (Jolls (1998):1654)

on context (Johnson (1989)).

However, today privacy is replaced by (or being adapted towards) informational privacy data protection in cyberspace, raising the question whether culture influences informational privacy as well. If culture does shape data protection law, Chinese policymakers must carefully examine cultural views and attitudes before allowing European data protection importation. Otherwise, the differences in cultural attitudes over privacy and over informational privacy may, in practice, prevent the imported data protection law from becoming rooted in China's legal system, endangering the data protection law transplantation scheme.

In order to explore the role of culture in shaping data protection law, I conducted my investigation based on a comparative, cultural-historical perspective. Laws in action may prove quite different from laws in writing and, like language, legal systems may evolve through actual communication practices, turning out to be quite different in different cultures. My findings may help China's policymakers gain insight into how to avoid the potential social cost that could emerge from ignoring cultural differences. It is important to specify exactly what I mean by culture in this Chapter before proceeding to the investigation, due to the complicated and broad features of culture.[37]

I use the term "culture" to refer to "cultural value patterns". As Hofstede identified, cultural value patterns emerge when "similarities and differences across societies are explained and predicted theoretically using dimensions of cultural variability" (Edmundson & Global (2013)). In an empirical research on IBM employees from 1966 to 1978, Hofstede derived four dimensions of cultural value patterns: power distance; collectivism versus individualism; femininity versus masculinity; and uncertainty avoidance (Hofstede *et al.* (1997)). Among the four dimensions of cultural value patterns, the 'individualism versus collectivism' dimension is the most relevant to privacy. This dimension displays the relation between the role of the individual and the role of the group in a society (Hofstede *et al.* (1997):74). According to Warren's seminal article (Warren & Brandeis (1890)), the respect of privacy is the respect of the 'right to be let alone'. Even though privacy has evolved over the past century and has encompassed many mechanisms that protect and vindicate individuals regarding personal activities, the fundamental underlying contents of privacy are about the relation between individual and society at large (Glancy (2000): 358). This is demonstrated exactly in the dimension of individualism-collectivism. Therefore, in this Chapter, in order to keep focus and not be diverted into far too complex a cultural discussion, I limit the term "culture" to refer to the dimension of Individualism versus Collectivism (Hofstede *et al.* (1997)). My analysis of cultural attributes that influenced the shaping of privacy and informational law in Europe and China is based on this dimension.

The Chapter is structured as follows. Section 2 describes the cultural backgrounds of privacy in Europe and China, followed by the exploration of the nuances emerging due to the differences in valuation. Section 3 discusses how these differences in valuation unfold in recent times, considering that developments in the digital environment (like data mining, cloud computing, social media, terrorism and market-based thinking). Sections 4 offer an evaluation of my findings.

[37] As described by Velkley: "The term 'culture,' which originally meant the cultivation of the soul or mind, acquires most of its later modern meanings in the writings of the 18th-century German thinkers, who were on various levels developing Rousseau's criticism of "modern liberalism and Enlightenment". Thus a contrast between 'culture' and 'civilization' is usually implied in these authors, even when not expressed as such. Two primary meanings of culture emerge from this period: culture as the folk-spirit having a unique identity and culture as cultivation of waywardness or free individuality. The first meaning is predominant in our current use of the term 'culture,' although the second still plays a large role in what we think culture should achieve, namely the full 'expression' of the unique or 'authentic' self" (Velkley (2002)).

Cultural value patterns on privacy

As mentioned above, the dimension of individualism and collectivism reflects the relation between the role of individual and the role of group in a society (Hofstede *et al.* (1997):74). A

society tends towards collectivism "when [...] the interest of the group prevails over the interest of the individual (Hofstede *et al.* (1997):74)". On the contrary, a society tends towards individualism "when [...] interests of the individual prevail over the interests of the group (Hofstede *et al.* (1997):75)". In a collectivist society, "we group/in-group is the major source of one's identity and the only secure protection one has against the hardship of life...Between the person and the in-group a mutual dependence relationship develops that is both practical and psychological (Hofstede *et al.* (1997):75)". However, in an individualist society, "this 'I', their personal identity, is distinct from other people's "I's" and these others are classified as characteristics... Neither practically nor psychologically is the healthy person in this type of society supposed to be dependent on a group (Hofstede *et al.* (1997):75)".

Hofstede developed and applied the 'individualism index' among 74 countries and regions, measuring the ties between individuals. His calculation shows that Europe, (when compared with China), is an individualist society while China is a collectivist one (Hofstede *et al.* (1997):78-79). In Europe, "self" refers to what Kant portrayed as the bearer of individual preferences and beliefs and the representation of humanity (Capurro (2005):42). It is the "most precious thing a person has" (Capurro (2005):42).The "self" is a highly individualistic perspective, since it juxtaposes intrinsic and extrinsic values of the self and refers to what Kant portrayed as the bearer of individual preferences and beliefs and the representation of humanity (Capurro (2005):42). Such thinking can be traced back to the Enlightenment, when European society was being reshaped, and Europeans were exposed to the fundamental doctrine that 'we, the people, are created as individuals with certain unalienable rights' (Dorff (1997):32). Generations of Europeans were periodically influenced by a more positive variant of this motif, disseminated via the theories of Kant, in which it is stressed that, indeed, the 'self' is the most precious thing a person has. The idea came to dominance in the European romantic era wherein, for instance, Adam Smith, Kant, Goethe, Van Beethoven and Rousseau occupied their respective stages and, in their particular ways, celebrated individualism.

However, in China the "self" of the person has been "unimportant and disregarded", and only "the people" seem to count (Crocker (1968):175). Such an inclination towards collectivism has been influenced by the school of Confucianism (Hofstede *et al.* (1997):80). The Confucian school of thought maintained that the stability of society was based on unequal relationships between people (Hofstede *et al.* (1997):80). There are five basic relationships marking the theory of Confucius: ruler-subject, father-son, older brother-younger brother, husband-wife, and senior friend-junior friend (Hofstede *et al.* (1997):80). These relationships contain mutual and complementary obligations: for example, the junior partner owes the senior respect and obedience, while the senior partner owes the junior protection and consideration (Hofstede *et al.* (1997):80). According to Confucianism, people should be willing to sacrifice their own lives if necessary in order to uphold the five basic relationships. The thoughts continuously absorb individual souls, which turn to be a sort of collective soul (Crocker (1968):188).

Cultural value patterns in Europe

In order to clarify the individualist inclination of privacy, I explore the historical trajectories of privacy evolution in Europe. In this part, with my analysis of Medieval Europe I provide a brief account of the evolution of the concept of privacy, in order to comprehend the changes of its function.[38] After investigating for aspects that characterize European thinking in medieval times, I find three strong, universal, early influences: (1) the roman-catholic church, (2) Latin as lingua franca of European intellectuals and (3) architectural and technical barriers rendering privacy - if conceived at all – practically impossible. In medieval times no conditions allowed for substantial privacy. As we understand it now, privacy simply wasn't there yet, at

[38] I am aware that the selected events below are highly stylized, abstracting from regional difference. Nevertheless, for my purposes, the exact historical analysis does not matter. What matters are the changes in the society that posed threats to what we, now, loosely understand as "privacy function."

least not in Europe:

> "… even in the upper levels of society, bedrooms were also reception rooms, even dining rooms, and the lack of division between sleeping and living continued to exist until comparatively recently … that throughout medieval society there was a very different understanding of personal space and privacy than exists today. Even a rich fourteenth-century London grocer had to find room for four beds and a cradle in his chamber … Life was very public in medieval times: death, dishonor, punishment and reward were all public events …" (Molyneaux & Stone (2004):208).

I consider the beginning of privacy in Europe, reflected in its functional feasibility, during the reformation era (generally considered to end with the peace of Westphalia in 1648, eventually leading to the formation of nation-states in Europe), wherein the clashes between roman-catholic and protestant approaches to religious practice took place, and when the availability of print allowed for reading in seclusion (and for hiding the evidence):

> "It is the practice of private spiritual reading that becomes instrumental, not only in encouraging personal choice in religious matters, but in linking the idea of privacy and autonomy. … In 1559, the celebration of the Mass was made illegal in England … In 1571 it became treasonous to import or publish any writings emanating from Rome … but the repression of the Catholic practices also fostered something new: … the growing experience that their personal religious practices need not be affected by outward adherence to official doctrine and attendance at Church of England services. Outward conformity permitted interior religious freedom" (Jagodzinski (1999):27).

As Spacks highlights after analyzing a great deal of English literature of the eighteenth century, experiencing an inner self, and juxtaposing it against the conception of the individual as a

social being, is considered to emerge increasingly – also outside the topos of the individual religious experience under duress (Spacks (2003)). In the eighteenth century, European privacy begins to encompass the (incidental) protection by seclusion against social duties unwished for in context (Oakleaf (2005), Spacks (2003)).

To illustrate the evolution of privacy, I select an example from the nineteenth century of how economic forces may have privacy-invading attraction and may evoke resentment against the discriminatory aspects involved. Odlyzko refers to the public feelings evoked by the price-discriminatory policies of USA railway companies in the late nineteenth century. His analysis seems all the more appropriate in the prospect of what we may expect in our information era:

> "The logic of price discrimination suggests a future drastically different from the anonymous shopping agents of [...] instead, it leads to an Orwellian economy in which a package of aspirin at a drugstore might cost the purchaser $1 if he could prove he was indigent, but $1,000 if he was Bill Gates or simply wanted to preserve his privacy. Such a future would justify the efforts that enterprises are putting into destroying privacy. It would also show that the public's concerns about privacy are well-founded, since current and historical precedents strongly suggest such a future would be resented … However, we will be catching an increasing number of glimpses of it, as enterprises move to exploit the opportunities that differential pricing offers" (Odlyzko (2004):191).

Thus, in the nineteenth century, the Western concept of privacy seems to be gaining an additional function: protection against discriminatory behavior in economic environments. Of course, this type of function gained urgency during and after World War II – when the administration agencies of the occupied countries' governments were utilized to single out the Jewish population. Then, privacy gained the additional function to protect against government abuse.

Starting in the 16th century, the conception of privacy in Europe took a complex path for several centuries before it evolved into its current meaning. That was not accomplished in a single action or event. My short etiology of the concept in European culture has identified a cumulative set of specific functions, each of which may be considered as a partial function of the more general right to be let alone:

- During Medieval times, privacy is not yet a palpable concept;
- During the Reformation, privacy cum printing technology allows for preserving a secret inner religious life: privacy as a function that protects dangerous but not shameful truths;
- During the eighteenth century, privacy gains (as shown by academic literature) a protective function of more secular aspects of the inner life, of legitimate seclusion, avoiding the obligation to comply with social obligations: privacy as protection against social expectations;
- During the nineteenth century, privacy gains an extra meaning under the emerging practice of discriminatory pricing in the economy: privacy as protection against price discrimination;
- During the twentieth century, privacy gains an extra meaning following the atrocious practices of Nazism that were facilitated by the availability of censor records: privacy as protection against power abuse by the government.

These functions have appeared in history and can be conceptualized into three interpretations of privacy. The first conception (emerging during the Reformation conflict and the eighteenth century) is to provide protection against intrusion into a person's private sphere (e.g. family life, home, correspondence). The second conception (emerging during the nineteenth century) is to provide protection against undue interference by private persons or organizations. The third conception (emerging during the twentieth century) is to provide protection against undue interference by public authorities.

The evolutionary process and the continuously accumulated privacy functions display that privacy aims to satisfy the needs of the individual versus the "outside" (private persons, organizations and public authorities outside of the private sphere). Privacy focuses on one's effort to look after oneself and to be sufficient, autonomous and independent. Therefore, privacy in Europe is influenced by a culture inclining towards individualism, while such culture has developed a consciousness of privacy protecting against transgressions on the "self".

Cultural value patterns in China

The collectivist inclination of privacy can be described as "shame culture"(Hofstede *et al.* (1997):89).

> "Persons belonging to a group from which a member has infringed upon the rules of society will feel ashamed, based on a sense of collective obligation... Whether shame is felt depends on if the infringement has become known by others. This becoming known is more of a source of shame than the infringement itself (Hofstede *et al.* (1997):89)".

In order to clarify the collectivist inclination behind privacy in China, I explore the concept of privacy from an etymological perspective. In Chinese, three phrases suggest a reference to the concept of privacy, although they are linked to three different degrees of meaning. In order to distinguish between the three compounds, I use Chinese phonetic letters to mark them. The three phrases are spelled as: "Yin3Si"/隐私; "Yin1Si"/隐私; and "Yin3Qing2"/隐情.[39] Since every Chinese character has its own

[39]Farrall (2008) (at page 998 etc.) explained some of the features of Chinese for Europeans in an understandable way: Chinese is a tonal language. Different characters may have the same way to spell, even to pronounce. The first phrase Yin3Si1 means the first word of the compound is pronounced using the third, dipping tone, and the second word is pronounced with the first, steady tone. The second phrase Yin1Si1, means the first

personality, I examine each word in the three phrases individually in order to comprehend the meanings behind them.

In any major English-Chinese dictionary (such as Hornby & Zhang (1984)), the English word "privacy" is translated into Yin3Si. This phrase combines the two words (characters) Yin and Si.[40] In isolation, the first character (Yin3) is a verb meaning "to conceal", and the second one (Si1) is a noun meaning "private, personal or selfish".[41] The combination of the two characters in the phrase shows that the intention of the phrase was to consider privacy as something that one wants to conceal or that is better to function in a non-transparent manner. Considering the word Si's derogatory sense, the term 'privacy' in the phrase implies connotations of illicit secrets and selfish, conspiratorial behavior (The Economist (2007)).[42]

The negative connotation appears even stronger in the second compound, Yin1Si1.[43] Compared with Yin3Si, a phrase imported

word is pronounced using the steady tone. The second word is the same as in "Yin3Si1". The third phrase Yin3Qing2, means the first word is pronounced using dipping tone, and the second one is pronounced with a rising tone.

[40]Etymologically, 'YinSi' is a word of Japanese origin. In "Global privacy in flux: Illuminating privacy across cultures in China and the US", Farrall thought that the word yinsi is a recent neologism whose use has been heavily influenced by exposure to both Western legal scholarship and popular culture in the mid- to late- '80s (Farrall (2008):998).

According to Farrall, at the time, the most typical and important import conceptualization concerns how to express 'legal right' . In isolation the word (Character) 'quan' comes into play here. The right to personal data protection has become yet another compound in the Chinese language 'Yin3Si1Quan'. It has been around for nearly one century (Farrall (2008):998).

Additionally, In Wang Binbin's paper, he mentioned that several legal compounds survive in modern Chinese, dating from the time that in Japan parts of western legal culture came to be absorbed (BinBin Wang (1998)).

At: http://www.china.com.cn/chinese/ch-yuwai/193347.htm, Wang's article is available.

[41]Hornby & Zhang (1984).

[42]Also see the article in the Economist (no author mentioned): "China, the long march to privacy," published in 2006 and available at: http://www.economist.com/node/5389362

[43]There is a special Chinese dictionary, 'CiYuan' (The source of words), dating from 1915, which introduces not only the meanings but also the

into modern Chinese in the early 20th century, Yin1Si emerged locally and may embody the conception of "privacy" in Chinese culture more authentically. The phrase is made of the words Yin1 (lady or negative), and Si (personal, private or selfish). The original meaning of this compound denotes secrets between couples that one is shy to talk about. In time its meaning widened, encompassing all personal information considered morally inappropriate to disclose. However, after the reception of Yin3Si, the use of the Yin1Si phrase was largely displaced and is now rarely used in practice.[44]

The third phrase "Yin3Qing2" originates in native Chinese as well. On its own, Qing means 'situation'. In the dictionary([45]), YinQing is described as "facts one wishes to hide". Yin3Qing2 lays special emphasis on the consequences of non-disclosure, while both Yin3Si1 and Yin1Si1 focus on behavioral motives. In fact, Yin3Qing2 is very closely related to the sense of being forced to hide. Here, I will discuss the example "HuiJiJiYi/讳疾忌医". The four characters combined represent a Chinese idiomatic expression and signify when a patient conceals his ailment and refuses to consult a doctor. The proverb originates in the story of an emperor who refused to see a doctor when he was seriously ill. Although the story does not explain why the emperor suffered in silence, it is implied by the proverb, due to the character Hui, that the disease is considered taboo to reveal even to a doctor. The emperor's reputation was at stake because, according to the Chinese concept of privacy, his disease was better kept secret.

- Yin1Si1 is the oldest and hardly used in practice any more, only to be found in dictionaries. It refers to all personal information one is shy about or ashamed of – for simplicity I will refer to it as "intimate" privacy;
- Yin3Qing2 is a native Chinese concept for personal attitude one wishes to hide – for simplicity I will refer to it as "secretive"

histories of the Chinese language's words and compound-words.

You will not find 'Yin3Si1/' in it, as it is an imported compound and CiYuan focuses on words of proper Chinese heritage. You will, however, find 'Yin1Si1' and 'YinQing'.

[44]At: http://news.xinhuanet.com/video/2011-09/08/c_122000871.htm Zhou's interview is available.

[45]Hornby & Zhang (1984).

privacy;

- Yin3Si1 was imported in the Chinese language about a century ago as a translation from the Western notion of privacy and is the term used in Chinese legislation.

Although the three phrases vary in meaning, they demonstrate that privacy in China is collectivism-driven. The three phrases are used to conceal private life, which is limited to intimate relations, leading to the derogatory connotation of privacy. If others had information of one's private life, one would feel ashamed and humiliated. Therefore, the conception of privacy as an instrument is to defend one's reputation. In brief, the cultural value patterns of privacy in China are driven by a "shame culture" and establish the commitment to prevent "hidden-shameful-truths" from being disclosed.

In conclusion, the analysis of the cultural value patterns of privacy demonstrates a contrast between Europe and China. On the one hand, the European conception of privacy exhibits strong indications of an individualist drive, which aims to protect the "self" against intrusion from the "outside". On the other hand, in China, privacy exhibits collectivism-driven patterns, and is performed as an instrument against being shamed by disclosure.

Diverse cultural value patterns and data-protection laws

Thus far, I have shown evidence, which correlates with common sense: major cultural differences have led to serious differences between Europe and China in privacy conceptualization. Yet, there have been recent worldwide developments, for instance technical innovations that not only challenge privacy regulations at large, but may also weaken their diversity. Nowadays, the concerns about privacy have been supplemented by the concerns about informational privacy, mostly articulated as personal data protection. In the next part I investigate whether the cultural attributes of privacy, that made the conception of privacy in the two regions so different, maintain their influence in shaping new data protection law.

The right to informational privacy in Europe

In Europe the reaction against the risks of informational privacy intrusion is evident, since both at the European and at the national level, laws have emerged in quick succession and continue being updated, due to the development of information technology and its ubiquitous use.

The Right to informational privacy is regarded as a fundamental right in Europe (Kuner (2007): 18). In "the Convention for the Protection of Human Rights and Fundamental Freedoms", art. 8 refers to the right to privacy (Council of Europe (1950)).[46] Through a series of case laws made by the European Court of Justice, the scope of the art. 8 was extended to cover informational privacy.[47] In the Charter of Fundamental Rights European Union (European Union (2012)), the right to informational privacy is separated from the right to privacy as an independent right. Article 8 states that "everyone has the right to the protection of personal data concerning him or her" (European Union (2012)). The European Court of Justice also recognizes the

[46] Article 8 of the ECHR provides in Council of Europe (1950): "Everyone has the right to respect for his private and family life, his home and his correspondence" and "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[47] The privacy concept as outlined in Art. 8 of the ECHR refers mainly to "the right to private and family life, respect of private home and private correspondence" (Council of Europe (1950)). However, the scope of Article 8 is continually extended. In 1979 the Case Klass V. Federal Republic of Germany (1979), government surveillance of telephone conversation was included into violation of art. 8 ((Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978). In the case Huvig V France (Application No.11105/84, Judgement of 24 April 1990) policy tapping of an individual business and private telephone lines were involved to be a violation of art. 8. In the case Harford V. United Kingdom, interception of private telephone calls made from business premises on a private telecommunication network was included into art. 8's scope ((20605/92) [1997] ECHR 32 (25 June 1997)). In the case Copland V. United Kingdom ((2007) 45 EHRR 37), monitoring of an employee's telephone calls, Internet usage and email at work constitute a violation of art. 8.

right to informational privacy's status as a human right. In Joined Case C-465/00 and C-138/01, the judges of the Court noted that the right to informational privacy, which prevents infringing fundamental freedom, should be interpreted in the light of fundamental rights.[48]

The major instrument of European data protection law is the Directive 95/46/EC (EC (1995)). The long-awaited Directive showed a convergence of political opinions in the Member states on how to regulate data protection.[49] The Directive is granted with legal binding forces because it requires "the Member States [shall] bring into force the laws, regulations and administrative provisions necessary to comply with this Directive" (EC (1995): art.32), which is enforced by the European Commission and ultimately by the European Court of Justice. That means that the Directive offers a framework and provides the member states with legislation to implement (Büllesbach (2010): 12). The Directive resolves two objectives, protecting data subjects' rights and ensuring the free-flow of data (Büllesbach (2010): 12). Although the Directive is a general law, certain types of data processing are exempted from its scope, including law enforcement, national security and criminal law (Kuner (2007): 21-22). [50]

[48]In Joined Cases C-465/00, C-138/01 and C-139/01 (Reference for a preliminary ruling from the Verfassungsgerichtshof and Oberster Gerichtshof): Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk, OJ C 79 of 10.03.2001 OJ C 173 of 16.06.2001

[49]The birth of the Directive experienced a long, arduous and contentious negotiation process. The first draft of the Directive was finished in 1990. The European Parliament made nearly 120 changes and was ultimately approved on 1992. In October 1992, a completely restructured proposal was submitted and eventually became the Directive 95/46/EC (Büllesbach (2010):9).

[50]Article 13. Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes necessary measures to safeguard:

(a) national security;

(b) defense;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offenses, or of breaches of ethics for regulated professions;

Since the 9/11 attacks and the events in London and Madrid, the whole world faces a new international context. In the wake of the 'War on Terrorism', as proclaimed by USA officials, the notion of privacy, even in Europe, is facing issues raised by the governmental focus on public security. Advancing public security requires immense efforts of surveying individuals and is in conflict with the protection against undue interference by public authorities, one of the European privacy functions.

Indeed, when public security is in conflict with the right to informational privacy, the Directive exceeds the limits over data processing, and, according to article 7, legitimates data processing if it is beneficial to public interest (EC (1995)).[51]

Data retention has become the focus of controversy in post-9/11 times. The basic principle of data retention is formulated by Directive 97/66/EC, which was introduced to strengthen and clarify data protection and privacy rules in the telecommunications sector (EC (1997)). Although the Directive has a sector-specific focus, its scope is much broader (Kuner (2007): 24). Article 6 of Directive 97/66 makes clear that the routine retention of traffic data for any purpose is banned without the data subject's consent, except for the purpose of billing:

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call.

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others (EC (1995)).

The three types of data processing fall under the "third pillar" of EU law.

[51]Article 7 (95/46 EC): "Member States shall provide that personal data may be processed only if: [...] (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" EC (1995)

2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued. (EC (1997):art 15)

After 9/11, many member-states' national security agencies asked for a revision of this ban.[52] The 1997 Directive was replaced in 2002 by Directive 2002/58/EC, which updated the data protection rules for traffic data retention issues (EC (2002)). In Article 6, the Directive 2002/58/EC obliges the providers of services to erase or anonymize the traffic data when no longer needed, which is similar to the 1997 Directive, unless the conditions from Article 15 have been met. This revised Directive allows member states to introduce legislation that obliges service providers to retain these personal data and then allows public agencies to get access to them. The Article states:

``1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in […] Article 6, and […] of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offenses or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on the European Union." (EC (2002))

In 2006, the European Union formally adopted the Data Retention Directive (2006/24/EC) and amended Directive 2002/58/EC. Against the background of anti-terrorism, the Retention Directive was adopted to harmonize rules on data retention in order to ensure the availability of traffic data (Kuner (2007): 31). The Retention Directive affects a wide range of data, including phone numbers, the duration of phone calls, IP address, log-in and log-out times and email active details (EC (2006): art. 5). Article 6 of the Directive requires Member States to ensure that communication providers retain necessary data as specified in the Directive, for a period of no less than 6 months and no more than 2 years (EC (2006)). The data are required to be available to relevant national authorities in specific cases, ``for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (EC (2006) :art.4)".

From a realistic perspective, in my opinion, some international agreements for working on anti-terrorist issues have also shaken the belief in the traditional European cultural value patterns of privacy. Such a case is the Cyber-crime Treaty, which is signed by several European Union member countries and other countries such as the USA and Japan. This treaty, aimed not only at hacking but also digital crime at large, has an anti-privacy function as an end in itself. It requires the signatory nations to install surveillance devices to monitor the individual's usage, to retain the personal usage records, and to allow the police to force individuals to disclose their encryption passwords if deemed necessary. In addition, as an international treaty, the cooperation between signatory countries is important, requiring countries to allow access to these data by other countries.

Consequently, after 9/11, the privacy function to protect against undue interference by public authorities has become a matter of concern, leading to intense debates. Simultaneously, the informational privacy exhibits a sense of diminishing on European cultural values patterns of privacy which is individualism-inclined, since the right is being strongly challenged by national security's requirement.[53]

[52] No sooner had the dust settled from the Madrid bombings, or the UK went public with plans to resurrect the Framework Decision; it also figured in proposals from the Commission and the Council. The proposal is in no way limited to terrorism and concerns "crime in general". Ireland and France joined the UK in putting their names to the proposal. This comes as little surprise - Ireland leads the member states in having introduced data retention for at least three years ("Directions" were issued by the Minister for Public Enterprise in April 2002 under the Postal and Telecommunications Services Act 1983), while France has mandatory data retention for up to one year (under Article 29 of the Law on Everyday Security of 15 November 2001).

[53] Capurro (2005): 42

Chinese material laws

China does not have a specific law addressing data protection issues. When any conflict due to this issue rose, it was often solved by referring to tort liability rules. Moreover, China's policymakers integrated some articles tailored to solve data protection issues into existing laws, in order to meet the requirements on data protection law. Thus, China's legal arrangement on informational privacy issues is framed by a set of articles, which are described below.

Protection under the Constitution The Chinese Constitution was enacted in 1982, with two articles relating to privacy. Since its enactment, the Constitution has been amended several times, but the two articles relating to privacy have never been changed.

Article 39: ``The residences of citizens of the People's Republic of China are inviolable. Unlawful search of, or intrusion into, a citizen's residence is prohibited."

Article 40: ``Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any grounds, infringe upon citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of state security or of criminal investigation, public security or procurator bodies are permitted to censor correspondence in accordance with procedures prescribed by law" (Constitution, PRC 2004)[54]

The two articles entail two instrumental functions: protection against intrusion into a person's private sphere, and against infringement of correspondence privacy, also by organizations. From the contents of the two articles, there are no obvious differences between China's Constitution and ECHR. However, I did not discover any guidance or interpretations made by China's Supreme Court indicating that the scope of the two articles extends to the right to informational privacy like in Europe. Thus, it is evident that the right to personal data is not yet recognized as a human right in China.

[54]Constitution Of The People's Republic Of China, Adopted at the Fifth Session of the Fifth National People's Congress on December 4, 1982 and adopted at the First Session of the Eighth National People's Congress on March 29, 1993. The law is translated by 'LawOfChina' and also can be seen in Constitution of the People's Republic of China-(1982)-www.lawinfochina.com

Protection under the civil law system The Chinese Civil Law system is determined by "The General Principles of the Civil Law" (Hereafter Civil Law). Compared with Constitutional Law, Civil Law is a more important legal means, supporting the protection of privacy de facto.[55] However, like in the Constitution, there are no references directly referring to the right to privacy. In Chinese academia, it is widely argued that the right to privacy, as a trait of one's personality, is protected under the umbrella of reputation, which is covered by the Civil Law.[56] Its Article101 states: ``Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited" (National People's Congress (April 12)).

The subsequent judicial interpretations, issued by the Supreme Court, expressed that privacy is covered in Article 101 which aims to protect reputation. In ``*Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation)*" (1988) I found:

> Article 140: In case that someone flouts another person's privacy in writing or orally and thus caused damages on the person's reputation, it should be affirmed as infringement of reputation.[57]

[55]General Principles Of The Civil Law Of The People'S Republic Of China, Adopted at the Fourth Session of the Sixth National People's Congress, and promulgated by Order No. 37 of the president of the People's Republic of China on April 12, 1986, and effective as of January 1, 1987. The law is translated by 'LawOfChina' and also can be seen in General Principles of the Civil Law of the People's Republic of China- -www.lawinfochina.com

[56]For instance, Wang Liming said that "the right to privacy falls into the category of personality rights. The right helps people to control their personal information, private lives and private space. But anything concern public interests can be excluded from the protective umbrella" (Liming Wang *et al.* (1994):492). Zhang Xinbao said: "the right to privacy falls into the category of personality rights. A person's private life is free of illegal intervention and his personal information is free of illegal collection, usage and disclosure." (Xinbao Zhang (1997):21)

[57]Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation), Deliberated and Adopted at the Judicial Committee of the Supreme People's Court on January 26,

The provision was copied in "The Answers To Some Problems On The Trial Of Cases Concerning The Right Of Reputation" (1993) and "The Interpretation Of The Supreme People's Court On Several Issues About The Trial Of Cases Concerning The Right Of Reputation" (1998). In 2001, the Supreme Court confirmed that the emotional damages caused by infringed privacy might be compensated.[58] The judicial interpretation states that the Courts should accept cases arising from any illegal act violating the interests of privacy.

In 2005, the "Law of the People's Republic of China on the Protection of Women's Rights and Interests (2005 Amendment)" incorporated the right to privacy in order to protect women who happen to be weaker in the community. This is the first legal piece in China's civil law system to incorporate privacy as an independent right. Similarly, the Tort Law which came into force in 2010, provides a very direct and independent position to the right to privacy.

> Article 2.
>
> Those who infringe upon civil rights and interests shall be subject to the tort liability according to the law. 'Civil rights and interests' used in this law shall include … the right to privacy.[59]

Notably, art. 36 of the law regulates tort liability on the Internet:

> Article 36: If a network subscriber or network service provider uses the network to commit a tort against the civil rights or interests of another, he/she/it shall bear tort liability.
>
> Where a network subscriber uses the network services to commit a tortious act, the injured person shall have the right to notify the network service provider to take necessary measures such as deletion, blocking and severance of the link. If the network service provider fails to take the necessary measures in a timely manner after receipt of the notice, it shall bear joint and several liability with the network subscriber for the additional injury caused.
>
> If a network service provider is aware that a network subscriber is using its network services to commit a tort against the civil rights or interests of another and fails to take the necessary measures, it shall bear joint and several liabilities with the network subscriber. [60]

In order to understand the tortious act on the Internet we need to consider the "Regulation on Internet Information Service of the People's Republic of China" which was issued by the State Council to regulate Internet information services so as to promote the healthy development of this sector.[61] The Regulation lists nine sorts of tortious acts, and one of them is when one "insults or slanders a third party".

In light of article 36, I argue that the scope of informational privacy in China's civil law system is narrower than that in Europe. Similarly, informational privacy in China is a tool to safeguard a subject's reputation. China's conception of privacy could be regarded as something negative, since to protect privacy is to protect one's reputation against shame. This characterization is shaped by Chinese culture, which relates privacy to "hidden-shameful-truths". The cultural attribute of privacy is fully integrated into the legal fabric of China.

1988. The Law is translated by 'LawOfChina' and also can be seen in Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation) - - www.lawinfochina.com

[58]The "Interpretation of the Supreme People's Court on Problems regarding the Ascertainment of Compensation Liability for Emotional Damages in Civil Torts, as adopted at No.1161 Meeting of the Judicial Committee of the Supreme People's Court on February 26, 2001. The law is translated by the 'LawOfChina' and also can be seen in Interpretation of the Supreme People's Court on Problems regarding the Ascertainment of Compensation Liability for Emotional Damages in Civil Torts–www.lawinfochina.com

[59]Tort Liability Law of the People's Republic of China, Adopted at the 12th Session of the Standing Committee of the 11th National People's Congress on December 26 2009 and effective as of July 1 2010, PRC President's Order (No.21 of the 11th NPC) translated by Lawofchina, http://www.lawinfochina.com/display.aspx?lib=law&id=7846&CGid=

[60]Id.

[61]Regulation on Internet Information Service of the People's Republic of China, Decree of the State Council of the People's Republic of China (No. 292), has been adopted at the 31st regular meeting of the State Council on September 20, 2000 and is hereby published. http://www.lawinfochina.com/display.aspx?lib=law&id=1668&CGid=

Protection under Criminal Law Although the right to privacy mainly appears as a civil right, the Criminal Law also contributes to privacy protection.

> Article 245. Those who are illegally physically searching others or illegally searching others' residences, or those illegally intruding into others' residences, are to be sentenced to three years or fewer in prison, or put under criminal detention. Judicial workers committing crimes stipulated in the above paragraph by abusing their authority are to be severely punished.
>
> Article 252. Those infringing upon the citizens right of communication freedom by hiding, destroying, or illegally opening others' letters, if the case is serious, are to be sentenced to one year or less in prison or put under criminal detention.
>
> Article 253. Postal workers who open, hide, or destroy mail or telegrams without authorization are to be sentenced to two years or less in prison or put under criminal detention. Those committing crimes stipulated in the above paragraph and stealing money or other articles are to be convicted and severely punished according to article 264 of this law. [62]

The criminal law protects the peace of private space as an instrument against criminal acts. In 2009, Chinese Criminal Law incorporated contents related to data protection. A new provision was inserted into Article 253 of the Criminal Law:

> Article 253 (A). Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined.
>
> Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph.
>
> Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph." [63]

Although art. 253 (A) does not explicitly mention data protection, it is clear that illegal provisions or selling of personal information by officials, professionals or staff members of institutions must include personal data in electronic form. As a concluding thought, it appears that some data protection is being provided by Chinese criminal law.

The article causes disputes over its applicability in implementation. In 2010, a relevant case was brought to Beijing District Court. The judges offered their interpretations of article 253, namely that to qualify as a criminal of illegally selling personal information, one must be an employer in specific units, including government, finance, telecommunications, transportation, education or medical treatment.[64] The interpretation was challenged by a case in Shanghai in the same

[62]Criminal Law of the People's Republic of China was adopted by the Second Session of the Fifth National People's Congress on July 1, 1979 and amended by the Fifth Session of the Eighth National People's Congress on March 14, 1997).The Law is translated by 'LawOfChina' and also can be seen in Criminal Law of the People's Republic of China–www.lawinfochina.com

[63]The Amendment to the Criminal Law of the People's Republic of China (VII), which was adopted at the 7th session of the Standing Committee of the 11th National Congress Conference. This is translated by 'LawOfChina' and is also seen in Amendment to the Criminal Law of the People's Republic of China (VII)–www.lawinfochina.com

[64]The case was brought into the District Court on March 2010. There were three criminals Gan, Lee and Zhou. Zhou was a staff member working in a airbus company and in charge of registering the boarding cards' information. Gan and Lee bought the card holders' information from Zhou. The two made fake cards and sold them to people. The businesses brought RMB 50,000 benefits. Zhou earned RMB 3000. In this case, the Court first affirmed that Zhou offended the right to personal data; second, judges gave a one year sentence and levied RMB 500 fines. Gan and Lee were on a charge of counterfeiting bills and tickets. The judges further explained how they apply Article 253 in this case.

year, since the Shanghai judges made a more flexible interpretation of this article to cover people outside of these specific fields to be the qualified subjects.[65] However, in another case in Jiangsu, judges supported Beijing judges' narrow interpretation of the applicability of the article, since a suspect was immune from prosecution because he is not from those specific units.[66]

They thought the crime of illegal selling personal information was only for the person working in State Organs or their special units. Rather, the charge of illegal collection is not limited to this. At: http://www.lawlib.com/fzdt/newshtml/shjw/20100613090211.htm more information about the case can be found.

[65]The case is a group crime. The chief criminal is Zhou Juan. She opened Shanghai Taimeng Information Technology companies (hereafter TM) in 2005. In fact, the firm is mainly for doing business with personal data. Until 2008, Zhou had gained RMB 1,000,000. In 2008, three staff members of the firm resigned and started a new firm which did personal information business as well. The three people collected more than 30,000,000 personal data records including investor data, car owner information, bank clients, security clients and so on. Most of people involved are people with high incomes. The approach for collecting their data is illegal. The suspects confessed that they even posted false employment information on job websites. The job candidates' information was unfortunately 'caught' by this firm. The price for personal information is very cheap. A complete personal information document only cost 0.10 - 0.50 yuan (or 0.012 - 0.06 euros). According to the police's report, a business partner of the firm bought more than 10,000,000 personal-information documents in one time. In August, the district court in Shanghai heard the case. The Court decided that all 10 suspects had committed the crime of illegal data collection. The Court sentenced 9 of the criminals to jail terms from six months to two years, and imposed fines of RMB 10,000 to 40,000. One criminal was exempted from punishment. At: http://www.hg.org/article.asp?id=19630 more information about the case can be found.

[66]In a case, the suspect collected personal information through a 'fishery' software created by him. He was arrested because of illegal collection. However, the judge decided not to press charge since he thought the suspect was not a qualified subject on charge of Article 253. The suspect is free of charge.

The APEC Privacy Framework of 2004[67] This regional organization initiated a Privacy Framework in 2004 (Asia-Pacific Economic Cooperation (2004)). This Framework is consistent with the core values of the Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines) (Organization for Economic Cooperation and Development (1980)). The Framework adopted nine privacy principles, i.e. preventing harm, integrity of personal information, notice, security safeguards, collection limitations, access and correction, uses of personal information, accountability, and choice (Asia-Pacific Economic Cooperation (2004):14-20). [68]

Safe-harbor like mechanisms On July 19th, 2008, the Dalian[69] Software Industry Association (Hereafter DISA) signed an agreement with JIPDEC, the Japan Information Processing Development Corporation.[70] It is part of Japan's national industry organization. DISA is 'an organization for regulation and supervision of information service industries.'[71] JIPDEC is 'a public corporation for the purpose of development of information processing and information processing industry in Japan.'[72] The agreement between them refers to a mutual recognition program that both parties recognize each other's authentication. Part of the agreement emphasizes the importance of information privacy. DISA has adopted a city-wide Privacy Information Pro-

[67]See also: Greenleaf, G., "Five years of the APEC Privacy Framework: Failure or promise?", Computer Law I\& Security Report 25, 1 (2009), pp. 28–43. Or "The EU Data Protection Directive: An engine of a global regime", Birnhack summarized Greenleaf's main opinions on APEC framework which is also our main sources.

[68]Greenleaf (2009) assessed the APEC's Framework. He thought this framework is weaker than the EU Directive and it is less ambitious in scope, since it just gives guidelines and directions to its member economies (Greenleaf (2009):35).

[69]As Wikipedia submits, Dalian is one of China's 11 "National Software Industry Bases" and one of its five "National Software Export Bases." Currently, more than 300 companies, including 32 Global 500 corporations, have offices in the park (*Wikipedia (2007)).*

[70]JIPDEC (2008).

[71]Id.

[72]Id.

tection Assessment program (PIPA).[73] According to the agreement between DISA and JIPDEC, the two accrediting systems are functionally equivalent, and each government recognizes each other's accreditation. Any entity given a PIPA mark or a Privacy mark can be mutually recognized as a good firm from a data protection perspective (JIPDEC (2008)). By April 2011, 77 firms in China have been accredited with the PIPA mark.

The main function of informational privacy in China is to protect against intrusion into persons private sphere, particularly against being embarrassed by shameful-truths. We argue that informational privacy slightly departs from cultural value patterns on privacy, though the ``keynote'' set by history is retained.

[73] Actually, the agreement and the PIPA are the by-products of an import embargo. Dalian is an important software production base, and Chinese firms are significant business partners. In 2008, Japan forbid import of software from Dalian due to the absence of data protection laws and the poor track record of Chinese firms concerning the violation of rights to personal data. In order to manage the crisis, the DISA wrote an industrial regulation 'Personal information protection regulation for Dalian software and information service', and created the PIPA mark system for accrediting firms. Japan recognized the effects of PIPA and signed the mutual recognition agreement with DISA (JIPDEC (2008)).

The cooperation between DISA and JIDEC is not limited to mutual recognition on data protection. The parties to the agreement share information about accredited firms' performances on data protection, in order to supervise the software markets involved and to take technical measures for verification and authentication of the mark. And regarding complaints and/or disputes filed by consumers in the program, the Mark accreditation body of DISA or JIPDEC, is to take on the settlement and, in cases where one of the bodies receives complaints, is to cooperate with the other in good faith (for instance for the provision of information) (JIPDEC (2008)).

Additionally, DISA expects that the PIPA system can be promoted to more and more industries in China. Dalian's trial proved successful, so much so, that several cities that face similar challenges are adopting the approach. The promotion of the PIPA mark system proves fruitful. The PIPA system is to be distinguished from legislation and judicial decision making. It is more like a safe harbor agreement – made, implemented and enforced by industrial parties.

Different laws and cultural value patterns

Now, I return to the question: do the cultural attributes of privacy maintain their influence in shaping new data protection laws?

Based on the above analysis, I conclude that informational privacy law in China is still shaped by a culture of collectivism. Neither in cultural practices, nor in the legal literature could I find any indications that there have been changes in, or additions to, the culturally determined value patterns in China. First, informational privacy in China is still adopted as an instrument to defend data subjects' reputation. It is because, as stated in the Civil laws, to protect data subjects' informational privacy is to prevent them being insulted or slandered by a third party. This originates in Chinese 'shame culture', which is a collectivism-driven value pattern of privacy. Second, what took place was a lot of articles while creating legal and semi-legal personal data protection mechanisms, predominantly focusing on supporting trans-border data flows. These mechanisms could also help to fulfill community interests: the APEC agreement is to enhance cooperation between member states, while the 'safe-harbor' mechanisms in Dalian are there to facilitate exportation.

In Europe, there is an obvious shift from an individualism-based cultural value of privacy towards a combination of individualism and collectivism. First, informational privacy retains the aspect of individualist inclinations, present in the cultural value patterns of privacy. The right to informational privacy is labeled as a fundamental right and the protection of the "self" and its autonomy is a primary goal. Second, the evolutionary process of the data retention principle demonstrates the inclination to uphold collectivist values, such as public security, which continuously undermine the individualistic aspect. There seems to be no compromise between private and public interests, but, instead, a shift towards recasting privacy from an end-in-itself to leading to something else. Indeed, although the legal workings in Europe are leading to a less strict conception of privacy (Capurro (2005): 42), I can argue, through the European rules, that informational privacy is still something considered worth protecting, independently of the circumstances. But the changes today are located where privacy is being challenged by the need to promote national security. The shift is driven by societal changes, particularly the

emergence of "anti-terrorism". In order to balance this society-wide shift, reactions in favor of the right to informational privacy could be expected, with individualism's value being emphasized as a human right.[74]

Conclusion

I began this Chapter by showing certain analogies between languages, cultures and legal systems. In brief, legal systems, like languages, evolve under the pressure of the cultures they serve and are part of. Consequently, by looking at the developments in their cultural environments, the differences between legal systems, both in writing and in action, may be better understood.

The analysis of cultural value patterns illustrates that the cultural background of privacy in the two regions displays a significant degree of variation and shapes the basic nature of privacy consciousness in Europe and China. When privacy is adapted to informational privacy, the cultural aspect is retained, since consciousness, acting as pre-existing constraint, characterizes the contents of data protection laws in both regions. As the above discussion of European data protection law demonstrates, its role emerges from the origin of European

[74]The event of Passenger Name Record, which happened in 2004, tests the strength of the two values in European legal system. Following with 9/11, the U.S. government issued a new legislation requiring airlines to provide American authorities with access to passengers' name record if the flight will to, from or cross U.S. territories (Kuner (2007): 22). After negotiation, the European Commission issued an adequacy finding on this data transfer requirement.(Council Decision (EC) 2004/535 of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (2004) OJ L235/11 Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, May 28, 2004, p. 5, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf.) The Commission's decision was driven by the collectivism consideration to protect security. However, the decision was challenged by European Parliament which oriented from an individualism perspective to defend European citizens' right to informational privacy (Joined Case C-317/04 and C-318/04 Parliament V Council (2006))

individualist value patterns of privacy. Although the social changes in Europe pushed towards a combination of individualism and collectivism, the inclination towards individualism was not abandoned altogether. In China, the current legal arrangement over data protection issues evolved directly from Chinese collectivist culture, which rewards the 'shame culture' aspect of privacy, and currently the inclination towards collectivism does not appear weaker. Based on these findings (illustrated in the previous), it is safe to conclude that culture helped shape both regions' data protection laws, and that information law is susceptible to being influenced by culture.

The findings in this Chapter suggest that culture, which embeds privacy practices, is complicated and has far-reaching implications on data protection law and the ways in which it will be upheld and enforced, suggesting the need for a cautious approach to legal transplantation.

First, China's policymakers should realize that European data protection law is not being transplanted to a legal and cultural "blank slate". On the contrary, in China there is a pre-existing set of data protection laws, privacy laws, and privacy-related cultural norms. China's policymakers should recognize that the imported data protection law would take time to be accepted, since Chinese society may need to assimilate the cultural implications that the imported law may bring but are not present in Chinese culture.

Second, it is crucial to think of the problems that the individual components of the European law may produce during the transplantation of the European data protection system. The European data protection law might prove too complicated and confusing compared to the relatively simple Chinese data protection conception.

Third, it may be better to borrow no more than a fraction of the aspects from European data protection law, rather than importing the whole system. The key selection criterion should be that the new law must fit the needs of Chinese society, including its cultural components.

Like everything else, technologies, laws and cultures change and evolve. Hence, when importing a legal culture, it is advisable to look at those characteristics which may improve (or deteriorate) the target legal system's resilience against changes. By now, I have established the differences and similarities between two privacy laws and

between the two cultures involved. At first sight, there are both risks and benefits regarding the law importation from the EU to China. To make an informed choice about the importation process, it is useful to analyze how the relevant laws support (or undermine) the recipient legal system's resilience in a changing environment. This very issue is my motivation for the next Chapter's analysis of incomplete law theory.

Chapter 4

Incomplete Data Protection Law

Introduction

In previous two chapters, I explored the differences between two regions' privacy laws and between two regions' privacy cultures involved. I have a basic understanding of what to import and what not to import. Yet, what I do not know is how to import or how to arrange the candidate law in China? That is an issue related to legal importation strategy.

This Chapter considers the issue. As I presented in Chapter 1, China's policymakers maintain that European data protection law is complete and therefore beneficial (Hanhua Zhou (2006)). Thus, their transplantation plan, based on that assumption, reproduces the contents about data subjects' rights and data controllers' responsibilities in European law. However, if instead the assumption cannot stand up and the targeted data protection law cannot unambiguously stipulate all relevant applications, China's policymakers need to re-adjust past legal transplantation strategy.

In this Chapter, I will find whether the EU data protection law is not as complete as China policymakers' expects? If not, how do European policymakers attempt to compensate for the defects of the incompleteness? In order to do the examination, I deploy an analytical tool from 'The Theory of Incomplete Law' (Hereafter ILT). The

theory is contributed by Katharina Pistor and Chenggang Xu. In fact, it is not a novelty to claim that law is incomplete. For instance, Hart argued that law is indeterminacy (Hart (1994):128). But what makes the ILT different from other ones, which establish the incompleteness of law is that the ILT addresses the problems brought by incomplete law. As Xu and Pistor suggest,

> *"Law is inherently incomplete which implies that it is impossible to write a law that can unambiguously specify all potentially harmful actions. Because law is incomplete, law enforcement by courts may not always effectively deter violations. Rather than attempting the impossible task of completing the law, the effectiveness of law enforcement may be enhanced by reallocating lawmaking and law enforcement powers."*[75]

The incomplete law theory is inspired by the incomplete contract theory (Xu & Pistor (2002a):933). Xu and Pistor develop the incomplete contract theory to cover the profound incompleteness problem in law when they assessed the governance functions in financial market (Xu & Pistor (2002a):937). The theory is of wide interest to legal research which not only can be used to compare legal systems, but also to analyze lawmaking and law enforcement in diverse jurisdictions (Xu & Pistor (2002a):966). In this Chapter, the application of the ILT is extended into a new field: data protection law.

This chapter is organized as follows: first, I will outline the characteristics of incomplete law theory (2). In Section (3), I will apply the framework to the European legal system over data protection issues. I analyze the legislative responses to challenges posed by the development of technology. Then, I explore the European institutional arrangement on data protection issues(section 4). In Section 5, I draw conclusions on the strategy to import European data protection law.

[75] Xu & Pistor (2002a):931.

The Incomplete Law Theory

In this Section, I amplify the analytical framework of incomplete law theory. Most of the contents in this section are concluded from a series of paper wrote by Xu and Pistor (such as Pistor & Xu (2002a, 2004, 2006); Xu & Pistor (2002b,a)). The purpose of this Section is to provide a complete picture about the theory.

Law is intrinsic incomplete

My first question when I met the ILT is: What is a complete law and what is an incomplete law? According to Xu and Pistor, completeness means that obligations *can be unambiguously stipulated in the law and the law can be enforced literally provided that evidence is established* (Xu & Pistor (2002a):938) In the enforcement process, completeness requires that *the law is self-explanatory, i.e., that every addressee agrees to the meaning of the law and, by implication, that there is no need for interpreting the law* (Xu & Pistor (2002a):938). If not, the law is incomplete. The two authors argue that laws cannot be complete since they have in their `genes' some characteristics that make them designed to *serve a large number of addressees for long periods of time and to cover a great variance of cases* (Xu & Pistor (2002a):939).

According to Xu and Pistor, it is questionable to create an intrinsic complete law (even though legislators try to avoid this energetically), since legislators *cannot foresee all future contingencies, nor can they correctly predict their probabilities*" (Pistor & Xu (2004):9). Of course, sometimes, a law can remain complete for a period of time when sufficient expertise is assembled (Pistor & Xu (2004):8). Nevertheless, it is difficult, even for a carefully designed law, to remain complete for a long time. New conditions, which lawmakers have not yet contemplated before, will arise over time to challenge the completeness of law and therefore its incompleteness is increased (Pistor & Xu (2004):8). Whatever happens, legislators can neither predict nor shape the future. As legal philosopher H.L.A. Hart argued, it is *a feature of the human predicament* that lawmakers simply cannot *regulate, unambiguously and in advance, some sphere of conduct by means of general standards to be used without further official direc-*

tion on particular occasions(Hart (1994):128). The world is simply too complex (Hart (1994):128).[76]

Moreover, some laws are enacted to be incomplete by the legislator's *deliberate design* (Xu & Pistor (2002a):932). In order to provide general guidance for helping others to *structure their relations* or to remain applicable to future disputes, laws may be created in a way that can *serve a large number of addressees for long periods of time and to cover a great variance cases* (Xu & Pistor (2002a):939). The positive side of the strategy is that a law can apply *equally all conditions described in the law, irrespective of the class, social status, or other attributes of individuals subject to the law* (Xu & Pistor (2002a):939). But the flip side is that law becomes too general to provide specific standards and procedures for each case. This can *affect the outcomes for a variety of cases that may arise in the future* (Xu & Pistor (2002a): 939).

Two types of incompleteness

Xu and Pistor classify incomplete laws into two categories based on the causes of incompleteness.

Type 1 *An incomplete law of Type I is one that broadly circumscribes outcomes without identifying particular actions or enumerating only a few actions* (Xu & Pistor (2002a):941). The example of Type I incomplete law is tort law (Xu & Pistor (2002a)).

> ``*General tort principles typically stipulate that damage to property, life, and liberty gives rise to a liability claim against the person responsible. Note that no single action is defined, only the broad outcome of damages to life, liberty, and property. Requiring intent or negligence or imposing strict liability can further circumscribe the scope of liability, but this still leaves open the question of what form actions might take that will trigger liability under the law.*"(Xu & Pistor (2002a):941)

[76]In the words of Hart, "If the world in which we live were characterized only by a finite number of features, and these together with all the modes in which they could combine were known to us, then provision could be made in advance for every possibility." He adds, "Plainly this world is not our world."

Type 2 *An incomplete law of Type II is a law that specifies the actions that shall be prevented but that fails to capture all relevant actions. To categorize laws based on types of incompleteness brings forth new ideas for legal study* (Xu & Pistor (2002a):941). The authors think Criminal Law offers an excellent example for incomplete laws in this type. As they state, Criminal Laws

> ``*usually contain a number of provisions aimed at protecting property rights, but each designed to cover a particular action, such as theft, embezzlement, damage to property, and the like. Closer inspection of these provisions reveals that the law has not captured all possible actions that could violate property rights*." (Xu & Pistor (2002a):941)

Institutional mechanisms for incompleteness.

When a law is incomplete, some new powers have to arise in order to decide how to deal with new cases through either interpreting or developing existing laws. Xu and Pistor name the new powers to be 'residual lawmaking and law enforcement powers' (Xu & Pistor (2002a):938) (hereafter *residual LMLEP*). The residual LMLEP is ``*the power to adapt or extend the range of existing laws to new cases that arise in changing circumstances*" (Xu & Pistor (2002a):933). Correspondingly, ``*the power to make new law from scratch*" is the original LMLEP (Pistor & Xu (2006):7). When law is complete, merely allocating the original LMLEP (in most cases, courts are naturally to grant with original LMLEP) is sufficient to achieve efficient levels of deterrence (Xu & Pistor (2002a):946). But when law is incomplete, it is insufficient. In this case, the residual LMLEP needs to be allocated explicitly (Xu & Pistor (2002a):964). The two authors claim that incompleteness can, to a large extent, be reduced when the residual LMLEP is allocated appropriately (Xu & Pistor (2002a):935).

Generally, residual LMLEP can be allocated to two different agents: courts and regulators (Xu & Pistor (2002a):946).[77] The two

[77]The agencies which are qualified to exercise the residual LMLEP are not limited to the two agents. For instance, self-regulators may be allo-

agents both have merits and demerits. The ILT offer a criteria to help policymakers to decide which one is preferred under certain conditions and constraints (Xu & Pistor (2002a):961). Herein lies a significant contribution of the theory to link the expected needs of the (incomplete) law on institutional LMLEP competence with competences already in place.

Courts

Courts could be allocated with substantive residual LMLEP. When law is incomplete, courts step in to clarify the incompleteness if it is required in the process of addressing a case. Through interpretation and further development of existing laws, courts decide how to enforce an 'old' law to new cases. This is the way how courts exercise residual LMLEP. Every case reflects courts' efforts to optimize the completeness of the law.

There is big difference between the two major legal families in the world on how residual LMLEP has been allocated to courts (Xu & Pistor (2002a):946). In Common Law countries, *courts commonly hold extensive residual LMLEP* (Xu & Pistor (2002a):947),[78] while in Civil Law countries, courts are constrained in and to exercising residual LMLEP (Xu & Pistor (2002a):947).

Yet overall and traditionally, courts are the natural agents to exercise residual LMLEP. However, courts have a weakness in exercising the residual LMLEP. That is courts do not ``have the power to take action *sua sponte* even when such an intervention might be desirable." In other words, courts enforce laws *ex post, ``after harm has occurred*." Judges cannot take action unless parties bring in motions.[79] Xu and Pistor are concerned that it may be insufficient to ensure optimal law enforcement of incomplete laws to solely allocate the residual LMLEP to courts (Xu & Pistor (2002a):949, Milgrom *et al.* (1990)).

cated to exercise residual LMLEP. In the data protection area, it is widely believed that self-regulators, from the incomplete law's perspective, are allocated with these residual powers in the USA. But when the theory was first established, the authors limited their analysis to regulators generically defined. In the following years, the two authors also analyze the efficacy of the approach to grant residual powers to agencies beyond courts and regulators. In my research, I also limit my analysis to regulators generically defined.

[78]The two authors mentioned that there is a substantial debate whether common law judges actually "make" law or whether they "find" the law based on legal principles. See, e.g., Jack G. Day, *Why Judges Must Make Law*, 26 CASE W. RES. L. REV. 563, 563-65 (1994). Incomplete law theory remains neutral to the debate. The authors consider that what judges in Common Law countries do is to make legally binding precedents, which fills in some gaps in the law. This lawmaking power is one of their major functions.

Regulators

It is an alternative approach to grant residual LMLEP to regulators. Regulators exercise residual LMLEP in a different way from courts, since regulator can adapt and enforce the completeness of laws proactively through various means (Xu & Pistor (2002a):948). For instance, a regulator can control *entry to markets and access to assets, monitor activities, initiate investigations, enjoin actions, and initiate the administration of sanctions against violators* (Xu & Pistor (2002a):948). The police, illustrated by the authors, is an example of a regulator (Xu & Pistor (2002a):948). The police can *monitor behavior and seek to prevent damages by enjoining actions that are likely to cause harm* (Xu & Pistor (2002a):948). Additionally, the supervisory authorities in stock markets or the banking industry, which are the main objects of observation for Xu and Pistor, also regulators that exercise substantive LMLEP.

Different from courts, regulators can exercise the powers both *ex post* and *ex ante* (Xu & Pistor (2002a):949). Regulators can exercise residual LMPEP to respond to incompleteness more freely (but within the scope of their lawmaking rights) (Xu & Pistor (2002a):950). Regulators also can *correct past errors on their own initiative and in a flexible and responsive manner* (Xu & Pistor (2002a):951). Therefore, regulators enjoy a comparative advantage over courts in exercising residual LMLEP more flexible and in a wider range of situations (Xu & Pistor (2002a):1012).

[79]Citations in this paragraph are from (Xu & Pistor (2002a):948-49). The two authors noticed that courts can also be asked to prevent harmful actions from taking place, for example to file a motion for preliminary injunction. But this procedure is still based on someone other's motion.

Nevertheless, regulators are superior to courts only under certain conditions and constraints,[80] since they are subject to infirmities in exercising residual LMLEP (Xu & Pistor (2002a):961). Typically, over- or under- regulation is the mistakes which could be seen frequently. *Over-regulation occurs when a regulation imposes costs that outweigh the benefits of proactive law enforcement by courts* (Xu & Pistor (2002a):951).[81] Over-regulation also occurs when it chills *too many potentially beneficial actions or when well-intended regulation stifles economic activities in other ways* (Xu & Pistor (2002a):951). According to Xu and Pistor, *Regulators may also under-enforce because they face resource constraints, mis-allocate their resources, or fail to detect risks of harmful actions* (Xu & Pistor (2002a):951).

Hence, the question turns to under which conditions it may be optimal to allocate the exercise of residual LMLEP to courts, and under which conditions to allocate them to regulators? Xu and Pistor suggest two important factors for consideration: standardization and the level of expected harm (externality) (Xu & Pistor (2002a)).

Standardization:

> *refers to the ability to describe actions and outcomes at reasonable cost so that regulators can exercise their proactive law enforcement powers effectively. The effectiveness of proactive law enforcement hinges on the ability of regulators to monitor the market and identify types of actions and outcomes that reasonably may be expected to result in harmful outcome. The assessment of which actions or outcomes fulfill these conditions may change over time. Yet it is essential that regulators be able to identify and standardize in order to use their resources effectively and avoid the pitfall of over-enforcing (Xu & Pistor (2002a):952)*

The level of expected harm:

> *The constraints of ex post lawmaking and reactive law enforcement may be tolerable when the expected level of harm is low, for example, when the harm victims might suffer is small or when only a few victims are affected by harmful actions [...] If, however, the level of expected harm is substantial, [...] court enforcement will not be effective. It will typically come too late, after harm has been done. Shifting to a proactive law enforcement regime that seeks to prevent the occurrence of harm through entry barriers, continuous monitoring, and investigation, will therefore be superior* (Xu & Pistor (2002a):952)

Accordingly, regulators are only the superior option to be allocated with the residual LMLEP, when these two factors are met. The cost of proactive law enforcement by regulators can be justified only when actions can be standardized and when these actions are likely to create substantial harm which cannot be fully remedied by reactive law enforcement (Xu & Pistor (2002a)).[82]

Section Summary

The ILT can be summarized into three propositions:

1. all law is intrinsically incomplete;
2. the optimal approach to incompleteness is to allocate residual LMLEP;

[80] On the tradeoff between monitoring and investigating and the cost implications of these regulatory enforcement mechanisms, see Dilip Mookherjee & I. P. L. Png, Monitoring vis-á-vis Investigation in Enforcement of Law, 82 AM. ECON. REV. 556, 557 (1992). Using a formal model to compare the tradeoffs, Mookherjee and Png conclude that the use of these alternative enforcement devices should be tailored to the severity of the offense. Smaller offenses should not be investigated, merely monitored. Larger offenses should be investigated in accordance with their severity, and fines should be maximized (Mookherjee & Png (1992)).

[81] The two authors illustrate that the direct costs of regulation include the funds needed to hire monitors and investigators, to maintain filing systems, and to launch lawsuits. The indirect costs of regulation are comprised of the costs market participants incur because they have to comply with regulations and that society incurs when regulators either over- or under-enforce the law.

[82] Of course (yet for my research questions off-topic), the deployment of residual LMLEP competencies must be monitored and exercised within the constraints as set by the legal system that erect the regulator, as all powers have to respect checks and balances.

3. regulators conditionally have advantages over courts for holding and exercising residual LMLEP -- *i.e.*, when actions can be standardized and when substantial harm is likely to be created.

The first proposition lies the foundation of the theory, and the other two supply an analytical framework to help researchers assess the design of legal institutions as well as the efficacy of law enforcement.

Incomplete Law: Examples from Directive 95/46/EC

In this section, European data protection law is observed through the lens of ILT. The purpose of the observation is not to illustrate how good or bad drafting the Directive is. Instead, what I am interested in is the European legal system's abilities to deal with ``unforeseen contingencies." Since issues related to data protection are too broad for a compact analysis, the analysis is limited to the scope of Directive 95/46/EC.

Directive 95/46/EC is intrinsically incomplete

The Directive 95/46/EC is intrinsically incomplete because it is a general law to ``*serve a number of addressees for long periods of time and to cover a great of variance of cases*" (Xu & Pistor (2002a):938-939). Hence, the Directive could not cover all possible situations. As I analyzed above, the feature of generality determined the Directive, from the first beginning, has accompanied with "incompleteness". Moreover, the Directive 95/46/EC tries to regulate a field which is closely linked with technology. According to (Xu & Pistor (2002a):932), the law which is affected by a high pace of technological changes, is more incomplete than others, because ``*such change constantly challenges legal solutions designed to solve "old" problems and thus requires frequent adaptations of the law if it is to remain effective."* The challenges caused by technological changes will be further presented in Section 4.3. Therefore, through the lens of ILT, Directive 95/46/EC is incomplete and it is even more incomplete than other areas which may not be featured by continuously exogenous changes.

A key aspect of incomplete law is both data subjects and data processors may trouble to determine whether an action falls within the forbidden scope (Xu & Pistor (2002a):949). Data processors may find it difficult to anticipate the consequences of actions within a particular situation. If they are careless, and assume that their action will not by punished by law, harms may be resulted in (Xu & Pistor (2002a):949). Xu and Pistor point under this situation law under-deters since data subjects may be harmed (Xu & Pistor (2002a):949). If data processors are too cautious to do what otherwise would be considered legitimate business, the over-deterrence are unfavorable to the development of economics (Xu & Pistor (2002a):949). In either case, the incomplete law could not prevent damages.

Courts' efforts to address incompleteness

In order to address the incompleteness, courts, as the natural agents to grant with residual LMLEP, step in to fill the gaps left by laws. In this section, I will moreover do some research based on cases that were decided by the European Court of Justice in Luxembourg (hereafter ECJ)[83] that are also referring to Directive 95/46/EC. The reading on the case law is in order to answer: Whether the Courts adequately remedy the incompleteness of Directive 95/46/EC through exercising residual LMLEP?

The ECJ is allocated with substantial residual LMLEP. The ECJ plays an important role in shaping the common 'character' of data protection in Europe (Kuner (2007):7).[84] The ECJ involves in data protection issues through two ways: first, a member state or the Commission may bring an action before the Court, and the other one is a Member State's national court may refer questions to the ECJ for interpretation (Kuner (2007):7). For the second way, a major part of the ECJ's judicial reasoning are to determine whether Directive 95/46/EC

[83] The information about the ECJ is harvested from its official website. Readers can get access to more details about the ECJ through the following link: http://europa.eu/about-eu/institutions-bodies/court-justice/

[84] According to European data protection officer, case law decided by ECJ is a significant building block of the legal framework for data protection law in Europe. See:
http://ec.europa.eu/dataprotectionofficer/legal_framework_en.htm

and its companion directives or cases laws could extend to new cases. In this situation, the ECJ exercises the residual LMLEP through settling legal disputes (or answering prejudicial questions addressed to it by member-state courts, deciding a case).

Following, I pay attention to case study. How the ECJ exercises their LMLEP is at the center of my analysis. The background and legal contents are cited from the ECJ's judgement.

Joined Cases C-465/00, C-138/01 and C-139/01 Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk[85] *ECJ (2003)*

- Directive 95/46/EC includes a provision that the purpose of the Directive is to ensure the personal data flow freely from one Member State to another (EC (1995). The dispute referring to the prejudgement sent to the ECJ is to answer: whether Directive 95/46/EC is applicable to issues, which seems to have no relation with the issue of internal market harmonization (ECJ (2003)).
- The ECJ's response: In this judgement, the ECJ held that the Directive should apply to cases which are no link with the issue of harmonizing internal market (ECJ (2003)).
- The outcome of the preliminary ruling: The Type I incompleteness was reduced. ECJ's judgement extended the scope of the applicability to cover any actions which are different from the expression of principles and criteria laid down in the Directive 95/46/EC (*ECJ (2003)*).

Case C-101/01 Criminal Proceedings against Lindqvist[86] ECJ (judgment of 6 November 2003))

[85]ECJ, Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof, Judgment of 20 May 2003. The judgement of the case could be get access to through the following link: http://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en

[86]http://eur-lex.europa.eu provides more information about the case.

- The Directive 95/46/EC has provisions referring to the scope of its applicability (Article 3); prohibited processing categories (Article 8); restrictions and exemptions of its applicability (Article 13) and cross-border data flow (Article 25). The disputes referred to the preliminary rulings include: whether " the act of referring on an Internet page to various persons and identifying them by name or by other means" falls into the scope of the Directive's applicability (ECJ (judgment of 6 November 2003)))? whether ``processing data such as giving their telephone number, or information regarding their working conditions and hobbies constitutes is covered by one of the exceptions in Article 3 (2)"? what kind of information concerns health (ECJ (judgment of 6 November 2003)))? whether ``a transfer of data to a third country includes the occasion that load personal data onto a page stored on a server which is hosted by a natural or legal person established in a Member State and thereby making those data accessible to anyone who connect the Internet including people from third country" (ECJ (judgment of 6 November 2003)))? And if no one from third country is accessed that data (ECJ (judgment of 6 November 2003)))? Whether ``the provisions in Directive 95/46/EC bring about a restriction which conflicts with the general principle of freedom of speech" (ECJ (judgment of 6 November 2003)))? whether it is permissible for the member state to ``provide for greater protection for personal data than required by Directive 95/46/EC" (ECJ (judgment of 6 November 2003)))?
- The ECJ's response: First, information on an internet page which could identify data subjects by any means falls into the scope of the Directive; second, the information about "injured foot" in this case is concerning health; third, there is no 'transfer of data to a third country' within the meaning of Article 25 of Directive 95/46 by loading personal data onto an internet page which is stored in a server hosted by legal or natural persons in another Member State, even though it is accessible by people from third country; fourth, there is no restriction on the principle of freedom of speech and it is the national authorities and courts' responsibilities to balance these general principles; fifth,

member states' legislators must ensure to comply with the provisions of Directive 95/46/EC but are not restricted to extend the protective scope above the Directive. (ECJ (judgment of 6 November 2003)))

- The outcome of the preliminary ruling: Type I incompleteness was largely reduced. However, the Type II incompleteness was increased. Each new extended scope will eventually give rise to new litigation, as technological development would go beyond the scope of its applicability. Since courts are limited by its reactive and ex post features, they cannot easily and quickly adjust laws in response to observed changes. Before they catch up with new developments via exercising LMLEP, there is always sharp learning and waiting curve.

Joined Cases C-468/10 and C-469/10 - Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/ 10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado ECJ (2011)[87]

- Directive 95/46/EC has a provision (Article 7 (b)-(f) referring to conditions relating to legitimate interest in data processing without the data subject's consent (EC (1995)). The dispute referred for preliminary rulings is about whether Member States' national laws are entitled to add extra conditions to those required by Directive 95/46/EC?

- The ECJ's response: "*Article 7(f) must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalized way, any processing of data not appearing in such sources*" (ECJ (2011)).

- The outcome of the preliminary ruling: Type I incompleteness of Directive 95/46/EC was reduced.

[87] In the case, Spain's Royal Decree 1720/2007 which was believed to impose the extra conditions relating to the legitimate interest in data processing without the data subject's consent, which does not exist in Directive 95/46, to the effect that the data should appear in public sources. The Tribunal Supremo (Supreme Court, Spain) asked the ECJ to interpret Article 7(f) of Directive 95/46. The contents in this section are cited from the judgement. The complete version of the judgement could be access following the link http://curia.europa.eu/juris/liste.jsf?num=C-468/10&language=en

C-518/07 European Commission supported by European Data Protection Supervisor v Federal Republic of Germany ECJ (2010)

- Directive 95/46/EC includes a provision (Article 28) that the data protection authorities must be able to exercise their entrusted functions independently (EC (1995)). The dispute in the case is: how "independent" should independent agencies should be?

- ECJ's Decision: *"by making the authorities responsible for monitoring the processing of personal data by non-public bodies and undertakings governed by public law which compete on the market (öffentlich-rechtliche Wettbewerbsunternehmen) in the different Länder subject to State scrutiny, and by thus incorrectly transposing the requirement that those authorities perform their functions 'with complete independence', the Federal Republic of Germany failed to fulfill its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"* (ECJ (2010));

- Outcome of the decision: The Type I incompleteness of Directive 95/46/EC was reduced.

C-553/07 College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands [88]

- Directive 95/46/EC includes a provision (Article 12) to entrust data subjects the right to access (EC (1995)). However, the provision does not indicate ``any time period within which it must be possible for those rights to be exercised'' (ECJ (2009)). The dispute referred to the preliminary ruling is about whether Member States could impose a time restriction in their national law (ECJ (2009)).
- The ECJ's response: It is not in-proportional for Member States to fix a time-limit for storage of that information and to provide for access to that information (ECJ (2009)). Nevertheless, the storage period must take consideration of both data subjects' interests and the burden on data controllers for storage (ECJ (2009)).
- The outcome of the preliminary ruling: Type II incompleteness of the Directive is reduced since the preliminary ruling specifics a situation that shall not be prevented. But Type I incompleteness is increased.

C-524/06 Heinz Huber v Bundesrepublik Germany

- Directive 95/46/EC has a provision that requires data processing for a task carried out in the public interest or in the exercise of official authority (EC (1995)). The dispute refereed to the preliminary ruling is about whether the provision could be enforced on the grounds of nationality (ECJ (2008a)).
- The ECJ's response: According to the ECJ's judgement,[89] "*Article 7(e) is interpreted in the light of the prohibition on any discrimination on grounds of nationality, unless: 1) it contains only the data which are necessary for the application by those authorities of that legislation, and 2) its centralized nature enables the legislation relating to the right of residence to be more effectively applied as regards Union citizens who are not nationals of that Member State*" (ECJ (2008a)).
- The outcome of the preliminary ruling: The Type I incompleteness of Directive 95/46/EC was reduced. But Type II incompleteness may be increased.

[88]The contents in this section are cited from ECJ (2009).

[89]The contents in this section are cited from the judgement.

C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy(ECJ (2008b))

- Directive 95/46/EC provides exemptions for processing personal data for journalistic purposes (EC (1995)). The dispute referred to the preliminary rulings is about in which circumstances the activities at issue may be regarded as the processing of data carried out solely for journalistic purposes could exempt or derogate from data protection (ECJ (2008b)).
- The ECJ's response:[90] the notion of "journalistic activities" should encompass " *all activities whose object is the disclosure to the public of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper or radio waves or an electronic medium such as the internet) and of the nature (profit-making or not) of those activities*" (ECJ (2008b))
- The outcome of the preliminary ruling: the way the ECJ response to Type I incompleteness might increase Type II incompleteness to the Directive 95/46/EC. The interpretation aimed at broadly encompassing all journalistic activities, but each conditions the ECJ designed covered particular situation, such as medium, format of data, nature of those activities.

[90]The contents in this section are cited from the judgement.

Joined Cases C-317/04 and C-318/04 (judgment of 30 May 2006/ European Parliament v Council of the European Union ECJ (2006)

- Directive 95/46/EC has a provision (Article 26) referring to non Member States' data protection level (EC (1995)). The dispute in the case is about: whether the Commission could validly adopt the decision on adequacy on the basis of Directive 95/46/EC (ECJ (2006))?
- The ECJ's judgement: "*the transfer falls within a framework established by the public authorities that relates to public security. The Court thus concluded that the decision on adequacy does not fall within the scope of the directive because it concerns processing of personal data that is excluded from the scope of the directive. Consequently, the Court annulled the decision on adequacy*" (ECJ (2006)).
- The outcome of the judgement: The Type I incompleteness of the Directive 95 was not reduced.

The ECJ's efforts enhanced the efficiency of lawmaking, if compared with depending on legislators to update law. But, whether the ECJ's reactive enforcements adequately remedy this incompleteness? My reading of the judgements does demonstrate that the ECJ's efforts do largely remedy the incompleteness of the Directive 95/46/EC. Nevertheless, in some cases (including C-101/01, C-553/07, C-524/06, C-73/07), I also witness that ECJ's judgments create new incompleteness to the Directive. This is not a satisfactory result.

A weakness in courts' action range

Data protection law is closely related with technology. How do Courts, the reactive law enforcement agency, overcome the challenges brought by technological changes? In this Section, I focus on the challenges presented by cloud computing for regulating transnational data flow.

Currently, cloud computing raises some unique law enforcement concerns regarding, for example, the location of potential digital evidence, its preservation, and its subsequent forensic analysis.[91] The transnational data flow agreement, the U.S. -- EU Safe Harbor Framework, is also tested in a cloud computing context. In European law aspect, the Framework is to facilitate personal data to be transferred under a presumption of adequacy to U.S-based companies that agree to be bound by the system (Kuner (2007):180).

Cloud computing technology threatens to render the Framework unsafe for ``the cloud." The Dutch Data Protection Authority (hereafter CBP) highlighted three personal data-related concerns surrounding the Framework: transfer, security and processing by sub-processors of personal data in the cloud.[92] The CBP observed that sole self-certification with Safe Harbor Framework may not be sufficient in a cloud environment. It is the controllers/data clients' responsibilities to ensure that the principles (from Safe Harbor principles, from the Dutch Data Protection Act and from other additional requirements) are complied with by safe-harbor companies (Dutch Data Protection Authority (2012)). Thus Cloud Computing practices challenge the conviction that the Safe Harbor Framework provides a viable compromise.

In fact, the three personal data-related concerns not only plague the Framework, but also test the limitation of Directive 95/46/EC. Article 25 and article 26 limit the flow of data to countries located

[91] http://www.dfinews.com/articles/2013/08/cloud-computing-presents-unique-forensic-challenge#.UpUc9pEUHlU

[92] The CBP presented the three challenges when proceeding to answer the questions posed by SURFmarket. SURFmarket is a Dutch organization that undertakes joint investments nationally and internationally in IT-driven innovations. The SURFmarket submitted three questions to the CBP:

1. Does the self-certification by the American provider to the Safe Harbor Framework offer sufficient safeguards for the transfer of personal data to the United States (U.S.)?
2. Does the Statement on Auditing Standards no. 70 (SAS 70) standard offer sufficient certainty regarding the security of the processed personal data, or are the International Standards for Assurance Engagements (ISAE) 3402 and Statement on Standards for Attestation Engagements (SSAE) 16 standards better equipped for this purpose?
3. Is the self-certification of the American provider to the Safe Harbor Framework sufficient to safeguard that sub-processors engaged by the provider satisfy a comparable suitable level of protection (Dutch Data Protection Authority (2012))?

outside the EEA when such countries (or the recipients) can not provide an adequate level of personal data protection (Article 29 Working Party (2012):17). These articles evoke discussion. The premise underlying them is that the location of personal data is clear. This premise is in step with the technology of the time when the Directive was enacted. Generally, the specific technological horizon was featured by relational databases and `island' computing, and by the business practices that these features supported for personal data processing. It may have been common sense at the time of enactment, that the location of personal data was easily identified: where the data is at a certain moment and by whom and how it is being processed. However, through the lens of current tech-level optics, this perspective has become obsolete for a growing collection of business practices. Against the diversity of cloud computing services, the cloud client[93] is rarely in a position to know in real time where the data are located, stored or transferred (Article 29 Working Party (2012):17). As the 'International Association of Privacy Professionals' described, ``*data are stored and processed remotely, or in places far away, often in multiple places with different jurisdictions and legal regimes*" (Hogan Lovells Law Firmer (2011)). And Widmer (2009) submits concerning e-mail services based on cloud computing: ``*the customer's data can be stored anywhere in the world, depending on where the servers are located*." Hence, it is impossible, both for the cloud clients/controllers and for the cloud providers/processors to say where the data are at a certain moment and by whom and how it is being processed. Thus employing the cloud computing platform for ICT services even further[94] tests in practice the efficacy of the Articles 25 and 26.

Moreover, data flows within Europe also test the limitations of the applicability principle in the Directive. The applicability principle is governed by Article 4.[95] According to Article 4, the applicability of national laws is determined either by the location of the establishments of controllers or by the location of the means or equipment being used when the controller is established outside the EEA (Article 29 Working Party (2010b):17). As Moerel concluded, ``the connecting factor for applying the Data Protection Directive is based on the territoriality principle and limited to situations where foreign controllers use processing 'equipment' located within the EU" (Moerel (2011):91). However, the complexity of applicability issues is multiplied by cloud computing. Personal data may be transferred within the cloud provider's proprietary cloud, which can cover several Member States. As a result, it is no longer quite certain who is the controller that ``*determines the purposes and means of processing personal data*" (EC (1995): Article 2). Moreover, Hon & Millard (2008) correctly warn in their blog that ``*cloud users who process personal data in the cloud will be controllers unless an exemption applies, e.g. private use only, as with purely personal webmail. Cloud service providers are generally treated as processors. But the roles taken by cloud service providers are not limited to being processors, but may also and concurrently, in some situations, turn into being controllers*." This feature blurs the demarcation lines between data controllers and non controllers, which might easily turn into another[96] force that works towards the dilution of EU privacy law.

[93]The "cloud client" is the W.P.'s equivalent for the Directive's controller where personal data protection "in the cloud" is concerned (see Hogan Lovells Law Firmer (2011):5 and Article 29 Working Party (2012)).

[94]As many expect to be the case, considering the growing success of the cloud servicing business model.

[95]Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

[96]Zwenne (2013) discusses the problems of privacy-law dilution that result from over-expanding the conceptual demarcations of "personal data."

The three arguments illustrate how cloud computing questions Directive 95/46/EC. Distinctions can be made between the technologies that are regulated by law and the technologies that are not (and that need to be regulated). These distinctions do cause problems for the Directive to provide clear formulations. Incompleteness of both types comes to the fore. As a matter of fact, the emergence of new technology like cloud-computing services has set the EU legislature more incomplete.

Naturally, cloud computing should not become a technology that can evade data protection requirements. However, the significant limitations of courts for exercising LMLEP are highlighted in this case. As the ``ultimate arbiter'' (Kuner (2007):7), the ECJ is passive and can only exercise their LMLEP after a motion has been filed. I do believe that the judges in the ECJ are aware of the data-protection problems under cloud computing business models. But they do not have the power to take action, since no case is brought to the ECJ (until now). The ECJ has to remain passive until others bring actions, even though judges may have designed a strategy on how to exercise their LMLEP. Thus, although it is possible that the ECJ would stretch the scope of Directive 95/46/EC to encompass cloud computing, uncertainties remain for the personal data processing industry about what actions would lead to liability in practice. This situation does, in fact, undermine the effectiveness of the law.

Legislators nor courts offer complete solutions

In this section, I used the example of Directive 95/46/EC to exemplify the proposition that the European legal system over data protection is intrinsically incomplete. The incompleteness is determined by the feature of generality, since it was designed to serve general cases. Moreover, legislators can not foresee unambiguously all future changes, developments and obstacles related to data protection issues, and therefore they can not write a law to regulate unambiguously all future contingencies. In fact, legislators have paid and are paying significant efforts (such as amendments) to prevent and to remedy incompleteness. Nevertheless, Directive 95/46/EC was written prior to the developments of and changes in the (in the ICT sector highly volatile) exogenous environment, independent of when or how it is

drafted. It is highly unlikely that it will always be able to offer clear answers to new cases and it is very probable that it will increasingly become incomplete with the life cycles of technological innovations becoming shorter, while concurrently the mechanisms that prepare adaptations of the law require more time.

In this situation, the ECJ steps in and tries to offset the incompleteness. The Court is quite capable of, as the Incomplete Law theory expected, ``adapting existing legal principles to the changing environment'' (Xu & Pistor (2002a):979). In each case, courts, as the theory worried, ``faced the dilemma of adhering to well-established legal principles or extending them to fit the needs of the new types of cases before them'' (Xu & Pistor (2002a):989). But in most cases, judges re-identified the scope of laws to include the new issues. Thus, the scope of the Directive becomes more and more extensive.[97]

However, the analysis above also demonstrates the limitation of courts' rulings when exercising the residual LMLEP. First, in some cases, the amendments even lead to new incompleteness, as each new development creates new questions. Second, the amendments can only come *ex post* and reactive to the specific exogenous change (and, of course, within the bandwidth provided by a reasonable interpretation of the Directive). In this section, I focus on the challenges presented to regulate personal data flow by cloud computing technologies. The analysis showed that prior to the current `big' developments in ICT technology (*e.g.,* cloud computing, mobile internet and telephone converging, etc.), the concept of data protection had been well defined and was in harmony with the current of the time. But along with the exogenous changes that happened in the environment, the existing law lost its clarity on some relevant issues and became ambiguous, especially when facing new ICT. However, the courts, constrained by their reactive enforcement mechanism, cannot help but watch the emergence of a growing protection gap.

The above discussion signaled that Courts do not offer fully satisfactory solutions in the ICT-related area, as it is subject to considerable exogenous changes in very limited time spans. It also signaled

[97] This might be an analogous mechanism as the one Zwenne brings to the fore. He argues, as hinted earlier, that the broader definition of "personal data" may lead to the indefinite expansion of the scope of the Directive, and consequentially, to a complete loss of foreseeability (Zwenne (2013)).

that the resulting ambiguities will decrease the law's effectiveness. Thus, that it is very difficult, perhaps even impossible, to address incompleteness of data protection law solely by depending on courts.

An alternative strategy: the regulator

In response to the problem, rather than frequently changing laws or solely depending on courts' reactions, European policymakers created a unique institutional mechanism, the "data protection authority," to take up the functions required. From the vantage point of the theory of incomplete law, the most important contribution of the Directive 95/46/EC is the creation of a multiple-layered regulatory system that combines *ex ante* rule-making with proactive enforcement powers. This does not mean that court enforcement has been replaced by regulators. Instead, regulators are vested with residual LMLEP to complement court enforcement. In the subsequent analysis, I will analyze the European data regulator's responses to the challenges posed by the incompleteness of Directive 95/46/EC.

The multiple-layered regulators' System

A multiple-layered regulators' system that combines *ex ante* rule making with proactive enforcement powers was created in order to ensure the compliance of data protection law in both European level and National level.

European Data Protection Supervisor (Hereafter: EDPS) is a significant supervisory agent at European level. It is an independent supervisory authority and responsible for making sure compliance of the EU institution and bodies with data protection law (Kuner (2007):7). The EDPS was established in accordance with Article 286 of the Treaty of Amsterdam[98] and Regulation 45/2001.[99] And the status of the EDPS and general conditions for governing were further clarified by Decision 1247/2002 (Kuner (2007):8).[100] EDPS is

[98] European Union (1997)

[99] European Commission (2001)

[100] European Commission (2004)

equipped with legal authority to exercise residual LMLEP. It has substantial influences on policymaking at EU level since it could advise European Commission, European Parliament and the Council on proposals for new legislation or amending (Kuner (2007):9).[101] And the EDPS could intervene ex ante since it could monitor the processing of personal data through prior checking processing operations likely to present specific risks, handling complaints and conducting enquiries (Kuner (2007):9).[102] In each EU institution, a Data Protection Officer is appointed to ensure the internal application of the Regulation in close cooperation with the EDPS.[103]

The EDPS is significant to cooperate national data authorities. The central platform for the cooperation is Article 29 Working Party. The Article 29 W.P. is established in accordance with Article 29 of Directive 95/46/EC. It is an independent advisory body comprised of representatives of national data protection authorities (Kuner (2007):9). The Article 29 W.P. publishes a large amount of opinions and recommendations on various data protection topics, for instance Article 29 Working Party (2009b) which will be analyzed in Chapter 5. Although the documents published by Article 29. W.P. do not have legal binding forces, the documents tend to be quite influential and in effect represent a sort of crystallization of legal opinion (Kuner (2007):9).

Moreover, at the European level, there are some other institutions which play the role of supervisory authority. For instance, the Article 31 Committee which is established in accordance with Article 31 of Directive 95/46/EC could take decisions for which Member

[101] e.g. Opinion of the European Data Protection Supervisor regarding a joint communication by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace

[102] e.g. Several cases before the General Court on the relationship between public access to documents and data protection: Cases T-170/03 (British American Tobacco v. Commission), T-161/04 (Valero Jordana v. Commission), T-194/04 (Bavarian Lager v. Commission) and the subsequent appeal before the Court of Justice, C-28/08 P, T-3/08 (Suárez v. Council), T-82/09 (Dennekamp v. Parliament) and T-190/10 (Egan and Hackett v. Parliament);

[103] The Information is cited from European Commission's official website about the Data Protection Officer, available at: http://ec.europa.eu/justice/data-protection/bodies/ officer.

State approval is necessary (Kuner (2007):10); and the European Ombudsman which is appointed by the European Parliament could investigate complaints from natural and legal persons (Kuner (2007):12).

At the national level, a Data Protection Authority (Hereafter: DPA) must be established and responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive (EC (1995): art.28). These authorities shall act with complete independence in exercising the functions entrusted to them (EC (1995): art.28). National DPAs are granted with substantial powers, although there are many differences in the powers granted by national legislation (Kuner (2007):15). The National DPAs are in charge with, but not limited to, investigating powers, powers of access to files and filing systems, intervention powers, the power to order the blocking, erasure and destruction of data, the power to impose a ban on the processing, the power of warning or admonishing the controller and the powers of sanctions. (European Commission (2003):39-41)

Regulators exercise LMLEP

This section explores the functions of data regulators in Europe, in particular in the deployment of residual LMLEP, both at the European and at the national levels.

The Regulators at European Level

Residual LMLEP are granted to regulators at the European level. In this Section, I focus on the role of Article 29. W.P. in mitigating the incompleteness of data protection law. The Working party is an unique event within the European institutional landscape since no similar agency can be found at European level (Poullet & Gutwirth (2008):2).

Since Article 29. W.P. does not involve in investigating and monitoring data processors' practice, the main efforts that it pays to mitigate the incompleteness of law is to adapt the European data protection legislative framework in accordance with the changing society, especially the new technologies which continuously create new privacy threats (Poullet & Gutwirth (2008):2), which can be seen as

ways to support the development of more complete laws (or law interpretations) to deal with data protection issues. For instance, with the emergence of Facebook, data protection in social networking services became the center of attention. The Working Party has not hesitated to intervene the topic. In 2009, the Article 29 W.P. delivered "*Opinion 5/2009 on online social networking*"(Article 29 Working Party (2009b)), to react the social-network issues at stake. WP 163 sets up very general standards for social networking service providers to comply with. Then the standards are employed by national data regulators to assess different cases. According to the Irish Data Protection Commissioner's audit report (Irish Data Protection Commission (2011)), the national regulators can adapt these rules and shape them to their special needs.[104] However, I could not find any actions that legislators do to adjust the rules in response to observed risks. This is a typical case to show how the Working Party exercises its residual LMLEP to adapt rule-interpretation in response to these technological changes. This reflects the flexibility of regulators on exercising LMLEP at multiple levels. As Xu and Pistor argue, "*regulators need not go through a lengthy lawmaking process, but may, within the scope of their lawmaking rights, adapt and change the law in a simplified procedure...*"(Xu & Pistor (2002a):950), *"...independent of whether violations have occurred, or when others have brought problems to their attention...*"(Xu & Pistor (2002a):954).

What is remarkable is that the Article 29 W.P. is just an advisory body. This means the opinions issued by the Working Party do not have binding legal character (Kuner (2007):10). Nevertheless, according to its rule of procedure, any of its issued documents will be automatically forwarded to EU Commission, to the European Parliament and other related alliances, even though the legislators do not have any motivation to amend any data protection legislative framework (Poullet & Gutwirth (2008):6). Through this way, they do help prepare law for legislators and they do influence law enforcement activities. Although it is one step removed from lawmaking and law enforcement, it thus combines important functions that I have associated with an agent which exercise residual LMLEP. In the light of

[104]Irish Data Protection Commissioner adopted the standards set by the Article 29. W.P. to evaluate Facebook's data protection level.

this performance, Article 29 W.P. bridges the gap left by legislators.

National Data Protection Authority

The National DPAs largely mitigate the incompleteness of data protection law when they exercise the residual LMLEP granted to them. The substantial residual LMLEP are taken up by national DPAs, as the ILT expected, ``in response to the problem of existing law's underdeterrence and the resulting widespread violations of data subjects' rights" (Pistor & Xu (2002b):996). It is not difficult to find cases which national DPA exercises its LEP. For instance, in Germany:

> *On November 23, 2010, the data protection authority (DPA) of the German Federal State of Hamburg imposed a €200,000 fine against the Hamburg-based savings & loan Hamburger Sparkasse due to violations of the German Federal Data Protection Act (the BDSG) for, among other reasons, using neuro marketing techniques without customer consent. The case – which attracted much negative publicity in Germany, including page 1 headlines and "top spots" in television news – may very well influence the assessment of neuro marketing techniques under data protection laws beyond Germany (Cohen (2010))*

Through the enforcement of residual LMLEP, national regulators link the standards and responsibilities for data protection compliance with provisions of Directive 95/46/EC in practice.

The national regulators also exercise extensive residual LMLEP to adapt rules in incomplete law when it deems necessary. Normally, national regulators engage in lawmaking activities proactively and promulgated industrial guidelines. For instance:

> *The German data protection authorities on September 26, 2011 adopted an "Orientation guide – cloud computing." The guide sets out mandatory and recommended content for any agreement between German users of cloud computing services ("customers") and cloud computing service providers. It highlights the customer's responsibility for full compliance with German data protection requirements for the cloud. Based on this orientation guide, customers and providers will have to review existing agreements in the German market.*
>
> *Privacy and data protection compliance has been a challenging and unclear issue for cloud computing customers and service providers. The new German "orientation guide", adopted by the Munich conference of the German data protection authorities gives clear guidance to cloud computing service providers and their customers in the German market. Privacy practitioners can expect that German DPAs will refer to this guide when addressing situations that raise close questions about the application of data protection laws to cloud computing (Stefan.S (2012))*

The lawmaking activities of national regulators enhance overall protection for citizens and increase the visibility of national authorities in society.

Summary:

The current brief overview demonstrates that data regulators are given extensive residual LMLEP. The story in Europe offers important insights into the benefits of a system that offered not only reactive but also proactive enforcement. Similar as regulators in financial, environmental and other areas, data regulators work differently from legislators and courts. Data regulators react to technical development much quicker than legislators who are constrained by procedures. Data regulators also exercise their residual LEP proactively rather than courts who can only apply their residual LEP reactively. Generally, data regulators exert the flexibility of the rules in Directive 95/46/EC. Although the original reason of the emergence of data regulators is not in response to the functional problems of incomplete law, the introduction of regulators can be seen as a successful shift from reactive to proactive law enforcement and reallocation of some lawmaking powers to regulators (Xu & Pistor (2002a)).

Limitation of study

In this Chapter, I have analyzed the problems that confront European laws over data protection issues as example. The analysis used the established framework of incomplete law theory.

The most obvious limitation of the study is its cross-sectorial application of the incomplete law theory. In fact, the incomplete law theory was created to explain/address the legal problems in financial market. The result of my experimental application thus was difficult to foresee. Indeed, Xu and Pistor believe their theory's basic principles are not limited to financial issues, but do apply to any field that "needs to consider the allocation of lawmaking and law enforcement powers"(Pistor & Xu (2002b):936).[105] Nevertheless, the framework has never been applied beyond corporate-law and financial-market regulations. Moreover, the uncertainties of the results increase since the theory is basically derived from the study of legal economy. Incomplete law theory is exploratory in itself. The theory is equally incomplete as incomplete laws are.

Second, when they established and analyzed the theory, Xu and Pistor "*downplay incentive problems different lawmakers and law enforcers may face, including problems of regulatory capture or corruption, in order to highlight the central issues associated with incomplete law*" (Pistor & Xu (2002b):935) Although they recognize that these issues are of great importance, Xu and Pistor do not analyze them and their relations to incomplete law theory.

Third, Xu and Pistor's study used samples of UK, US and German experiences over financial market's development. However, this selection led to a problem for generalization, which may be limited by contextual differences in policy, governance, culture, and history as well as other potential differences in regimes which were not selected in this study. For instance, the analysis in '*Beyond law enforcement-governing financial markets in China and Russia*' shows that the intervention by financial regulators which is recommended by incomplete law theory works less well in transition economies (Pistor & Xu (2004)) Moreover, incomplete law theory can not explain the divergent experiences of Russia and China in developing financial markets

[105]The two authors illustrate that *environmental, safety, food and drug regulation* are fitting fields to adopt this analytical framework.

and the standard enforcement practices (Pistor & Xu (2004)). These findings show us that incomplete law theory is not always relevant (or complete).

Further work is needed to validate the applicability and relevance of the theory and the implications for different legal regimes. Here, I will leave these questions open. On methodological ground, I argue that the theory provides a useful conceptual analysis model for my research where it concerns EU data protection regulation. It produces a useful model for the design of effective enforcement. And it offers me a fresh perspective to peer into the European legal system over data protection issues. My analysis suggest, that the theory is both appropriate and useful as a framework for guiding our analysis.

Conclusion

The chapter deploys the theory of Incomplete Law, which is created by Xu and Pistor. The theory includes three propositions: 1) law is intrinsically incomplete, since lawmakers are unable to foresee all future contingencies and thereby they cannot write a complete law; 2) when a law is incomplete, law enforcement that relies exclusively on courts which enforce laws reactively is not sufficient; 3) regulators, which are vested with proactive law enforcement and residual lawmaking powers, is the optimal solution in an incomplete legal world in order to achieve optimal deterrence effects, given specific conditions (Xu & Pistor (2002a)). Regulators can better respond to the problem of ineffective enforcement caused by incomplete law, since they perform their functions flexible and reactively (Xu & Pistor (2002a):1012).

In this chapter, I applied the theory to the European legal system over data protection issues. The analysis shows that, in Europe (i) lawmakers can not formulate all relevant issues in data protection laws and (ii) courts could not offer satisfactory solutions to incompleteness of law. But the problem caused by incompleteness of law is largely mitigated by an unique European creation: a multiple layered data authorities. I paid attention to the Article 29 W.P. and to the national data authorities (DPAs) that take significant roles in keeping the regulation in step with technologic innovation. My finding is that data regulators are vested with substantial LMLEP. Data regula-

tors are more flexible in adapting law over time than legislatures are. Many challenges brought by technical developments do not make the legislator modify laws because regulators preemptively fill the gaps. Regulators determine the flexibility of these rules by clarifying the conditions that companies should comply with in order to respect the right to personal data keeping up with exogenous changes. As proactive law enforcers, they can initiate actions and exercise enforcement rights in situations where courts, by design, must be passive and wait for others to bring action. Many potentially harmful actions do not make it to the ECJ, because they are caught preemptively by regulators. Regulators enforce laws to recover or prevent injuries caused by harmful actions.

The story in Europe offers important insights into the benefits of a system that not only offers reactive but also offers proactive enforcement. The findings in Chapter 4 reject the assumption (which China's policymakers nurse) that European data protection law is complete, and that the transplantation scheme can be confined to material, positive data protection laws. I show that, beyond their expectations, issues of dynamics in technology are not trivial and require measures that safeguard the availability of a highly informed and highly responsive authority that has sufficient residual LMLEP to guard the law's incompleteness will not become intolerable. I conclude that legal transplantation as envisaged will not ensure effective consequences unless a competent regulatory authority is in place. The lessons drawn from this Chapter call for a rethink of China's legal transplantation strategy.

Until now, the previous three Chapters, from Chapter 2 to Chapter 4, focus on legal design from a positivism perspective. However, this is not enough since there is an underlying tension between performance of law and design of law which requires a binary treatment (Rappaport (2014):7). Without an exploration on the performance of law from a realism perspective, it is unlikely to realize the competences of law which will not be achieved in performance. This would influence China's policymakers to anticipate the effectiveness of imported law. The following Chapter is stressed by this need.

Chapter 5

Compliance With Law

Introduction

In the previous chapter, with the help of ILT, I showed that the Directive 95/46/EC is highly incomplete. Hence, the residual LMLEP should be re-allocated to maintain the efficacy of data protection law, as the ILT suggests. In chapter 4, I provided evidence for the hypothesis above by analyzing the European allocation of LMLEP to regulators. What is, therefore, evident is that data authority should be paid attentions to by China's policymakers.

Yet, the importance of data authority is only the starting point, giving rise to two series of questions. First, how do European data authorities supervise data users? What are the implications of EU data protection law transplantation to China, considering especially the institutional need for law enforcement in such an unpredictable environment of data protection? Second, even if data regulators in Europe can provide more safeguards to data subjects that data authorities in other regions cannot, the question remains whether any agency in China would be competent enough to undertake the task of supervising such a rapidly changing sector. What would happen if the roles of the European data authorities were transplanted to China? Even in Europe, data authorities have trouble-conducting audit. For instance, the French data authority, the CNIL, received several warnings and complaint letters and one financial sanction, just because it underlined its audits of video-surveillance systems (over 170 audits in 2012) ((Maxwell & Souza, 2013)).

In this Chapter I answer the two series of questions above, by placing RenRen in the hypothetical position of promoting its business in Europe, while establishing its European headquarters in a fictional European-Union member state (RR-EU). In doing so, I can analyze the application of European data protection law practice to an existing Chinese personal data use practice. Through testing how EU data regulators would implement data protection to China's Facebook, I attempt to anticipate the daunting challenges that need to be faced by China's policymakers and the relevant legal agencies in the process. The reason why I use Social Networking Services (Hereafter SNS) as the unit of analysis is because there is already an established audit report on Facebook, made by the Irish Data Protection Commissioner (Irish Data Protection Commission (2011)). In this audit report, the Irish data authority took the "Opinion 5/2009 on online social networking" (Hereafter WP163), released by the Article 29 Working Party (see Article 29 Working Party (2009b)), as a yardstick on researching the compliance of Facebook's practice. Therefore, the same set of standards is applied to RenRen in order to test its data user's compliance. Concerning SNS and based on WP163 and the directive, I describe the main issues regarding the proper implementation of data protection principles and rules, as follows:

1. **Adequate security measures**. WP 163, p 7 states: *"Controllers must take the appropriate technical and organizational measures, 'both at the time of the design of the processing system and at the time of the processing itself' to maintain security and prevent unauthorized processing, taking into account the risks represented by the processing and the nature of the data* (Article 29 Working Party (2009b))."

2. **Adequate default privacy settings**. WP 163, p7 states: *"SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties. Restricted access profiles should not be discoverable by internal search engines, including the facility to search by parameters such as age or location* (Article 29 Working Party (2009b))"

3. **Adequate information to be provided by SNS.** WP 163, p7 states: "*SNS providers should inform users of their identity and the different purposes for which they process personal data according to the provisions laid out in Article 10 of the Data Protection Directive...*(Article 29 Working Party (2009b))"

4. **Special regime for sensitive data.** WP 163, p 7 states: *"Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life is considered sensitive ... As data controllers, SNS may not process any sensitive data about SNS members or non-members without their explicit consent* (Article 29 Working Party (2009b))."

5. **Only legitimated processing of personal data of non members.** WP 163 explicitly forbids SNSs to process such data about non-members (Article 29 Working Party (2009b)). The criteria for exemption are laid down in Article 7 of Directive 95/46/EC.

6. **Transparent filtering of third party access**. WP 163, p8 states that if third-party applications are offered by the SNS, the site should "*provide clear and specific information to users about the processing of their personal data and that they only have access to necessary personal data. Therefore, layered access should be offered to third party developers by the SNS so they can opt for a mode of access that is intrinsically more limited. SNS should ensure furthermore that users may easily report concerns about applications* (Article 29 Working Party (2009b))." If the third party access is mediated by users, SNS should *"provide for a level of granularity that lets the user choose an access level for the third party that is only just sufficient to perform a certain task*."[106]

7. **Legitimate direct marketing.** The Working Party emphasizes that marketing should comply with data protection requirements identified by the Data Protection Directive. Since the requirements for direct marketing are still in dispute, the Working Party

[106] Article 29 Working Party (2009b).

has not yet given its opinions on this issue (Article 29 Working Party (2009b)).

8. **Legitimate retention of data.** Different services provided by a SNS may fall under different Directives' obligations on data retention. When we turns to SNS, the retention issues, particularly to determine the appropriate retention periods, becomes even more complicated. Different services provided by a SNS may fall under different Directives' obligations on data retention (Article 29 Working Party (2009b)).

9. **Inspection and rectification rights of the users.** WP 163, p11 states: ``*SNS should respect the rights of the individuals concerned by the processing according to the provisions laid out in Articles 12 and 14 of the Data Protection Directive* (Article 29 Working Party (2009b))." The rights include ``*a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her* (EC (1995))."

10. **Adequate support for the protection of children and minors.** The Working Party sets a multi-pronged strategy to address the protection of children and minors' data in the SNS context (Article 29 Working Party (2009b)).

These ten principles provide an adequate specification model of a minimal set of measures that administer a minimum level of data protection. I will use these principles as indicators to investigate how RR-EU fits in the European privacy standards. Thus, I produce a functional description of the criteria that RR-EU would have to meet in reality.

Compared with Chapter 2, a different set of methods is adopted. The conclusion of the thought experiment in Chapter 5 reflects a perception based on the provisions in written codes. Although Chapter 5 starts (like Chapter 2) with a thought experiment, the comparison is not for demonstrating the differences in the two regions from a formal-law or positivist perspective. Instead, it explains that China's legal arrangement over data protection issues might (from a realist perspective not be equally successful as the European one in creating a sustainable data protection environment, even though it may follow the blueprint of the European model.[107]

The Chapter proceeds as follows: In Part 2, I use the experience of regulating Facebook and China's Facebook (in a thought experiment) to exemplify the strength and weakness of data regulators. In part 3 I identify the key conditions that may undermine the classic form of law enforcement that has been tried and tested in Europe. I conclude that the standard regulatory mechanism of law enforcement in EU may not work effectively during the early period of the data protection institution's development.

Regulatory institutions and company behavior

In this section, I explore the experience of the two companies in order to examine the compliance with the law in practice.

[107] This two-prong approach, positivism and realism, finds support in the very recent study by Rappaport (Rappaport (2014)) - to be published in the California Law Review). An important citation form this work:

> " ... the Court must decide whether to address its decision directly to rank-and-file officers or instead to political policymakers, such as legislators and police administrators, who in turn will regulate officers on the street. In the former, dominant model, termed here first-order regulation, the Court tells officers precisely what they can and cannot do. In the latter model, second-order regulation, the principal objective instead is to enunciate constitutional values and create incentives for political policymakers to write the conduct rules. Framed differently, the Court, as principal, enlists political policymakers as its agents in the regulatory enterprise. This Article is the first to apply an agency framework ... "

This quote shows that Rappaport's conceptualization of first- and second-order regulation of law enforcement is quite coherent with my two-pronged approach (i) in the sense that the intended audience is important, (ii) in the sense that Rappaport's first-order regulation employs a positivist perspective and Rappaport's second-order regulation is only visible from a realist perspective, and (iii) in the sense that positivist and realist perspectives are not conceptually anomalous – their audiences may exclude each other, but both perspectives may help our understanding concurrently.

The case of RenRen

Here I describe the experience of European data regulators while supervising RenRen. I "act" as an authorized researcher. It is my task to assess whether RenRen provides an adequate level of protection, concerning the personal data it has access to. First, I provide a brief overview of RenRen.

The RenRen Network (pinyin: Renrenwang; literally "Everyone's Website"), formerly known as Xiaonei Network (literally "on-campus network"), is a Chinese social networking service, founded in 2005.[108] It has been called the "Facebook of China", and is popular amongst college students ((Davidoff, May 31)). Unsurprisingly, the site has stored a rich and wide variety of its users' data. [109]

Yet, RenRen does not have a good reputation for its data protection policies and practices. It is not uncommon to find news in the media about RenRen's infringing privacy protection. A case in point happened on December 22th, 2011, when RenRen leaked the personal data of 5 million users, whose user names, passwords and email addresses, all in clear text, became available online to download.[110]

That incident illustrates the relevance of my research question: If RenRen had a European office and was widely used by European users, such a scandal would make RenRen prima facie vulnerable to severe sanctions by the European data protection system and by its users. If that were the case, it is necessary to understand how a data authority would conduct an audit in reaction to the event. Hence, I hypothesize that a citizen or a privacy advocacy group in the fictional European member state has submitted a complaint to its data protection authority regarding RenRen's data leakage. Consequently the Authority decides to conduct an audit on RR-EU's data protection

[108]The information is from RenRen's site.
http://www.renren-inc.com/zh/info/breakingnews.html

[109]The information is from SinaNews "Chenyizhou: RenRen has 200 millions Users.", in 2012-02-14. The link to the news is
http://tech.sina.com.cn/i/2012-02-14/12486721576.shtml, last access 2013–4-29

[110]The information is from Sohu News: RenRen suggests its users to change password because of security reasons" in 2011-12-23. The link to the news: http://news.sohu.com/20111223/n329982775.shtml, last access 03/04/2013)

practice, assigning me, the authorized researcher, to identify and report on the compliance level of RenRen's data-protection practices.[111] The audit report follows.

Adequate security measures Adequate security is a necessary condition for any online firm's appeal to users. Consequently, the motivation to support the security of RenRen's operation does not need any backing by law or agreement. Since `digital' security in practice is beyond my focus, the issue is considered complied

Finding: RenRen has ample incentives (think of the 2011 scandal) to take measures for adequate security.

Privacy setting When a user registers in RenRen, the default settings chosen by RenRen are liberal. RenRen explained that this might help users interact with each other. Meanwhile, RenRen offers privacy-friendly options that its users may specify. The privacy options allow users to freely and specifically consent to any access to their profile's content. Users can decide who can get access to their personal webpage, who can connect with them, whether the user's content can be searched, and how to prevent being disturbed by someone. The access options are layered over three levels, from liberal to restricted: everyone (liberal), friends and city-mate, company-mate, school-mate (medium) and friends (restricted). I analyze the options in the sequence of four categories.

First, RenRen offers several settings for access. The User is able to decide (using web forms) who can get access to his personal page. I give a single screenshot as an example in following Figure.

[111]The investigation and our task are analogous to what the Irish data protection commission did on Facebook in Europe. The Office of the Irish Data Protection Commissioner, Ireland published the outcome of its audit of Facebook Ireland (FB-I) on 21 December 2011. The audit was conducted over the previous three months including on-site in Facebook Ireland's Headquarters in Dublin. The Report is a comprehensive assessment of Facebook Ireland's compliance with Irish Data Protection law and by extension EU law in this area. See Irish Data Protection Commission (2011).

Figure 5.1: Example of a RenRen screenshot

RenRen also offers a privacy shortcut to users to decide who can see 'my file'. Then, any access to their webpage is filtered by this general standard. Meanwhile, users can also set different access levels to different kinds of content. RenRen further offers settings to users to decide who can look up their profile, including basic information, personal information, educational background, career, 'post on your wall' and wall-posts by others in their profile. It also offers settings for contact information to enable users to decide who can see the contact information they provided to RenRen, including QQ or MSN numbers, telephone numbers and personal blogs. In addition there are settings for template contents, including albums, posts, sharing and gifts, to enable users to decide who can see their "file" in the future.

Second, RenRen offers settings for connection. Users can decide who can send friend requests and who can send RenRen messages.

Third, RenRen offers default privacy settings to restrict public search. Users can control whether people who enter their name in a search engine can see a preview of their RenRen profile or ensure that uploaded photos cannot be enabled by default. Since some search engines cache information, their profile information is only available for 7 days after their turn the public search off.

Fourth, RenRen offers settings to prevent online harassment. A user can block someone from befriending him and can prevent him from starting conversations or seeing what the user has posted.

Findings: RenRen has made efforts to design privacy settings and make them easy to understand and use. Privacy controls are available for users to create an appropriate balance between free interaction (which is the nature of a social network in any case) and an individual's control over sharing personal information.

Information to be provided by SNS RenRen has a very short privacy policy. From this privacy policy, I collect some basic information that I can measure with the above indicator-principles.

- Usage of the data for direct marketing purposes (Article 29 Working Party (2009b)): I could not find related paragraphs in Privacy Policy.
- Possible sharing of the data with specified categories of third parties (Article 29 Working Party (2009b)): RenRen states that users take the burden of privacy risk if they give permission for third party access. Yet, the SNS does not clearly inform the users that when they use an application, their private content and information will be shared with the application.
- An overview on profiles: their creation and chief data sources (Article 29 Working Party (2009b)): Users can get an overview on profile.
- The use of sensitive data (Article 29 Working Party (2009b)): RenRen does not give users any information on special protection of sensitive data.
- SNS providers provide adequate warnings to users about the privacy risks to themselves and to others when they upload information on the SNS (Article 29 Working Party (2009b)): RenRen states to its users that it will try its best to protect user privacy. It appears that RenRen considers this as a sufficient warning to its users to care themselves about privacy risks, considering I do not find any other, direct warnings about this issue.
- SNS users should also be reminded that uploading information about other individuals may impinge upon their privacy and data protection rights (Article 29 Working Party (2009b)): RenRen's Privacy Policy does not contain any notice to inform users that processing others' information may lead to privacy risks for others.

- SNS users should be advised by SNS that if they wish to upload pictures or information about other individuals, this should be done with the individual's consent (Article 29 Working Party (2009b)): RenRen's Privacy Policy does not contain any notice to inform users that others should give their consent for processing such data.

Findings: RenRen has made some efforts to keep its services transparent for its users but, taking the EU principles in to account, it is recommended to improve transparency further.

Sensitive data In a RenRen user's personal profile, the key personal information is one's college, high school, and hometown. Additionally, users can also decide to publish information about how to be contacted, about hobbies, favorite music, movies, and the clubs they joined, etc. I do not find any sensitive data solicited for by RenRen in its users' profiles.

Findings: RenRen meets the requirements on avoiding collecting sensitive data.

Processing data of non-members RenRen has a 'find your friend' feature. This feature not only allows users to try and find friends on RenRen, but also allows RenRen to send invitations to non-members to join. RenRen generates the addresses for the invitations automatically. For RenRen, the feature of 'find your friend' thus becomes an important marketing instrument for increasing its user base.

*Findings:*RenRen does not offer any opportunities to non-users to give consent for the retention and processing of their information. Thus, the RenRen's feature of 'find your friend' is designed to be used in conflict with the requirement related to processing non-members' personal data.

Third party access In July 2007, RenRen facilitated access to its open platform to allow third parties to develop applications.[112]

[112]Information is from RenRen's APP website "Xiaonei.com opened its App Platform for third-party developers 07/2009", http://www.renren-inc.com/zh/info/breakingnews.html, last access 2013-04-05.

Third-party developers can publish and document application programs, such as games and quizzes, in the open platform and then integrate them into the RenRen platform. Third-party applications can help users enjoy improved efficiency and added facilities. However, the third party can get access to the users' personal data (like their current location). In fact, when a user releases these data to the application, the responsibility to protect the user's privacy falls on the third party.

RenRen states that a third-party application only can gain access to a user's personal data when the user grants permission to add the application. Moreover, a third-party application is only activated for a user when a user grants permission to it.

Here I employ the application of a personality test as an example to show how users can grant permission to an application via a permissions screen. Via this screen, users grant permissions to the third party to access `my profile' and `friendship' information, to access their posts, to post to RenRen under their identity, to publish game and app activities. The permission screen does not contain any link to the relevant privacy policy. Neither does RenRen notify users in cases when a third party has no privacy policy at all. Hence, arguably RenRen does not provide the user with appropriate information and appropriate tools to make an adequately informed decision. Furthermore, I could not find any guidance provided by RenRen to teach and empower users how to control personal information about friends and contacts which might be shared with a third party.

Findings: it appears RenRen does not take sufficient responsibility for due diligence towards the information and empowerment of its users' (and their contacts') privacy with respect to third-party applications.

Retention of data Our focus on this issue is on data retention by RenRen after an account is deleted.

In RenRen, a user can choose to delete his account by filling the suitable form in the account settings page. Nevertheless, after finishing this process, the deleted account remains in RenRen. In fact, it does not permanently delete an account, which instead remains in RenRen's data collections. The deletion service that the SNS offers is restricted to de-activating the account.

Findings: Concerning personal data deletion, users cannot remove their accounts and all the personal information related to it. The only choice is to deactivate the account. RenRen keeps users' data even when it is requested by users to remove these data.

Rights of the users Here I discuss three of these: the right to access, to rectify and to object.

Right to access: A RenRen user can – as long as he has not de-activated his account – get access to information via his activity log, profile and other accessible data collections such as profile information, wall posts, photos, videos, networks, groups, friends, subscriptions, Apps, "likes", newsfeed settings, comments on wall-posts, photos, videos, inbox messages, notes, wall-posts on other users' profiles and public pages, comments on other users' profile, tags, status updates and friends requests.

Right to rectify The right to rectify means users can seek to correct any of the above information where they deem necessary.

Right to object Users cannot object to the processing of data relating to them, even on compelling legitimate grounds relating to their particular situation. Such objections can be particularly important when RenRen incorrectly relates users to a profile, sells the profile data for marketing purposes and allows the results to be targeted back to the user.

Findings: RenRen has made some effort to ensure its users' rights to access, rectify and objection. However, these users' rights have severe limitations concerning RenRen's profiling and other forms of processing and aggregating personal data.

Children and minors Minors are emphatically present in the European legal system concerned with data protection issues. The Working Party sets a multi-pronged strategy to address the protection of minors' data in the SNS context. Even though RenRen's services are utilized by minors, it does not provide any particular protection for them.

Findings: RenRen has no dedicated policies or services that help protect minors that are RenRen users.

Here I assess RenRen's data protection performance by a possible EU state. In the paragraphs above I discussed RenRen as if operational in Europe, complete with its privacy practices as currently operational in China. I used EU data protection principles as formulated by the Working Party as indicators and I presented a summary in the Table 5.1. The first finding is:

> Current Chinese SNS data protection is below par when looked at through the lens of EU data protection principles. RenRen, as it currently operates in China, does not comply with 61% of the European data protection standards as embedded in my indicators. This means that more than half of the elements that make up the principles are complied by RenRen.

Requirements	
Principle	Measure
1. Adequate security measures	Personal data collections are adequately protected against outsider interference.
2. Default privacy settings	**Users are able to restrict access to their profile; users are able to restrict being searched by external engines.**
3. Information to be provided by SNS	On data use for direct marketing purposes. On possible sharing of data with third parties. **On profiles: their creation and chief data sources.** On the use of sensitive data. **Warnings to users about the privacy risks to themselves and to others when they upload information on the SNS.** Advice to get other individual's consent if they wish to upload pictures or information about other individuals.
4. Sensitive Data	**On sensitive data not being processed without the data subjects' explicit consent.**
5. Processing data of non-members	On the fulfillment of criteria for exemption when non-members' data are processed.
6. Third party access should be layered	Providing for layered access to third party developers so they can opt for a limited mode of access, sufficient to perform the task. Providing for a level of granularity that lets the user choose an access level for a third party that is only just sufficient to perform a certain task.
7. Legal grounds for direct marketing	**Direct marketing respecting SNS users' privacy.**
8. Retention of data	No data retention after deletion of account by user.
9. Rights of users	**Right to access. Right to rectify.** Right to object.
10. Children and minors	Special attention for children and minors.

Table 5.2: RenRen EU-law compliant? (The complied principles are highlighted in bold font.)

The case of Facebook

To analyze this I take Facebook Ireland as a case. Fortunately, the Irish Data Protection Commissioner has already published its Report of Audit on Facebook Ireland Ltd on December 21, 2011. The overall conclusion of the audit seems positive. I extract it from page 4 (FB-I refers to Facebook Ireland Ltd) and adopt it as the second finding:

> FB-I provides a service that is free to the user. Its business model is based on charging advertisers to deliver advertisements, which are targeted on the specific interests disclosed by users. The user acknowledges this basic "deal" when s/he signs up to FB-I and agrees to the Statement of Rights and Responsibilities and the related Data Use Policy. ((Irish Data Protection Commission, 2011))
>
> A key focus of the audit was the extent to which the "deal" could reasonably be described as meeting the requirements of fair collection and processing under the Data Protection Acts. While acknowledging that this is a matter of judgment, ultimately by Irish and European Courts, the general conclusion was that targeting advertisements based on interests disclosed by users in the "profile" Information they provide on FB was legitimate. I also concluded that, by extension, information positively provided by users through "Like" buttons etc could legitimately be used as part of the basic "deal" entered into between the user and FB-I. The legitimacy of such use is, in all cases, predicated on users being made fully aware, through transparent notices, that their personal data would be used in this manner to target advertisements to them. And any further use of personal data should only be possible on the basis of clear user consent ((Irish Data Protection Commission, 2011)).

The conclusion of the Irish Data Protection Commissioner concerns Facebook's compliance with EU data protection laws.

Preliminary evaluation: Facebook vs. RenRen

After the analysis of the variables, I identify the three main aspects RenRen could pay more attention to. From their formulation, it becomes clear that the data protection level of the FB-I service would also benefit from such attention:

- The level of transparency that RenRen/FB currently provide to their users is not enough. Although RenRen/FB take transparency seriously, most of the data-protection deficiencies measured are still related to matters of transparency.
- The means and levels of meaningful support provided by RenRen/FB to their users and to third-party service providers, for managing balanced personal data access arrangements, are not enough, especially where users are linked to anonymous user profiles for commercial processing.
- The means and levels of meaningful support provided by RenRen/FB to allow their users to end their accounts of RenRen/FB and to concurrently withdraw their personal data form RenRen's/FB's data collections are not enough.

To European data authorities, their governance on personal data is not flawless. If, instead of substantive law, the Working Party's principles and measures would have been used by the Irish Data Protection Commissioner to assess Facebook's data protection practices, things may have been less ideal for Facebook's data protection performance. In fact, the Commissioner's audit did pay some attention to the Working Party's principles and measures, which did lead to a multitude of recommendations to FB-I to improve its service, yet its final conclusion on legitimacy was not affected. According to Finding 2, a problem merges from the combination of the service being free and the agreement being made between the individual user and FB-I. This can also be an indication for European policymakers how to think about improving the data authority's enforcement capacity, for example by increasing its rules' effects.

China's context: Is the ILT's proposal realistic?

There are strong indications that Chinese legislators could learn from their European counterparts when establishing a new layer of data regulation. However, there is still the question which body would be competent enough to take the role of supervision. Until now, there is no agency in China that has a sufficient number of trained personnel with enough experience to engage in comprehensive supervision of data protection ((Xinbao Zhang, 2007)). This challenge raises the question whether data regulation in China can reproduce the same success as in Europe.

In the past decades, there has only been one unit in China that undertakes limited data authority's tasks, China's Ministry of Industry and Information Technology (Hereinafter MIIT). According to the department's introduction, the MIIT:

> "is the state agency of the People's Republic of China responsible for regulation and development of the postal service, Internet, wireless, broadcasting, communications, production of electronic and information goods, software industry and the promotion of the national knowledge economy".[113]

The MIIT is functionally best compared with the European Telecommunication Authorities. Yet, similar to data authority in Europe, the MIIT combines lawmaking and law enforcement functions that – as has become visible quite recently – also concern data protection issues. As an agent equipped with substantial residual lawmaking powers, the MIIT, just as legislatures, can make and enforce laws for the ICT industry ex ante. It develops policies designed to respond to social needs and to promote data protection in China.

However, the MIIT's small contribution on law enforcement shows its limited competence as a data regulator. Regarding the regulatory infrastructure for data protection, I observed that, although not officially vested by law, the MIIT has the role of overseeing the market participants over data protection issues. Compared with other

[113] Found at: http://www.gov.cn/english//2005-10/02/content_74176.htm "The major responsibilities of MIIT," last access 18-09-2013.

agencies that oversee industrial activities (for example, the Banking Regulatory Committee monitoring the National Credit Reporting Database), the MIIT is the key agent for data protection supervision. However, the scope (restricted to players in the ICT industry) and the repertoire of sanctions it can choose form (refusal or withdrawal of a licensing certificate required for doing business, imposing fines) limit the powers of the MIIT. Regulatory tools enforced by the MIIT may take several forms, ranging from informal verbal warnings to a formal ruling (e.g. fines) and refusal or withdrawal of the licensing certificate required for conducting ICT-related business. However, there is hardly any evidence yet that the MIIT monitors market participants effectively by ensuring rule enforcement. Until now, I have not found evidence of any case that the MIIT exercised its regulatory tools on data protection. Compared with what I illustrated in Chapter 2, in the case of China's Credit Reporting Database, I did not find any analogous roles by the MIIT on data protection: before the database was created, the MIIT did not provide any consultation about data protection issues, and after the database was setup, it was criticized by the media on its data protection practice, and the MIIT did not act on the criticism. Even in the case of RenRen's data leakage scandal, the MIIT limited itself in simply acknowledging the case, without indication of pursuing it further.[114] Thus, the MIIT does not seem to be a competent regulator whose capabilities of understanding data protection's meanings, and application in specific cases, are largely tested.

Even if the Directive 95/46/EC were imported into China, it would start from the very beginning to establish the data protection system For instance, the scope of informational privacy needs to be identified, considering it cannot be discerned from statutory law alone. Even in Europe, the scope of art. 8, which is the foundation of the right to personal data, took several years to be finalized.[115] Due to language, cultural and political differences, the European case law that may help interpret the imported Directive is not easily transferable. Chinese legislators may need a long time in order to establish a data regulatory system, which can lead to respect for the right to privacy. Only after a substantial body of domestic cases has been well developed, will data users, as well as law enforcers, know the reach and limits of the new law. Before that, data regulators need a more complex set of skills given that they must virtually start from scratch.

[114]The information is got from Sohu news of 2011-12-28 under the title "MIIT: strongly condemned stealing personal data"
http://it.sohu.com/20111228/n330575855.shtml

[115]Chapter 1

The fact that data regulation matters is only the starting point. The questions remain whether the Incomplete Law Theory's proposal is realistic and if Chinese legislators should expect the data protection issues to be addressed via introducing regulators. It would be wise to accept the in-feasibility of data regulators to address a comprehensive array of problems. Enacting a law is only the very first step in establishing an effective system. Governing a dynamic industry (as revealed in Chapter 4) is a much more difficult and complex task that calls for enforcing adherence to a set of rules and regulations.

Chapter conclusion

In this Chapter, I analyzed the strength and weakness of data regulation in Europe, using Facebook and RenRen as two cases. It is clear from the discussion that RenRen's current practices are neither in compliance with European Data Protection principles, nor with EU data protection laws. Consequently, if RenRen would open its EU headquarters in any member state in Europe, the firm may receive multiple complaints about its data protection practices. Given the fact that China's data protection performance is not as developed as the European one, it is not a surprise that my finding corroborate this prediction.

Regarding FB-I, I conclude that, even though its current practices seem to comply with EU data protection law, they do not fully comply with European Data Protection principles (based on the recommendations by the Irish Commissioner in his Report). This leads to the straightforward conclusion that what is acceptable to EU privacy laws needs not be acceptable through the lens of the Working Party's principles. On the one hand, this means the level of data subjects' protection increases substantially to a higher level, primarily due to data regulators' performance. On the other hand, European policymakers may consider giving more importance to data authorities' principles.

This is a further illustration of the proposition that, in order to address the effectiveness problem of data protection law, it may be

advisable to introduce regulators. However, merely pointing to the element of a strong data regulator does not ensure the desired outcome, at least at the outset of the data protection institution's development. Data protection law in China is less complete than in Europe, as most such laws have only been recently enacted, and law enforcement agencies lack the experience to apply and interpret them to a variety of newly emerging cases. This is particularly the case in the MITT's performance. Thus, Chinese legislators face a predicament: they really need to develop a European type of data protection system, and yet they lack the instruments to do so.

Therefore, what can be done to mitigate the weaknesses of such an institution, short of waiting, until it becomes an experienced authority (since governing data protection issues are pressed upon China's policymakers)? This requires a serious top-down analysis to explore. After the Conclusion Chapter, I will provide suggestions in order to allow China's policymakers better understand the subject matter of data protection. Such an endeavor may inform and aid them in developing practical and effective policies.

Chapter 6

Conclusion of Part I

Summary

Following the Introduction, in Chapter 2, using documentary evidence and interview results, I compared the positive laws over data protection of the European general system with the Chinese credit reporting system, and provided a positivist interpretation-based assessment of the data protection levels in the two regions. In doing so I employed a set of measure sticks that I derived from 2013 version of the OECD guidelines. Differences between the two regions on data protection issues are marked. Generally, the comparison reveals that European data protection laws cover the principles of informational privacy as embedded in OECD 2013 far more complete than Chinese data-protection laws do (when available at all). Considering the Chinese credit reporting database CRC in Chapter 2 thus provides evidence that this database, were it operational in Europe, would be in danger of being deemed illegal, since the CRC's operations violate three types of privacy guarantees under European data protection law.

The first violation type concerns *the data subject's rights*. The two rights in the OECD 2013 are recognized by both regions. Yet, the right to object, which can be considered a species of the right to challenge is a peculiarity of European data protection law and is not observed in Chinese laws. The second type of violations concerns *the data controllers' obligations*. The Directive recognizes all OECD principles on the data controllers' obligations, while Chinese Credit Reporting Laws miss the collection limitation principle, the use lim-

itation principle, the openness principle and the accountability principles. These omissions are serious indeed. The third violation type concerns the *procedural issues*. Implementation principles are largely recognized by European data protection law, except the national strategy, which was only incorporated into the OECD guidelines in 2013. Yet, China misses most of the procedural core issues. Only three principles are found in China's system, including ``reasonable means for the individual to exercise their rights, adequate sanctions and complementary measures." Again, Chinese positive laws on data protection for credit reporting lag seriously behind Directive 95/46/EC when looked at through the lens of OECD 2013. Therefore, under China's legal arrangements such CRC database use by the government might very well be legal. Yet under European law the very same database use would clearly be illegal.

Based on the above comparison, I conclude that if China's policymakers introduce European data protection law, it can upgrade China's legal arrangements, considered from a positivist perspective. Consequently, and assuming the ``all other things being equal" assumption, European data protection law can serve as a point of departure for improving China's legal arrangements. But since we know that all other things are not equal between Europe and China, I think further investigations are needed and may suggest improvements to the plan to transplant, simply and directly, legal texts from Europe to China.

In Chapter 3, I investigated the evolution of privacy and informational privacy in Europe and China as these evolutionary paths have certainly unwound under different conditions. I began the Chapter by showing some considerations on the analogies between languages, cultures and legal systems: like languages, legal systems evolve under the pressures of the cultures they serve and are part of -- consequently, by looking at the developments in their cultural environments, how the differences between legal systems may be better understood -- both in the book (the positivist perspective) and in action (the realist perspective). Based on the analysis I conclude that differences in culture helped shape differences in data protection law. As the discussion of European data protection law in the Chapter demonstrates, it has emerged from the (functional) roots of European privacy conceptions that came to flourish under the pressures of continuities in the

environment. These functional roots are there first, and are soon followed by the emergence of the first legal forms of privacy protection by law. Privacy functions and laws kept on co-evolving in Europe and culminated after World War II not only in elaborate functional (and thus instrumental) legislation, but also in the rather Kantian idea of privacy as an intrinsically individualist human value (as expressed in art. 12 of the UDHR). In China, the current legal arrangement over data protection issues grows directly out of China's collectivist culture, which only rewards the instrumental-goods aspect of privacy. The findings in this Chapter suggest that China's policymakers should realize that European data protection law is neither being transplanted from, nor to jurisdictions with culturally blank or neutral slates. Instead, both Europe and China has pre-existing sets of data protection laws and privacy-related cultural norms. The cultures that embed privacy practices are complicated and have far-reaching implications on the ways that data protection laws are and will be understood, and on how they will be received, upheld and enforced. Therefore, I suggest that China will adopt a cautious approach to the realization of the legal transplantation plan.

At the end of Chapter 3, I have established differences between two positive law arrangements and between the two cultures involved. There is a lot that at first sight seems a valid candidate for importation from the EU to China. Yet, there are risks. For instance, both technical innovation and the uptake of social media services are highly dynamic and tend to make adequate legislation difficult. So in order to make an informed choice about what to import and what not to import, it is useful to analyze how the legal systems under discussion support (or undermine) the recipient legal system's resilience in a changing environment.

This very issue is my motivation for Chapter 4's excursion into Incomplete Law theory. In order to impose an interpretation on the phenomenon in question, I deployed the theory of Incomplete Law, created by Xu and Pistor, for the analysis. It showed that European data protection laws, as represented by Directive 95/46/EC, are incomplete. The reasons can be categorized in three. First, the generality of the Directive makes it difficult to provide rules that are specific enough; second, technology, that strongly influences data protection law's subject matter, changes at high speed and therefore renders the

Directive more incomplete as it lags behind; and finally, lawmakers are unable to foresee all future contingencies also those contingencies that emerge through mass adoption of emerging services. Particularly, technology's changes strongly challenge even the short-term ``fit'' of the Directive. The Directive 95/46/EC was designed to regulate the data processing technologies a couple of decades ago and thus focused on ``old'' problems while digital technologies have experienced radical revolutions. New advanced digital technologies were being introduced into public communications networks and in the community. Access to digital mobile networks has become available and affordable for the public at large. These digital networks have huge opportunities for processing personal data. All these changes, thus, required frequent adaptations of the law for it to remain effective. This led to problems with the law's focus and mechanisms to remain connected to reality.

How does Europe arrange to face the resulting incompleteness? European policymakers created a new role, the data protection authority who assumes residual LMLEP (law making and law enforcing powers), in order to make interventions possible for mitigating the problems of incompleteness. In Chapter 4, I focused on the Article 29. Working Party and the national data-protection authorities that take significant roles in regulating and law enforcement for reducing incompleteness. The investigation confirmed that the emergence of data authorities responded to the problem of under-enforcement caused by highly incomplete law. Data authorities are more flexible than legislative agencies on adapting the law to a changed technical environment (although the scope of their lawmaking rights is limited), since their swift reaction time allows them to better keep up with the fast pace of technology. And Data authorities are more proactively than courts, since they can initiate actions to enforce data protection law in situations where courts, by design, have to wait for a file to be suit.

Consequently, the findings in Chapter 4 reject the assumption (which China's policymakers nurse) that European data protection law is complete, and that the transplantation scheme can be confined to material, positive data protection laws. I show that, beyond their expectations, issues of dynamics in technology and in mass use of social media are not trivial and require measures that safeguard the availability of a highly informed and highly responsive authority that has sufficient residual LMLEP to guard the law's incompleteness will not become intolerable. I conclude that legal transplantation as envisaged will not ensue effective consequences unless a competent regulatory authority is in place.

As a follow up to this conclusion, I analyzed in Chapter 5 what gaps between the law in the books and the law in action the data authorities have to face when they regulate American or Chinese Facebook (RenRen). It is clear from the discussion that RenRen's current practices are neither in compliance with European Data Protection principles, nor with EU data protection laws. Consequently, if RenRen would open its EU headquarters in any member state in Europe, the firm may receive multiple complaints about its data protection practices. Regarding FB-I, I conclude that, even though its current practices seem to comply with EU data protection law, they do neither fully comply with European Data Protection principles (as recommended by the Irish Commissioner in his Report). This leads to the insight that what is acceptable to EU privacy laws needs not be acceptable through the lens of the Working Party's principles. On the one hand, this means that the level of data subjects' protection may increase substantially to a higher level, dependent of the data regulators' performance. On the other hand, the same finding shows that it is difficult to enforce the law rigorously in order to influence the data protection behavior of a world leading SNS player like Facebook. In other words, the efficacy of the law in action is complex, and difficult to anticipate by looking at the law and its enforcing officials in isolation.

In China, the tension between the efficacy of law in action and the optimal standard of legal design is mounting, at least at the outset of the data protection transplantation plan. The incompleteness of data protection law in China is more severe than in Europe, as many of such laws simply are not there at all and most of such laws that exist have been enacted recently. The incompleteness is also more severe in China than in Europe, because law enforcement agencies simply lack the experience that accompanies the adjudication in a substantial number and variety of cases. This is particularly relevant to the MIIT's performance. Thus, Chinese legislators face a predicament: they really need to develop a European type of data protection system,

and yet they lack the instruments to do so.

Considering China's transplantation plan

Now, I can answer my main research question: "Is China's transplantation plan advisable?" My approach concludes that it is not feasible to solely transplant EU data protection law (as China's transplantation proposal suggests), unless an equivalent to the EU data authorities is included. Chinese Data protection law is less strong than EU privacy law (chapter 2). However, cultural differences (chapter 3) and inherent incompleteness of the EU law (chapter 4), coupled with the fact that institutional arrangements in the EU that reduce incompleteness will not work in China (chapter 5) make me conclude that of the effectiveness of the an imported European data protection law cannot be expected too much.

Applying what I have learned from research project as reported in the previous chapters, I translate my findings into a set of recommendations that those involved in designing and adapting legal arrangements over data protection issues for China would need to consider.

1. It is necessary for China to develop a more general data protection law, that can catch all CRC-like and RenRen-like programs that involve large-scale personal data collection and processing. Drawing on European experiences, China's legal arrangement over data protection would only need be modestly changed by adding the right to object, and the principles of collection, use limitation, openness and accountability, to the basis of the Measure 2005 (and by making its scope more universal).

2. China's policymakers should recognize that imported data protection law needs to take some time to be accepted since the society may need the time to absorb the cultural assumptions that the imported law is based on and that China does not currently share. During the time, policymakers should try to educate the public about data protection, as well as about the privacy values that the imported law is based on. Education efforts should continue in an effort to increase both data subjects and companies' data protection awarenesses. Yet before doing all this it should be established that the cultural changes needed are acceptable to the Chinese community in reality.

3. It is better to avoid transplantation of the European data protection system as a whole, when no thought is spent on the problems that the individual components of the European law may induce. To China, whose data protection conception is relatively simple, the European data protection law might prove to be too complicated, too confusing and contextually too European.

4. Thus, it may be much better to borrow no more than a fraction of the European data protection law rules, rather than importing the whole system. What should the key selection criteria be? The new law must fit the needs of Chinese society, including its cultural components. It might be wise, for instance, to think twice before trying to import the intrinsic-good value from the European data protection law system into the Chinese law system, where it might easily turn into a confusing anomaly for the law in action.

5. Data Authority Matters. In Chapter 4, the assumption (which is maintained by China's policymakers) is confuted that the Directive 95/46/EC is complete. Given that the targeted law is incomplete, China's legal importation plan, when the focus is on material law only, carries large risks. The Data authority, the institution to supervise personal data use, will not be well supported, then. And, as I showed in Chapter 4, a well supported data authority will make the difference between success and failure of data protection regulation in action.

6. In Europe, the existence of a data authority largely compensates the defects of incomplete data protection law. Yet, the findings in the Facebook audit revealed that the effectiveness of the data authority's enforcement is inhibited, probably due to the limited powers granted to it. Thus, I propose China's policymakers to consider giving the data regulator some extra (compared with Europe) authority in order to monitor and constrain all personal data users, and especially the giant users such as Facebook, RenRen and the CRC.

7. Be prepared that during the early period of establishing a data protection system, the regime may not work as effective as hoped and perhaps expected. While the practical significance of an independent data protection authority perhaps can be exaggerated, neither is it obviously trivial. It all may depend on whether several important other differences between the two jurisdictions (for instance of a cultural nature, or simply of having had the opportunity to gather experience and expertise) would allow or even support such an institution to thrive eventually.

Challenges ahead

The research in the previous Chapters demonstrates some interesting phenomena relating to data protection law's subject matter.

In Chapter 4, I witnessed the complexities of enforcing data protection law to whoever processes personal data, since whoever processes personal data tends to be connected. Whoever processes personal data is connected and thus forms a network. There are lightly connected nodes in this network like you and me, but there are also huge, heavy connected nodes, hubs if you like, like Facebook, RenRen, the CRC database, Google and Baidu. All are connected together, through data flow. The nodes in the network cannot be isolated from it. Thus it may prove very difficult, perhaps even next to impossible, to govern the behavior of the system/the network around Facebook as a whole by regulating Facebook and all other nodes individually, *as if* autonomous and in isolation.

Furthermore, a finding in Chapter 3 showed that data protection law in Europe and China are built on historically existing social constructs. And those historical arrangements constrained the processes of creating the contents of data protection laws. The resulting data protection law systems, therefore, are likely to demonstrate path dependence. Path dependence is a well known, yet difficult to capture phenomenon, mainly because it flies in the face of what is generally considered to be rational. It is also a phenomenon that is closely related to decision making under incomplete information in complex situations.

I also found, that data protection law's subject matter as a whole is adaptive to social and technological changes. In Chapter 3, the focus/main concerns of data protection law in Europe are co-evolving with the social background: before 9/11, the main focus of Directive 95/46/EC was directed to ``data collection and personal data processing.'' After 9/11, the main focus of subsequent data protection laws was directed to ``data retention'' and to support Government's information positions. In Chapter 4, I also found that European data protection law has to face the changes in technology. The law has to depend on the data authority as an agent, to improve its ``fit'' with technological dynamics.

The phenomena that I encountered in Chapters 3-5 and that characterize the subject matter for personal-data protection can be summarized with six characteristics: networked/connected, leading to emergent interdependencies, now and then showing path dependent behavior, dynamic, complex and adaptive.

My research has raised the question whether data protection law, as seen from the two mainstream legal-theory perspectives, is up to the challenges posed to it by its subject matter. The management of such subject matter presents fundamental challenges. So I cannot help but be concerned: what course does data protection law need to follow?

Looking around, not only China's policymakers but also European policymakers are often trying to regulate connected, dynamic, complex and adaptive subject matter. And data protection law is not the only area of the law that is chronically the subject of legislators that keep struggling and adapting -- often in vain. Looking through a purely legal lens at the data-protection subject matter may not be sufficiently effective -- like looking through such a lens may neither be sufficiently effective when considering the regulation/domestication of unstable situations, e.g., with welfare distributions, with environmental sustainability, with ethnic, religious and political fundamentalists, with legal cultures and with scientific paradigmatic. Somehow, such situations call for the law to intervene. Yet nowhere is hope that the law will be able to go it alone when the subject matter is complex and adaptive, and I am afraid that aiming for the transplantation of formal laws implies the assumption that the law will be able to go it alone. I, on the other hand, assume that looking at webs of situations wherein the law is only a part may help us find pathways out of those clutches that lock us in, in our traditional perspectives. In

this connection, I decided to investigate the possible fertility of one additional, yet radically non-traditional perspective.

So in the Second Part of my research project I explore what additional opportunities can be discerned when adopting the perspective offered by complexity theory, and when considering the subject matter of data-protection regulation to be a complex adaptive system (hereinafter CAS).

Again: the phenomena that I encountered in Chapters 3-5 and that characterize the subject matter for personal-data protection can be summarized with six characteristics: networked/connected leading to emergent interdependencies, now and then showing path dependent behavior, dynamic, complex and adaptive.

> *These characteristics happen also to be defining characteristics of what has recently been established as complex adaptive systems - the subject matter of complexity theory.*

In the Second Part, I will show that there are good reasons to believe that data protection law is trying to tame a CAS. Hence, it is logical to approach its subject matter through the lens of complexity theory.

In the following chapter, I first investigate whether complexity theory can help improve our understanding of the data protection situations that keep us locked in, before considering legal relief. I think this shift of focus does help, and in due course I show how and why. The Second Part is the beginning of an effort to better understand data protection law's subject matter, and to subsequently identify, in a well-founded manner, some issues for further research.

Part II

Can Complexity Theory be of any use?

Chapter 7

A heuristic display

Social ecologies react to the respective environmental niches they live in. Over time they prove either resilient against or sensitive to legal attention and other interventions and vice versa. That explains why different legal systems have emerged. We faced an example of the influences of different niches when discussing Chinese-EU-privacy/data-protection-law importation plans in Part I. At the end of that Part I accepted that even the combination of legal positivist and realist perspectives does not allow to create a picture that is complete enough to rationally advise the Chinese legislator on the EU data-protection law transplantation plan. To me it seems that contributions form multiple disciplines are needed, as proves standard procedure when complexity theory is invited in. It is emphatically not my aim to degrade the efforts that have been made by positivists and realists to face the problems mentioned in the realities of their occurrence.

In this Chapter I do not consider any individual law, treaty or institution to be my main subject matter. Instead, I look at the global cluster of personal-data users, as a whole. For better understanding that global, multi-level and multi-niche cluster of networked personal-data devouring and producing individuals and institutions, I need a systematic perspective. I consider it to be at the core of legal scientific ethos to strive for improved understanding of what legal rules and institutions will accomplish when decisions have to be made concerning unforeseen contingencies (by the legislator) and under incomplete or false information

Yet I must concede that neither the positivist perspective nor the

realist perspective is opening up to help us out, here. And nowhere is a real hope that the law will be able to go it alone when its subject matter is complex and adaptive. So my aim is to look for knowledge that will have added value.

Improved understanding of such situations has become focal to several multidisciplinary academic networks.[116] The scientific perspective that emerged in these institutions is often referred to as complexity theory, or simply `complexity,' and participants often work on problems that, for a solution, not only seem to require a diverse bunch of science, but also seem to require well founded and coordinated guidance by the law (like economic ``bubbles" or ``global warming" -- in fact like most of the Big International Problems of our times.

Because complexity theory is itself rather new, incomplete and spanning a diversity of disciplines, my efforts to understand its uses for legal scholarship and informed legislation are by necessity explorative and incomplete.

In the Chapter I first explain why I address the possibilities of complexity theory (Section 1) and subsequently sketch the networked character of the community that is addressed by personal-data protection laws (Section 2) and name it the PDC. In order to be able to decide on the applicability of complexity theory, I first list a set of essentials that define its subject matter, complex adaptive systems (CASs, Section 3). Then I analyze the PDC, and identify it as a CAS (Section 4), my most important result in this Chapter. In Section 5 I provide some considerations for further research into the exploration of combining complexity theory and legal scholarship, by mentioning some of the models/results/approaches that were developed by complexity theorists. Where I can relate them to legislative issues.

Why complexity theory?

First, I witnessed the complexities of enforcing data protection law to whoever uses (and thus: processes) personal data, since whoever

[116] As for instance initiated at the Santa Fe Institute (SFI), the Edge Foundation, the Michigan University Institute for Complex Sciences, The Institute for New Economic Thinking (INET) and the Nanying University Institute for Complexity. To us it appears a missed opportunity that legal scholars do not (or hardly) seem to belong and/or take part.

processes personal data tends to be connected. Whoever processes personal data is connected and thus co-creates (and is a node in) a network. There are lightly connected nodes in this network like you and me, but there are also huge, heavy connected nodes, hubs if you like, like Facebook, RenRen, the CRC database, Google and Baidu. All are connected together, through data flow. The behavior of the network as a whole cannot be predicted by studying the constituent nodes in isolation. Thus it may prove very difficult, perhaps even next to impossible, to govern the behavior of the system/the network around Facebook as a whole by regulating Facebook and all other nodes individually, *as if* autonomous, *as if* in isolation and *as if* equal for the law. Yet this seems to be our fate, for the law addresses autonomous and responsible individuals.[117]

Furthermore, I witnessed that data protection laws in Europe and in China are built on historically emerging, yet diverse, social constructs. And those historical arrangements constrained the processes of creating the contents of data protection laws. The resulting data protection law systems, therefore, are not only different (having followed different paths), but are also likely to be subject to the forces of path dependence. Path dependence is a well-known, yet difficult to capture phenomenon, mainly because it flies in the face of what is generally considered to be rational. It is also a phenomenon that is closely related to decision making under incomplete information in complex situations.

I also witnessed that data protection law's subject matter as a whole is adaptive to social and technological changes. The focus/main concerns of data protection law in Europe are co-evolving with the social background: before 9/11, for instance, the main focus of Directive 95/46/EC was directed to ``data collection and personal data processing." After 9/11, the main focus of subsequent data protection laws was directed to ``data retention" and to support and improve the Government's information positions (Directive 2006/24/EC). I also witnessed in this context that European data protection law continually needs to face changes in technology. The law has to depend on the data authority as an agent, to improve its ``fit" with technological

[117] Or their aggregate equivalent: legal persons (or institutions). And, as we shall see, the network discussed is emphatically not a legal person.

dynamics.

The research has raised the question whether data protection law is up to the challenges posed to it by its subject matter. The phenomena that I witnessed in my research, and that characterize the subject matter for personal-data protection can be summarized with six properties:

(i) networked/connected/dependent/diverse/autonomous individuals,

(ii) often aggregating in institutions, that now and then show

(iii) path dependent,

(iv) dynamic,

(v) complex and

(vi) adaptive behavior.

Looking around, not only China's policymakers but also European policymakers are trying to regulate connected, aggregate, path dependent, dynamic, complex and adaptive subject matters (or subjects) like for personal data protection and legitimate personal data use.

> *These characteristics happen also to be important properties of what has recently been established as complex adaptive systems - the subject matter of complexity theory.*[118]

And data protection law is not the only area of the law that is perpetually the subject of legislators that keep struggling to regulate complex and dynamic subject matter by adapting the laws. Looking through a purely legal lens at the data-protection subject matter may not be sufficiently effective -- like looking through such a lens may neither be sufficiently effective when considering the regulation/domestication of sometimes unstable complex situations.[119] Often, such situations nevertheless call for the law to intervene.

I am afraid that aiming for the transplantation of formal laws suggests that the law will be able to go it alone. I disagree and submit that looking at webs of situations wherein the law is only a functional

[118] See for instance: Miller & Page (2009), Mitchell (2009), Holland (2012)

[119] *E.g.*, as with welfare distributions, with environmental sustainability, with ethnic, religious, political and market fundamentalists, with legal cultures and with scientific paradigm.

part may help us find pathways to improve our understanding of what the law may in fact be capable of. Thus, I decided to investigate the possible fertility of the only additional, radically non-traditional and radically multi-disciplinary perspective that I think may fit the bill: Complex Adaptive System theory, or CAS theory.[120]

According to Mitchell (2009):13, a CAS is a system in which large networks of diverse components with simple rules of operation operate, a system without central control, a system that gives rise to complex collective behavior, a system that is capable of sophisticated information processing, a system that is capable of adaptation via learning or evolution. As the term suggests, CAS-theory is the collection of conceptual models built for understanding such CASs. The theory suggests that CASs, regardless of their particular subject matters, universally exhibit certain characteristics, of which the most critical ones include self-organization or emergence (Tussey (2005):148).

I believe that CAS theory can open a few windows for legal scholarship, by offering an additional perspective that allows to combine forces with the natural sciences, the social sciences and the humanities. Although CAS-theory gained more attention from the natural sciences, and from mathematics and computer science (see, *e.g.*, Mitchell (2009), Newman (2011) and Holland (2012)), it has also become attractive to and has been applied in the social sciences (see, *e.g.*, Anderson (1999), Beinhocker (2006) and Pagel (2012)).

In the legal world, there are several efforts of employing CAS theory for looking at the law/legal systems themselves and sometimes also at their subject matter.[121] Mostly, these efforts offer completely

[120] The Santa Fe Institute has worked since its founding in 1984 been working on CAS theory. On its website (http://www.santafe.edu/about/faq/) it explains what complex system research is about: "Complex systems research attempts to uncover and understand the deep commonalities that link artificial, human, and natural systems. By their very nature, these problems transcend any particular field; for example, if we understand the fundamental principles of organization, we will gain insight into the functioning of such systems as cells in biology, markets and firms in economics, and phase transitions in physics and human social systems. This research relies on theories and tools from across the sciences."

[121] The CAS-theory approach in law is far from mainstream, yet these examples are not eccentric exceptions either. As exemplified by, e.g., Jones

fresh information to legislators and researchers.

For example, Tussey has done a survey of the music industry from the perspective of complexity science, combined with organizational theory.[122] In her paper, Tussey issues a compelling invitation to look at (and understand) the music industry as a CAS, in which ``*legal, political, economic, socio-cultural, and technological subsystems converge, interact, and coevolve.*'' [123]

Another example is provided by Ruhl, who introduced CAS-theory into the legal field. He wrote several papers about the application of CAS theory to the legal system.[124] In ``*Thinking of environmental law as a complex adaptive system: how to clean up the environment by making a mess of environmental law*,'' Ruhl adopted CAS-theory to analyze environmental law and all the issues around and inside it. Ruhl found that, not only environmental law, but also the subject matters of environmental law such as ecosystems, technology, economies and land use arrangements are all CASs and share CAS-characteristics. Based on these findings, Ruhl criticized environmental law's methods as reductionist, linear and predictivist, ignoring the underlying CAS characteristics. Ruhl thereby suggested that to manage the impact of human society in the inherently chaotic, adaptive environment, the environmental-law system itself must adopt and possess dynamic qualities.[125]

The works by Tussey and by Ruhl show us that the ``marriage'' between CAS-theory and legal research are possible and can bear fruit. Yet, the possibilities of what CAS theory can offer to legal scholarship is by no means exhausted yet. What CAS theory can offer to legal scholarship is immense, I submit, yet it is hardly on the discipline's agenda.

(2008) (considering the implications of networks, complex systems, and nonlinear dynamics to the future of the law), Holz (2007) (applying CAS theory to judicial decision making), Katz *et al.* (2008) (identifying the conditions under which network effects are present in the development of the common law), Post & Eisen (2000) (on the fractal nature of law), Bloche (2008) (discussing USA health care law with its resulting implementation as an emerging CAS), Tribe (1989) (shedding light on the character and structure of constitutional analysis as a process), Axelrod (1986) (investigating the emergence and stability of behavioral norms in the context of a game played by people of limited rationality), Picker (1997) (uncovering the boundaries of legal rules and defining their proper limits have traditionally vexed students of the law).

[122] Tussey (2005).

[123] According to her analysis, digitization and global networking can be considered as disruptive perturbations of the music industry as a system, that thus shows a typical CAS characteristic. The main challenge that the music industry is confronted with is how to respond evolutionarily to the new environment. Tussey's prediction, based on CAS-theory, is not as pessimistic as many others. Instead, the music industry which is a polyfocal, multi-level, evolving, dynamic system, is adapting successfully to the digital environment and there is hardly any need to worry about its survival, she observes. Tussey predicts that *"new models of information creation and dissemination will naturally emerge over time from the millions of individual interactions among users and providers of content and digital technologies, for instance the emergence of the P2P file sharing is the outcome the interactions. The P2P technology has fed back into the music system and has produced emergent responses in the form of new online business models*" ((Tussey, 2005): 103-104).

[124] For instance to the co-evolution of law and society and its practical meaning for democracy, administrative law, environmental law, European justice and so on See Ruhl (1996a,b, 2008, 1997); Ruhl & Ruhl (1997); Ruhl (2009, 2005); Ruhl *et al.* (2007).

Data-protection law's subject matter: the PDC

As a starting point, I am going to describe the data protection law's subject matter as a human-created system within which all sorts of data users either cooperate or compete with specific references to personal data.[126] For the connivance of our following analysis, I ``arbitrarily'' tag the system as ``*Personal Data Community*'' (PDC).

For obvious reasons I will focus on data protection law as the control system of the PDC, although I believe that there are other control systems, such as technology, culture, the economy and the environment. For the moment I conceptually separate the law (and the other control systems) from the PDC, and imagine them all as its

[125] See Ruhl (1997).

[126] Systems could occure, either by nature, such as ecosystem(Levin (1998)) or earth(Steffen *et al.* (2006)), or by human design, such as music system(Tussey (2005)), international environmental law systems(Kim & Mackey (2013),Ruhl (1997)). (Tussey (2005))

environment. The reason is that I want to be able to ``theorize'' about the relationship between data protection law and its subject matter, which may easily become too complicated when the latter is regarded to be part of the former.[127]

I take it that the term *community* refers to any social network with shared common values.[128] Community in `personal data community' follows this definition. It provides an analogy that can serve as a tool for understanding data protection law's subject matter as a system: the PDC is the community that is constituted by all connected data users that share an interest in using personal data. The network *is* the system. Thus, by imagining the PDC as a system I pave the way for discussing it as a unit, as a single object.

Below, I draw a figure to help imagine what this object looks like. Herewith, I followed Lessig's lead[129] and represent the PDC/system as a dot. Figure 7.1 shows what the PDC/dot looks like in isolation.

[127]The current orthodoxy in the CAS in Law studies is that law exhibits some key characteristics akin to its subject matter. That is: both the legal system and its subject matter can be considered complex. I think this to be true, yet I also think that the relationships between the two may easily become confusing. In this article, I focus on better understanding complex subject matter and on how it relates to the law (that I imagine – for the analysis, applying the ceteris paribus mechanism – to be static).

[128]According to Wikipedia, Community includes two distinct meanings:

> 1) Community can refer to a usually small, social unit of any size that shares common values. The term can also refer to the national community or international community, and 2) in biology, a community is a group of interacting living organisms sharing a populated environmentWikipedia (2010).

Community in this paper took the first one.

[129]I follow Lessig's representation of an agent that is regulated in a regulatory field as a dot (Lessig (2006)).

Figure 7.1: The PDC-"dot" to be regulated

But the PDC is not as simple as it appears to be in Figure 1. In the initial conceptualization, all data users, both individual and institutional ones, together constitute the PDC. These (sub) units are not visible in the dot. Nevertheless, these sub-units include individuals such as data subjects and individual data users, but also data using organizations such as banks, governments, social groups (e.g. hacker groups), big or small companies (e.g. google, Facebook, twitter, RenRen) and other data-using stakeholders, as long as they are represented by an autonomous and responsible agent, as long as they are nodes in the network and as long as they share an interest in the use of personal data.

The PDC has many sub-systems, for example: European and Chinese (based on both cultural and territorial criteria). These subsystems are PDCs themselves. There are PDCs in the banking industry, PDCs in the Social Networking Services industry, PDCs in Security/anti-terrorism systems and so on. Further, as the social networking PDC shows, autonomous, responsible agents can be personal-data users as well as personal-data subjects.[130] Moreover, PDCs are constituted by units that may concurrently take part in several subsystems. I sketch an example in Figure 7.2 to show the internal structure of the PDC.

Prior to discussing the PDC as a CAS, it is necessary to stress that the PDC, as discussed in this Chapter, is a web of webs (a network of networks, a PDC of PDCs) with personal data users at its nodes,

[130]For instance, in the social networking world:

> "*person A may comment about what person B did in school that day, while person C reads the post but says nothing. Person D may post a photo from dinner about person E which gets a thumbs up from person F. On these facts, there are no distinct "users" or "data subjects"* " (Swire (2012):138).

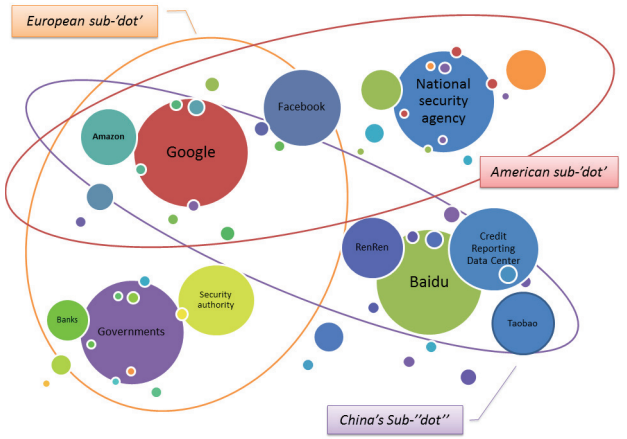

Figure 7.2: Dots (like the PDC) have internal structure

users that are responsible for the instruments employed for storing these data locally, and that are responsible for the local mechanisms that import, process and export such data over its edges or links.

When I assume as a working hypothesis that data protection laws constitute the main control system for the internal and the external behavior of the PDC and its sub-PDCs, I can already now postulate that it will be really important to try and understand how PDCs are formed from sub-PDCs (emergence) and how sub-PDCs are formed by other sub-PDCs (reproduction). And how PDCs influence their sub-PDCs and *vice-versa*.

And what the law has to do with it, and the other non-legal regulatory forces, as in our current story this has not yet been touched upon. But before doing that, I discuss complex adaptive systems as such.

A framework of CAS essentials

Before explaining the PDC from a CAS perspective in greater detail, I turn to a brief overview about CAS essentials.

CAS theory's emergence Philip Anderson published his extensively cited *More is Different* in 1972.[131] It is widely considered to have provided a cradle for CAS theory. Although CAS theory began to seriously surface in the 1980s, it took another decade for the activities in the Santa Fe Institute to begin and crystallize into a niche theory and -research approach. The Santa Fe Institute, which is the dominant contributor to the field, was founded in 1984 by a group of physicists (including Anderson and Gell-Man), economists, and others interested in studying complex systems in which the agents of those systems change.[132] In 1994, John Holland gave a famous presentation titled 'Hidden Order' and subsequently published a book under that name (Holland (1995)). In the book, he offered a comprehensive picture of CAS theory as it was at the time. Thereafter, CAS theory began to stand out as a new and productive paradigm for multidisciplinary work. Nevertheless, its main contributions took many years to be digested and received by researchers in many fields. In the past decades, multiple subject matters in the universe have been re-observed from the lens of CAS theory. Its observable facts are across the whole spectrum of the universe, including systems of sub-atomic particles, protein systems, eukariotic cells (and systems of such cells), *weather systems*

> Chan explained that weather is a complex system which is fundamentally unpredictable. Very small changes in initial conditions in the weather system can lead to unpredictable consequences, even if everything in the system is causally connected in a deterministic way. The current state of the weather is no predictor of what it will be in a couple of days time because tiny disturbances can produce exponentially divergent behavior (SeeChan (2001)),

immune systems

> Grilo thought immune systems, ecological systems as well as many others, are difficult to control or describe

[131] Anderson (1972).

[132] Brownlee *et al.* (2007)

using traditional computational methods. Two main difficulties are ensued when modeling such a system. The first problem arises from nonlinear interactions among system components. The second is issued when system's units can evolve, or change their specification, over time. Systems with these properties are sometimes called Complex Adaptive Systems (See Grilo *et al.* (2002)),

ant colonies

Ant colony is a canonical example of a complex adaptive system. In this system, each individual ant has a decision role. Each one also interacts with the other ants. A lot of that is local interaction. What emerges from their behavior is an ant colony (See, Kay & Schneider (1995)). Also see ``An interview with Michael J. Mauboussin by Tim Sullivan," in the Harvard Business Review, on Embracing Complexity,[133]

social systems,

such as the global macroeconomic networks within a country or group of countries. In "Unit-based computational economics: modeling economies as complex adaptive systems", the paper outlines the main objectives and defining characteristics of the unit-based computational economics methodology which is identified as evolving systems of autonomous interacting units (See Tesfatsion (2003)).

In, *From simplistic to complex systems in economics*, Foster applies CAS theory to economics and tries to evaluate and compare it with standard approaches that are based on constrained optimization. Foster recommends that the prevailing simplistic theories, based in constrained optimization, can better be replaced by 'simple' theories, derived from network representations in which value is created through the establishment of new connections between elements.[134]

[133]See http://hbr.org/2011/09/embracing-complexity.

[134]See Foster (2005).

In another paper, *Why is economics not a complex systems science?* Foster discussed why a complex system perspective can hardly develop in the mainstream of economics (See Foster (2006)).

In *Rethinking the financial network*, Haldane adopts network theory (with other evidence) to explain the emergence of two characteristics in the financial network over the past decade – complexity and homogeneity. And he subsequently offers his diagnosis of the troubles under the economic crisis of the time. Haldane -- who is the Chief Economist of the Bank of England -- bases his diagnosis on CAS theory (See Haldane (2009)),

language

Briscoe suggests in *Language as a complex adaptive system: co-evolution of language and of the language acquisition device* that the reciprocal evolution of language learning procedures and of language creates a coevolutionary dynamic system (See Briscoe (1998)).

In *Language is a complex adaptive system: Position paper*, the authors re-interpreted language to be a CAS as languages have every feature a CAS should have. Their approach reveals commonalities in many areas of language research, including first and second language acquisition, historical linguistics, psycholinguistics, language evolution and computational modeling (See Beckner *et al.* (2009)),

organizations

In *Organizations as complex adaptive systems: Implications of complexity theory for leadership research,* Schneider and colleagues presented leadership in a Complex Adaptive System (CAS) may affect the organization indirectly, through the mediating variables of organizational identity and social movements (See Schneider & Somers (2006)).

In *Health care organizations as complex adaptive system* by Begun, Brenda and Dooley, the authors identi-

> fied a series of key differences between complexity science and established theoretical approaches to studying health organizations. They found that complexity theory can broaden and deepen the scope of inquiry into health care organizations, and that it can expand corresponding methods of research, and that it increases the ability of other theories to generate valid research on complex organizational forms (Begun *et al.* (2003))

and *cyberspace*

> Phister thinks cyberspace has exhibited the traits of a CAS, since networks and information systems that are being constructed today are complicated. Integrating these networks together into a global Internet yields an extremely complicated environment (See: Phister Jr (2010)).
>
> Andrus pointed out that the rapidly changing circumstances in which intelligence communities operate take on lives of their own that are difficult or impossible to anticipate or predict. The only way to meet the continuously unpredictable challenges ahead of us is to match them with changes of our own. We must transform into a community that dynamically reinvents itself by continuously learning and adapting as the national security environments change (See Andrus (2005)).

CAS theory has emerged, developed and grown up around the study of such different systems.

CAS characteristics Contrary to the conventional way of thinking about systems (as having equilibrium searching mechanisms and dynamics), CASs show a few key features not always acceptable to conventional approaches. We have to choose, for even in the CAS-theory communities there does not exist real consensus on the comprehensive set of characteristics that define a CAS. I think that it is possible to harvest a useful framework with CAS characteristics from Maguire's literatures ``Complexity Science and Organization Studies"(Cilliers (2002)).[135]

I summarize the characteristics that I harvested in Table 8.1. The table concurrently summarizes the elements in the framework that I use to decide whether a system is a CAS (or not) and to indicate what CAS-theory may have to offer to whom and under what conditions.

Systemic	A CAS is a whole, has a boundary, aggregates agents	*that are:* networked, diverse, signaling, metabolizing, CASs themselves (often)
Dynamic	A CAS is adaptive yet it is sensitive	*by:* (co-)evolution, learning; *to:* critical transitions
Complex	A CAS shows emergent behavior	*often:* without central control, path dependent, non linear

Table 7.1: CAS characteristics summarized

The three main characteristics concern *system* (being a whole, aggregating agents or parts that operate, and may be aggregates themselves etc., etc.), *dynamics* (changing over time, by learning and/or evolution) and *complexity* (showing emergent behavior that is without central control and resists to being modeled with linear math). In the next Section I discuss why the PDC has these characteristics.

Understanding the PDC as a CAS

In this Section I discuss how the PDC shows the characteristics of CASs and how this awareness may be useful to legal scholarship.

[135] In this book, CAS is featured by 1) consisting of a large number of elements; 2) that elements interact dynamically; 3) that interactions are rich, any element in the system can influence or be influenced by any other; 4) that interactions are non-linear; 5) that interactions are typically short-range; 6) that there are positive and negative feedback loops of interaction; 7) that they are open systems; 8) that they operate under conditions far from equilibrium; 9) that they have (and their behavior in influence by their) histories; 10) that individual elements are typically ignorant of the behavior of the whole system in which they are embedded. (See Maguire *et al.* (2006) at page 166).

Each of the characteristics mentioned in Table 1 is discussed in a Subsection below. There I first highlight the characteristic in the light of one or more of the example CASs mentioned earlier and subsequently argue why the PDC has the characteristic too and why this is useful for legal scholarship.[136]

CASs are systemic – so is the PDC

According to Merriam-Webster's Collegiate Dictionary, generally, a system is ``a regularly interacting or interdependent group of items forming a unified whole: as a gravitational system, thermodynamic system, digestive system, river system, a computer system, capitalist system."(Merriam-Webster Inc. (2004)) A CAS is also a system following this definition, but much more complicated. As Meadows defines, a system, in the context of ``CAS", is

> ``a set of things—people, cells, molecules, or whatever—interconnected in such a way that they produce their own pattern of behavior over time. The system may be buffeted, constricted, triggered, or driven by outside forces. But the system's response to these forces is characteristic of itself, and that response is seldom simple in the real world."(Meadows (2008):2)

This type of system description considers identity, invariants and stable interactions in equilibrium to be focal. This is a manner of looking at the world that clearly helps us understand. One might even stipulate that we need such descriptions to support our comprehension by temporarily fixing a moving world into a series of snapshots of which we analyze the elements. This approach is so successful, that we tend to reverse the argument and assume the world to be in a state of equilibrium (or to be working towards such a state). But this would be ill-advised, as my discussion of the dynamic and complex characteristics of CASs shows.

When I look with the ambition to describe what CASs are, I have identified the systemic requirements for being a CAS to include being

[136] I hesitate to use 'legal theory' or 'jurisprudence' here. I am not quite sure that these disciplinary niches will consider my work to be within their domain.

a whole, networked aggregation of diverse agents, that signal, that operate simple rules, that may be CASs themselves.

Any CAS is a whole To be able to consider something to be a CAS, it must have identity; it must be possible to consider the thing to have a boundary and some internal coherence. I think that immune systems, ant colonies, economies, languages, organizations and cyberspace do not need additional evidence for establishing their capacity to have boundaries.

Local weather systems are not self-evidently wholes with an identity. Yet, this may be accommodated in several ways. One of them would be to consider a weather system to equal an atmospheric domain that has an isobar (a line connecting points of equal pressure) as its boundary. Within such a system, several subsystems may exist and interact with each other.

The PDC is a whole

In the Second Section of this chapter, I already discussed the internal structure of the personal-data community as a whole (a ``dot") that has internal structure. The body of the PDC contains a large amount of data users (in fact: all connected personal data users, world wide). The whole is the network. Its boundaries are determined by any ``no further links to responsible individuals" situation.

Kaliya Hamlin drew a personal data list in a mind map to show the diverse uses (and thus the diversity in values) of personal data.[137] According to Kaliya, the contents of the mind map are derived from a long list in the *Rethinking Personal Data Pre-Read Document,* published by the World Economic Forum in June 2010.[138] I replicate the list in Figure 7.3.

[137] See http://www.identitywoman.net/personal-data-list-in-mind-map-form

[138] See also: P Klaus Schwab & Hoffma (2011).

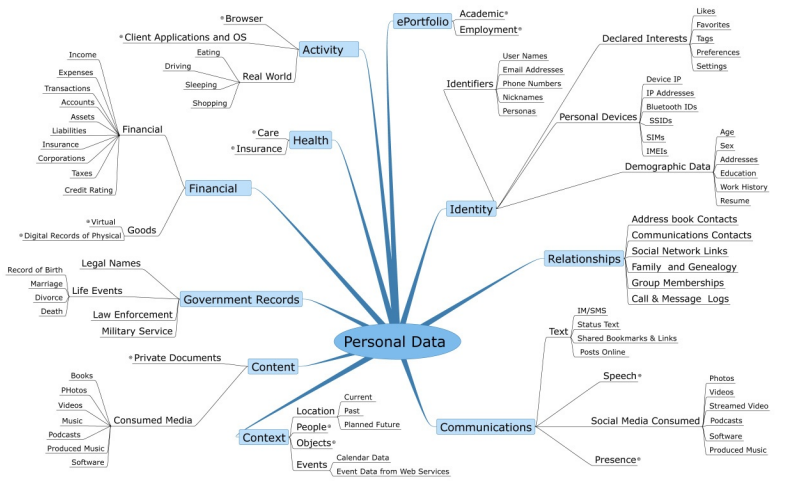

Figure 7.3: Diversity of personal-data use and -values by Kaliya

The complicated mind map in Figure 7.3 shows us how diverse the data users are in the PDC. It is beyond our abilities to give an exact number about how many data users exist in the PDC. But, they vary to a significant degree, in terms of their objectives,[139] data types,[140] legal nature[141] and so on. Among these data users, some are relatively widely scoped (e.g. Google) while others are more specialized, focusing on particular problems such as the Military and the Police.

I submit that the PDC is a system, having identity, but also having internal structure in the form of collections of interconnected institutions, service providers, individual users and so on, composing a multi-layered network with hubs and overlapping communities.

[139]For instance, Google collects personal data in order "to develop new ones, and to protect Google and our users...(and) use this information to offer you tailored content – like giving you more relevant search results and ads." See, Facebook's Privacy Policy, access via https://www.google.nl/intl/en/policies/privacy/. World Health Organization collections personal data for normal web site usage and personal identifiable use. See, WHO's privacy policy, access via http://www.who.int/about/privacy/en/

[140]For example, financial institutions pay more attentions to personal data related to economic information, while others, such as health institutions, may concern with health data.

[141]Some data users, like Google, Facebook and Tecent, work for the benefits of companies, while the others are non-profits organizations, such as governmental data users.

Why considering that the PDC as a whole is useful

It is useful for legal scholarship to consider that the PDC is a whole because legal scholars tend to think in jurisdictions. The concept of the PDC provides an image of subject matter for regulation that does not coincide with the classic conditions that accompany the notion of nation-state related jurisdiction. Recognizing the related anomalies as relevant may well be a necessary condition for facing their consequences.

CASs are complex – so is the PDC

Ottino (2003) stressed, since systems are formed by networks of interactions, that the first that must be done when discussing complex system is to distinguish complex from complicated systems. Complexity emerges only when ``the collective behavior of the parts together is more than the sum of their individual behaviors" (Newman (2011)). The relationships in the system are not simply the aggregations of the individual static entities, but like ``a cat's cradle of interactions"[142] between dynamic units. Complex systems are not controlled centrally and resist their behavior to be modeled linearly.

The PDC self organizes

Any CAS operates at least partially without central control

Complex adaptive systems have internal structure (may show multiple levels of aggregation) and a dynamic history -- they emerge, live and survive, in a co-evolving environment.

The PDC operates without central control

[142]I borrowed the term from Haldane,"*Rethinking the financial network*". Haldane thought financial network is CAS. "*Complex because these networks were a cat's-cradle of interconnections, financial and non-financial.*" His paper inspires me a lot. It provides a fresh insight for looking at financial systems and to treat financial crises (See Haldane (2009) at page 23).

Among the diverse data users that constitute the PDC, no pure or ideal agent represents the system as a whole. One can argue that Facebook is the flagship in the social network ecosystem. But Facebook is not the ideal agent in charge of the whole PDC, and neither is its structure representative for the structure of the other agents that make up the PDC. It is fair to say that giant services like Facebook and Google are keystone agents that have disproportionally large effects on the PDC they are a part of. For instance, China's Facebook RenRen is strongly and unidirectionally influenced by Facebook.[143] Yet I prefer to say that these keystone agents strongly influence their sibling agents (at the same level) than that they control the whole ``dot." In terms of network theory,[144] they are ``hubs" in the small-world[145] networks that connect those agents in the PDC that represent the social networking ecology.

The PDC clearly exhibits the feature of self organization. Various units come to the system voluntarily and even without leaders from inside or outside the system. For instance, the development of the Facebook social networking technology by an undergraduate student, and then the rapid emergence of the Facebook community is a result of self-organization within the PDC. The appearance of the Facebook community was not designed or commanded. The local, individual actions and communications of technology providers, businessmen, service providers and individual users of social networking did produce the patterns that became the Facebook community. In fact, there are many PDC ``sub-communities," such as around search engines, file sharing, online chat services and Wikipedia. These all emerged in the PDC in a manner similar to the one described for Facebook. Peltoniemi & Vuori (2004) said, as mentioned above, that emergent properties are the result of self-organization. Thus I assume that emerging phenomena are the result of self-organization. Consequently I accept that the PDC shows the third characteristic of what makes a CAS.

Why considering that the PDC operates without central control is use-

[143] Zhang & Schmidt (2013).

[144] See, for instance, Barabási & Albert (1999).

[145] As discussed by Watts & Strogatz (1998) and Barabási & Frangos (2002).

ful

It is useful for legal scholarship to consider that the PDC emerges and operates without central control because this may become a systemic risk to legal systems. It is essential to legal practice that human individuals can be identified as being responsible for behaviors in and by the CAS. It is our contention that the ``responsibility drain" as implied here is currently in full swing for the law's grip on PDC behaviors.

The PDC cannot be modeled as linear

No CAS can be modeled as linear

The feedback loops in a complex system result in non-linear behaviors. Nonlinearity means that the behaviors based on relationships between system units I wish to measure are not mathematical proportional: outputs may be disproportional to inputs; small inputs can produce large outcomes; and large inputs can produce small outcomes ((McDaniel Jr *et al.* , 2009):193). The inputs of a CAS flow through a multitude of feedback loop that tend to produce nonlinearly related outputs (Ruhl (1997):946). And as complexity theory allows for the analysis of all CAS behavior as being dynamic (or as having time related feedback loops), complexity theory allows for the study of phenomena that cannot be modeled with mathematics that yield solutions.

The PDC cannot be modeled as linear

The previous analysis has shown that the PDC can be described as a decentralized system which comprises a web of interdependent data users. But is the PDC's behavior non-linear or is its behavior simply that of a system with a complicated internal structure? The characteristic that helps establish a system as a complex system is its having non-linear feedback loops between its diverse units.[146] As I analyzed above, a complex system that has these non-linear characteristics often shows a capacity to self-organize into emerging aggregate agents.

The feature of emergence exhibits itself very clearly in the PDC.

[146] Feedback loops exist in complex systems when information flows in the network follow paths that work circuitous, as in direct or indirect loops (Ruhl (1997) at page 948). For a more detailed discussion of the nature and characteristics of feedback loops (see, Tussey (2005)).

Different patterns of phenomena or behaviors emerge from the interactions among agents, rather than being designed into the system.[147] In fact, even the PDC itself is an emergent community, produced by the individual activities of local agents without a clue about what their collective behaviors would look like or lead to. The PDC emerged from the local interactions of agents, particularly technology providers, service providers, institutional users, consumers, businessman and other stakeholders, pursuing their own interests. These interactions produced (led to the emergence of) vast and networked communities through which personal data (and much, much more) can be transmitted fast and easy. This PDC is neither invented nor designed by any individual agent. Rather, it emerged from interactions of a large amount of ``constituent'' agents that reacted to opportunity and need.

I thus conclude that the PDC has the characteristic of nonlinear feedback loops what are the hallmarks of a complex system, since the inputs of the PDC flow through feedback loops and produce nonlinearly related outputs (Ruhl (1997):946).

Why considering that the PDC cannot be modeled as linear is useful
It is useful for legal scholarship to consider that the PDC cannot be usefully captured in simple linear models because this may prevent legal scholarship from falling into the type of trap that has lured large communities in economic scholarship astray.[148] Legal scholars may well have hesitated to join forces (and scientific stories) with disciplines like economics and physics because considering the subject matter of legal scholars -- autonomous decision making and relating that to individual responsibility -- has long been considered resilient to scientific investigation. Only in the last three decennia there have

[147] See also Rouse (2008):38.

[148] Happily machining away from their models the mathematical difficulties that would ensue when accepting that diverse, dynamic and context dependent forms of autonomy and responsibility are at work in the decision making of the agents in the systems observed. In stead, these scholarly communities preferred to face the continuous falsification of their mathematical models by simplifying agents into being unidimensional "rational economic men" and by concurrently making the models more and more mathematically complex. See Bowles (2006) for an extensive discussion.

become generally available methods[149] of and machinery[150] for simulations that allow for further investigation into behavioral models of diverse, dynamic and context dependent forms of autonomy and responsibility. Simulating the behavior of agents with distributed types of rule sets they follow has become a hall mark of complexity science. [151]

I thus conclude that the PDC has the characteristics of self organization and non linearity, the characteristocs that make a system complex. In Figure 7.4 I give a sketch to show what the PDC might look like if described as a networked complex system.

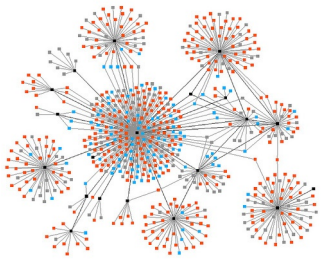

Figure 7.4: Hubs in a small-world network

CASs are dynamic – so is the PDC

CASs change over time, by learning and/or evolution or co-evolution. It has been observed that the number of personal data users is increasing every year, every month and even every day. For instance, in

[149] Agent Based Modeling – see Schelling (1969) for an early example.

[150] See http://ccl.northwestern.edu/netlogo/.

[151] For instance, the "Living Lab" at Leiden University provides promising initiatives and applications of agent-based models to test policy decision options. In their presentation, Yuan Yuan Zhao and Professor Katzy took the German Solar Panel Industry as an example and showed that computational policy simulations could be used to inform policy choices. See, e.g., www.centre4innovation.org

February, 2014, Facebook announced a new iPhone app called ``paper." The app could [...] ``to supplement its computers in recommending articles and blog posts on a dozen topics." The app would be an artificial (or intermediate) personal data user, since it delivers the articles and videos that it expects you to like, based on the analysis of your personal data as collected by Facebook (Goel & Somaiya (2014)). Thus, the PDC changed and its network increased in size.

Any CAS does (co)evolve and/or learn What distinguishes CASs from other complex systems is their capacity to adapt. According to Tussey (2005) at page 109:

> ``... adaptation most often results from coevolution, in which the system responds to changes in other systems with which it interacts, and those systems similarly respond to changes in the primary system ..."

According to Kim(Kim & Mackey (2013):8),

> ``...CASs as complex systems with the ability to adapt to changes in the external environment as a result of experience via conditional action and anticipation."

Adaptation of a CAS implies that a CAS has the capacity to co-evolve with its environment. No single CAS does exist independent from its environment. Each and every CAS is closely linked to its environment. And a CAS does not only exist within its 'environment', it becomes intimately related to it. Thus, most CASs have bidirectional relations with their environments: as the environment changes, the CAS needs to change along in order to ensure an adequate fit; and when the CAS changes, the environment is changing along to. This is a continuing process: as its environment is changed, the CAS needs to change with it, and vice versa, and so it goes on and on.[152] Perhaps, co-evolution can be seen as a process wherein CAS and environment try to re-tune their reciprocally dependent fitness in the dynamics of unfolding time.

This co-evolutionary process will show *as if* both the CAS and its environment are learning. But in its biological origin there is in the

[152]See also Capra (1997) and Holland (1995).

evolutionary process no conscious process like learning involved. I submit nevertheless that CASs that have consciously behaving agents can learn, and thus influence their fitness consciously -- and thus may tilt the coevolutionary process towards their perceived interest.

The PDC does (co)evolve and/or learn The PDC is as open as other CASs to coevolve in response to internal dynamics[153] and environmental stimuli. It continuously tunes itself in order to find states of adequate fitness.[154] The PDC is itself a result of ongoing social interactions. The environment provides pre-existing constraints, provided by culture, law, technology and so on. These constraints determine the space wherein the PDC can find adequate co-evolutionary forms.

When describing the constraints of provided by the environment, I follow Lessig's lead.[155] Lessig's work modeled how cyberspace is regulated and, as a part of that, on modeling how law might regulate cyberspace. What I will borrow from Lessig is the model he created to analyze regulation from the perspective of the subject that is being regulated.[156] His model helps us to examine the relations and interactions between the PDC and its environment.

In his book, Lessig represented the thing that is to be regulated by constraints as a ``dot."[157] He identified four constraint-delivering forces: law, market (or economy), architecture (or technology) and norms (or culture). The resulting constraints trie to regulate the dot. Lessig presents the constraints in a Figure.[158] I replicate it in Figure 7.5.

[153]Of course, if a CAS has CASs as its constituting agents, it is concurrently the environment to these constituting agents and will also co-evolve with them.

[154]See also: Tussey (2005):120.

[155]Lessig (2006).

[156]Very much a realist perspective, at least initially.

[157]This is the dot I discussed in Section 2.

[158]Lessig (2006):123.

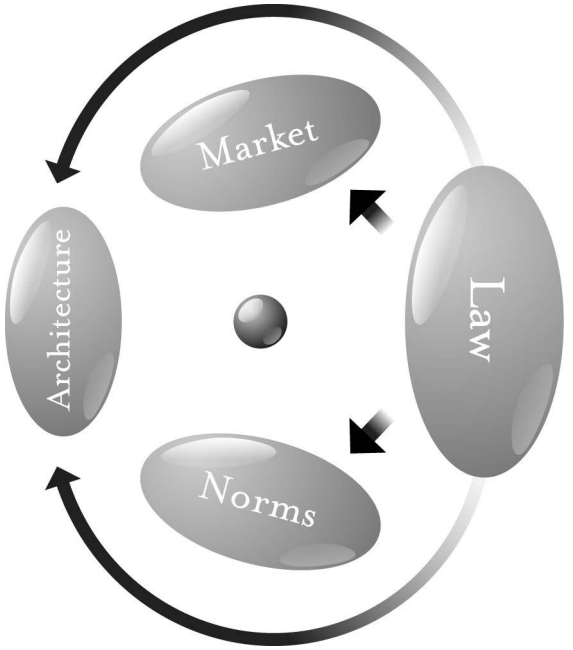

Figure 7.5: Lessig's regulatory forces interacting.

I trim Lessig's regulatory forces and direct them to our PDC, and representing them as the environment with which the PDC co-evolves. An important regulating force mentioned by Lessig is what he calls ``regulation by architecture."[159] I assume them to be the regulatory forces that stem from environmental and infrastructural conditions that in the context of behavioral choices most often have to be accepted as stable, like the legislative system, the Berlin Wall, or the IPv4 protocol. However, these architectures are sensitive to change -- be it in their own ways. One might consider a ``dot" to be thrown into an environment that shows a structure that constrains its behavior, but into an environment that is itself a moving target -- that even can possibly be moved by the dot itself.

Co-evolution of the law, the legal subject and the environment be-

[159](Lessig, 2006):127

comes problematic when the political system that can adapt the formal laws is too slow in its operation. Understanding what the problem is (and how to address it) would be useful. In Chapter 4, I adopted Incomplete Law Theory[160] to explore the dynamics of what I can now call the environment wherein the PDC must live. In the Chapter, I started from technology-constrained data protection law and ended by exploring the dynamics of technology and its wide, architectural influences on legal arrangements. My observations and further evidence suggest that the most striking constraints for PDC- and PDC-agent behaviors do arise from the dynamics in technology. Agents, such as companies, are concerned with technological changes and these changes affect the agents' behaviors. Indeed, changes in technology have real consequences. And although their characteristics remain architectural in the sense of Lessig, their dynamics have sped up to a level where traditional legislatures cannot keep up with the pace required. It may well be, that some reactive change in the legal system as architectural environment is required.

Additionally, the PDC is influenced by the other elements in its environment. For instance, the mutation in social-economic backgrounds which were brought on by the 9/11 tragedy did feed into the "dot," which brought changes to the behaviors of units in the PDC and led to a ``tug-of-war of conflicting interests" between national security values and privacy values: the protection of national security values implies that inroads have to be made into the protection of the right to be left alone.[161]

Moreover, in the PDC is not an uneventful ``dot" itself. Instead, it is an ever-changing one. Strategic changes of one unit may strongly affect the strategies of other units in it. As argued in Chapter 5, I analyzed the interaction between Facebook and its Chinese counterpart RenRen and imagined RenRen and Facebook to compete (for instance on data protection issues) in a single commercial arena (as provided

[160]As described in Xu & Pistor (2002a).

[161]In Bignami's "European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining", this conflict of interests is analyzed more in detail. By comparing the legal arrangements over data protection issues in America and Europe, Bignami showed the fierce conflicts between privacy and national security, which led to the changes on the environment of the USA PDC. (See Bignami (2007)).

by the web). The mere suggestion of such competition suggests that we may presently witness the tantrums that will unavoidably accompany the conception, birth and emergence of a unified global complex adaptive judicial system for governing the web as a unified market.

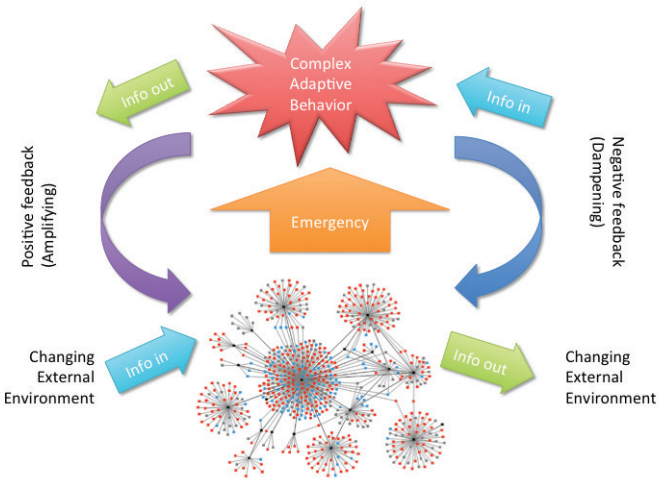

Figure 7.6: The PDC as an ecology

Within the system, the different units aggregate, cooperate, interact and develop with a specific reference to personal data, while without the system it co-evolves and competes with other related systems. These outside relations of the PDC, construed as a CAS, can be mapped out as depicted in Figure 7.6.

Why considering that the PDC does (co)evolve and/or learn is useful
To legal scholarship it is useful to distinguish (co-)evolution on the one hand and learning on the other, especially when considering subject matter the level of social ecosystems. (Co)evolution refers to a blind mechanism that happens to lead to adaptation. Learning (and teaching) use conscious mechanisms that result from conscious behavioral choices and result in social and scientific cultures (that help preserve, adapt and reproduce local knowledge bases).

I think that it is useful for legal scholarship to respect the distinction between the mechanisms of (co)evolution and learning -- even when these tend to get into a confusing tangle. Legal scholarship is founded in accepting the concept of conscious behavioral choice,[162] and not in accepting subconscious behavioral choices (sensitive to nudging) as definitive. As such, legal scholarship's primary domain is related to learning, to the learning of behavioral choices that do not subjugate to subconscious impulses. The issue of where the boundaries of the disciplines meet in these issues is important, and can only be understood in cooperation with multiple disciplines.

The PDC as a CAS – summing up

Our goal of looking at complexity theory is to find out whether interpreting the PDC as a complex adaptive system does improve our understanding of the data protection law's subject matter. I established

- that the PDC is of systemic nature, showing several levels of aggregation and thus providing not only handles for interdisciplinary communications, but also providing several extra handles for monitoring the multi disciplinary consistency of our findings. An important aspect brought to the fore by looking at agents in levels of aggregation makes explicit that the possibilities of scientific prediction of the behavior of agents that do not have consciousness is something quite different from the prediction of the deliberate behaviors of the subjects of the law, of economics and of the social sciences;
- that the PDC is a dynamic system -- on the one hand through the non-deliberate mechanisms of (co-)evolution and on the other hand through the deliberate mechanisms that I classified under learning; and: as a complex adaptive system, I expect that the PDC may have to face the risks of critical transitions (and that legal arrangements may be designed to minimize such risks);
- that the PDC is a complex system, that operates without central control and in a manner that cannot be caught in a linear model

[162] Consequently it does not consider (co-)evolution to be directly in its domain. However it can enter its domain via conscious behavioral choices that influence evolutionary processes.

> -- these aspects are the corollaries of agents that follow context dependent conditional rules in a network of direct and indirect feed-back loops. As a consequence, scientific understanding of the PDC has to remain very incomplete, yet is becoming larger through new practical possibilities for serious agent based modeling using serious computation capacity.

I consider these findings to have added to our understanding of the subject matter of the data protection laws.

I began by suggesting to look at data-protection laws' subjects (and their environment) as a complex adaptive system in the hope that this will also allow us to provide a unified account of seemingly unrelated phenomena as characteristic CAS-properties in a single system.[163] Our research does also fulfill this hope. I added to our understanding of the PDC through combining our current knowledge with knowledge and experiences from different examples of CASs, and from different disciplines. Basic knowledge about CASs informs us that the PDC comprises a complex web of interdependent nodes (units or agents) that link to one another and that make some of them emerge as ``hubs." These stylized but explorative considerations can be woven into a perspective that understands data protection law's subject matter as a CAS.[164]

[163]See also (Beckner *et al.* , 2009):3.

[164]In fact, both the PDC network and the data protection law surrounding it are CASs. The same framework I adopted to analyze the CAS-characteristics of PDC could be applied to the data protection law too. In previous Chapters, we witnessed the difficulty of attempting to design static legal regimes to regulate the PDC. We are inevitably stuck in the co-evolution of law and the systems it regulates. Efforts to build rigid legal regimes to control thus are destined to fail eventually as the social system under regulation evolves in ways that work around or exploit the legal system. Data protection law itself is a CAS bound in a co-evolutionary, multi-system "system of systems" so it is going to be adaptive over the long run if it is designed with adaptation as a primary attribute. For the issues of the CAS-characteristics inherited in law, Professor Ruhl has done a lot of promising research on this and readers could know more about this hidden nature of law in his books.

Peering from a complexity-based perspective

The goal of introducing the CAS-theory is to improve our understandings of how the data protection law's subject matter operates (section 4). Previously, I witnessed how a CAS perspective might move data protection law into new and interesting directions. From the perspective of CAS, I recognized that systematic nature of the PDC, the complexity of the system, and the necessity of recognizing its co-evolution aspects. The PDC hence can be understood as a CAS. However, challenges follow with findings.

A pressing question comes to the fore: does our CAS-analysis push the PDC out of control and thus beyond the reach of useful governance by law?[165] I will answer this question in the negative. As Clark (1999):1 argued: this kind of system can be led, influenced and enabled in a variety of ways. Among these ways, legislation and legal enforcement are also included. As a matter of fact, CAS-theory has become more and more prominent because it helps to understand and influence what otherwise could only be qualified to be systems of unapproachable *complication*. Consequently, when considering legal arrangements for a PDC, the legislature is wise to bear in mind the inherent CAS characteristics of it. Data protection law cannot treat the PDC as anything else. As a "*society's problem-solving mechanisms*,"[166] legal arrangements are seeking to regulate a CAS. In these cases, Ruhl mentions that ``*it is very difficult to solve problems in such systems unless you think like a complex adaptive system*"(Ruhl (1997): 51).

Undoubtedly, this approach may present insurmountable hurdles for policymakers. Yet, policymakers of data protection law can draw a number of lessons from other CAS projects in areas such as econ-

[165]In fact, Law making and law enforcement is a multi-level affair: they are, for instance, often directly linked to unit behavior, yet have the ambition to nudge the emergent, overall behavior of the PDC as a whole towards improvement. I consider a distinctive characteristic of how the forces of laws are understood and enforced to be the assumption that they are backed by reason.

[166]See Ruhl (1997): 51

omy,[167] epidemiology,[168] biology[169] and finance[170] to inspire their exploration of the subject matter. It is against this background that I expect that regulation over data-protection issues stands to benefit from being informed through the lens of CAS theory, integrating the contributions of a diverse bunch of scientists and scholars.

Therefore, in this section, I provide some tentative policy heuristics that build on recent advances in our understanding of the PDC and that incorporate findings and methods from disciplines that have paid more attention (and also contributed more) to CAS-theories than the legal discipline.[171] I only know of these methods yet in a sketchy and incomplete way. I offer them as personal insights that need further research and interdisciplinary attention. More specifically, I extract some heuristics for the design of legal mechanisms that, in my opinion, may become significant for the support of rational policymakers considering the adaptation of laws. These heuristics concern (i) the monitoring of the effects of legal intervention, (ii) understanding the environment, (iii) attention for incentives (mechanism design), (iv) ``hub" control and (v) leeway for learning and adaptation.

(i) Monitoring the effects of intervention

When any group of ``things" is considered to be a system, it is formulated from the perspective of the system being a whole, rather than from each individual participant's perspective. Discussing the PDC is no exception. Since it is an interconnected system, policy makers could seek to promote the continuing health of the PDC by maintaining some aggregated measure of balance among them. When considering legal interventions, policy makers will realize that they are trying to intervene in a global interconnected system, which means that any intervention may have consequences in the whole of the PDC, at

[167] Arthur (1999)

[168] McDaniel Jr *et al.* (2009)

[169] Levin (1998, 2000)

[170] Haldane (2009)

[171] In this context, I mention as examples models and modeling as developed in engineering, the sciences and economics, network analysis, computer science, biology and genetics and some other cross-discipline methodologies, like computer simulation.

unexpected locations. Thus, it is important to investigate what benefits a legal intervention into the PDC will have as seen from a systematic perspective.

To assess the benefit of legal interventions means to measure. When I discuss the measuring aspects of ``moving targets" like the order in the PDC, measuring may focus on stable equilibria as related to the regulatory `attractor' forces of legal arrangements. According to Page (2012)

> `` ... if under a wide variety of assumptions the system goes to equilibrium, then we can have some measure of confidence that comparing equilibria is sensible. If, though, it is extremely difficult to produce equilibria, then equilibria may not be the appropriate solution concept"(Page (2012):16).

It is not easy to evaluate the result of legislative intervention. As Page also mentions

> `` ... one way to evaluate mechanisms might be to consider a variety of initial conditions and a variety of possible behavioral rules and to examine what arises given those combinations" (Page (2012):16).

Suggesting to estimate the value/benefit of legal intervention regarding PDC behavior in terms of equilibria seems in contradiction with our earlier argument about the PDC being a complex adaptive system. But as I do think (know) that neither the long-term future, nor the long term behavior of CASs can be predicted accurately, the heuristic that suggests to estimate the value/benefit of legal intervention only makes sense for short-term predictions. These predictions can be interpreted against actual behavior in order to establish whether CAS behavior `follows' the model and for how long. Such predictions may work like weather forecasts - when I know enough about the forces that work the system's behavior, I may actually gain some short term predictions that can be trusted.

For this approach, models of Markov processes can be used to evaluate the benefit of legal intervention.[172] Dependent on parameters specified, Markov processes converge to a fixed equilibrium,

[172] My discussion of Markov processes is based on *Chapter 5, Markov Pro-*

independent of what the initial state of the system is. A major assumption is that transition probabilities between states remain constant. Evaluating the benefit of a legal intervention can be further simplified by constructing two Markov models for the PDC' s ``health states," one with and one without the intervention.

My main point is that estimating and measuring the value/benefit of legal intervention requires to create models and measures, and to test, use and interpret them consciously. And, most important, that linear models (of which many are available and well understood) like models in Markov processes can be *useful* for short-term monitoring of CAS behavior, yet will be *dangerous* for long-range predictions and evaluations of complex adaptive systems.

One of the reasons that long-range predictions of the behavior of CASs is dangerous relates to the fact, that such predictions, even if the working mechanism are completely known and deterministic to be extremely sensitive to initial conditions.[173] This means that complexity theory warns us that transplanting EU data protection law to China is highly unlikely to produce the similar results in China when compared to the effects in Europe.

(ii) Understanding the environment

I found that the PDC is adaptive. This helps us realize that understanding the environment that underlies and surrounds the PDC remains of importance. The impacts of other constraints in the environment, neither on/from the ``dot" nor on/from each other, should be underestimated or forgotten altogether. I simply assume that institutions that receive regulatory forces always have the potential to feed back to the regulating institution. *E.g.*, the PDC that is regulated by law may propagate constraining forces as a feed-back to the legislature (or, more down to earth, Facebook may, in the face of the personal-data protection laws that threaten to regulate it, propagate feed-back forces by lobbying the legislature).

In terms of CAS-theory, the environment that co-evolves with

cesses by prof. Scott Page (yet unpublished manuscript, I assume), available at: http://vserver1.cscs.lsa.umich.edu/~spage/ONLINECOURSE/R10Markov.pdf"

[173] See for instance Mitchell (2009).

the PDC, includes at least Lessig's interacting regulatory forces. I think that the subject for regulation, the PDC, and all four regulatory forces that Lessig identifies (laws, norms, market, architecture) have links and feedback links to all other units. In Figure 7.7, I have painted this picture. What emerges, is that all units are in a network.

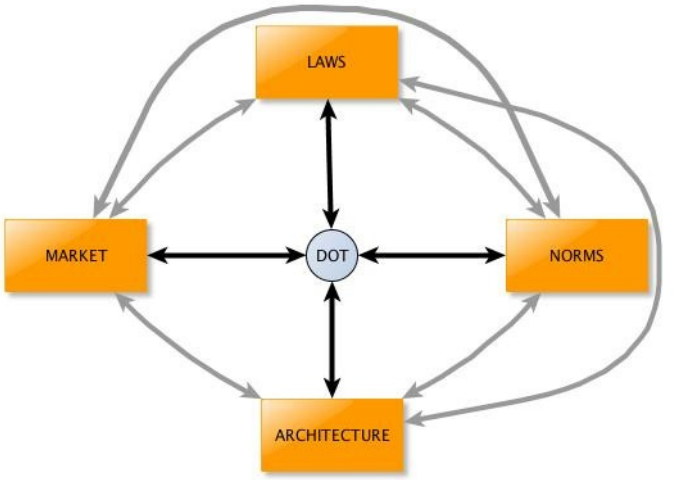

Figure 7.7: Lessig's regulatory forces and their "dot" as an ecology.

Feed-back loops are the hallmarks of ecologies. In other words, Lessig's approach to modeling the regulation of a ``dot" gives rise to an orderly picture that clarifies a lot of the structure of the ``regulatory ecology" wherein a PDC is a ``dot."

However, as I have seen in Section 2, imagining the PDC as a ``dot" is an oversimplification. The same goes presumably for the other nodes in the network of Figure 7. And, as indicated, I expect that such oversimplifications may be at least partly addressed by applying a CAS-theory approach, because in this approach legal scholarship will be forced to consider what chain-reactions may cascade through the regulatory ecology as a result of the publication of a single policy

decision. (Of course, the same is true for the other nodes.)[174]

The findings on the influences of the environment on the PDC does supports the conclusion made in Chapter 6 that transplanting EU data protection law to China is highly unlikely to produce the same results. The environment that underlies and surrounds the PDC forms the initial conditions for any data protection law. As mentioned, one CAS property is "sensitivity to initial conditions," meaning relatively small changes in the conditions of a CAS can lead to disproportionately large differences between the original and altered systems at later times. Over time—perhaps soon or perhaps much later—those two systems could diverge tremendously as a result of that one seemingly trivial difference, so that one would never know that at some point in the past they were almost identical. And the legal cultures in the EU and in China are not even close to being identical at the outset.

And it is important to bear something else mind. Legal systems and subsystems are parts of the PDC's environment and can themselves be CASs as Ruhl (2008) convincingly argues. In other words, both the PDC network and the data protection law surrounding it are CASs. This emphasizes the difficulty of attempting to design static legal regimes to regulate the PDC. We are inevitably stuck in the co-evolution of law and the systems it regulates.

Moreover, once transplanted to China's PDC environment, even if in exactly the same form, EU data protection law becomes part of its new home CAS and will instantly begin co-evolving in an environment that does not resemble the EU's PDC environment. Because of sensitivity to initial conditions, these environmental differences will inevitably take the transplanted pod of EU law into different directions, lead to co-evolutionary responses in the Chinese PDC that the EU PDC would not have produced, etc. Even relatively small differences between the EU and Chinese PDCs could produce vastly different trajectories, hence the large differences in the EU and Chinese.

[174] An example may be read in the issuing of the Commodity Futures Modernization Act of 2000 (by the legal node) that was based on highly esteemed economic expertise (by the market node) and that caused great harm to each and every node in the network by marking the onset of what would become the financial and economic crises of 2007/8.

(iii) Hubs are special

Here, I pay attention to another perspective on networks, that helps to ensure appropriate control. For example, we may learn from experiences in epidemiology and the role of small-world network theory for deciding on who to vaccinate in order to prevent a pandemic. Analogously, when Haldane (2009) complained that the financial network's super-hubs challenge the stability of the whole system, he accepted a good lesson from HIV controlling strategies, particular from the Australian experience on epidemiology. Australia is successful in controlling the rate of HIV and AIDS incidence in its country.[175] Why? According to Haldane (2009) the short answer appears to be government policy:

> ``*Australian policy has been grounded in biology and systematic thinking, with evidence-based and preventative policies. Education and prophylactic measures have been widely available. But there have been targeted initiatives for high-risk groups – for example, sex workers and drug users – through subsidized needle and syringe exchanges and free condoms. The results of this program are clear in the statistics*"(Haldane (2009):25).

Haldane found that the Australian approach could be translated to the financial system: it is crucial to target high-risk "super-spreaders" in the financial network.

This gives important lessons to consider when striving for personal data protection too. As I mentioned above, Facebook, Google, Apple and other giant units are such huge forces in the PDC global network. They are the leading powers in the network since they create their own standards and influence the outcomes of the PDC. This kind of units in the PDC to be super-hubs. Super-hubs are also the high-risks to data protection law's enforcement just like 'super-spreaders' in financial network and high risk groups in the HIV contamination network. Inspired by Haldane's work, I suggest to introduce more specific requirements and to monitor them on these super-hubs. The

[175] According Haldane's data, By 1994, rates of incidence in the US were six times those in Australia. By 2003, the per capita prevalence of HIV in the US was ten times that in Australia (See Haldane (2009)).

logic underlying the suggestion is to support the immunity of the PDC as a whole at the expense of 'inoculating' and monitoring, the super-hubs.

Moreover, I have shown that the PDC comprises a complex web of interdependent units that link the nodes to one another and that make some of them emerge as ``hubs", and even ``super-hubs". Hubs are ``super-connectors." They emerge often in small-world networks. And as discussed before, in the PDC, the units, and units-based sub-systems or sub-subsystems interconnect in networks where data, services, dependencies and other forms of information flow, in a manner that allows to consider the resulting system analogous to natural ecosystems where energy, waste and other materials are passing through different nodes, through the local infrastructures. As mentioned, such systems tend to form small-world networks that show the emergence of ``hubs." This enhances their communicative efficiency, but concurrently increases their vulnerability to hub-directed attacks.[176] And much of the behaviors of and in such ``dots" do, when inventoried, show a ``power-law" distribution rather than a ``normal" distribution.[177]

For policymakers, this is an important lesson. At present, policymakers try to the control the PDC's units as much as they can. I do not mean this is wrong. But the approach may leave policymakers navigating in dense fog when assessing the dynamics of the PDC because of the diversities of units. In order to better control the PDC, more attentions should be paid to regulating the hubs. This means the assessment on the efficacy of data protection laws should be atomistic: node by node, or super-node by super-node. More fundamental, the information about the links to one of the nodes should be collected as much as possible. These data are central to understanding the PDC's dynamics.

(iv) A role for agents' incentives

Data Protection policymakers can possibly benefit by analyzing the problem of behavioral incentives. The sketch mentioned hereafter

[176] Barabási & Frangos (2002)

[177] Barabási & Frangos (2002)

is based on and largely extracted from Maskin's paper for his Nobel Prize Lecture (Maskin (2008)).[178] In the paper, he offered an general model of implementation theory, which can be applied to provide recommendations on how to best set the rules (e.g., for data protection) as a function of the data subject's demands and the nature of the relevant personal data community. In this general model, the mechanism design for data protection law is simplified into the following three points:

1. *Desired outcome*: what I mean by desired outcome is naturally dependent on the context. For legal arrangements, seeking to regulate data users' behaviors, the desired outcome is compliance with the law by regulated agents (Maskin (2008):1).

2. *Mechanism and mechanism designer*: A mechanism is an institution, procedure, or game for determining outcomes (Maskin (2008):2). Not surprisingly, who gets to choose the mechanism -- i.e., who is the mechanism designer -- will depend on the setting. In the case of legal arrangement over data protection issues, mechanisms include law, enforcement institutions, and others (Maskin (2008):2). For mechanism designers, I normally think of the legal agencies, both lawmakers and regulators, who enact law and also enforce it. However, as legal arrangements always leave discretionary powers to the PDC, also the PDC can be considered a relevant mechanism designer.

[178] As Page concluded:

> The mechanism-design literature characterizes an economic or political institution as consisting of six parts: an environment, a message space, a space of outcomes, a response function (or behavioral rule) for individuals, an outcome function that maps behaviors into the space of outcomes, and a social choice correspondence: a set of idealized outcomes given the environment. This analytic framework proves sufficiently general to encompass most institutional settings, including exchange economies, networks of banks, and legislative bodies. It can also help to organize our thinking about how complexity arises, why complexity matters, and what we might do to harness complexity for our betterment.(Page (2012))

In this article, I just offered some very superficial knowledge about mechanism design. In the future, I may work on more comprehensive trials to adopt the mechanism design approach to predict complexity.

3. *Problems in mechanism design*: In a world wherein regulated agents do strictly behave according to legal arrangements, optimal rules of data protection would be straightforward: Glachant (1998) suggests that the lawmaker then has only to pass a law mandating this outcome. The role of data regulators then will become senseless too. Yet, we do not live in such a world. Glachant (1998) suggests that lawmakers and regulators do not know which outcomes are optimal in advance, that they have to proceed more subtle and indirect, than to simply prescribe outcomes in a linear fashion.

The problems are exacerbated by the fact that the regulated agents do have their preferences and may not have the incentive to behave in a direction that the law points to (Maskin (2008):4). The gap in incentives is one of the most widely studied aspects using mechanism design techniques and models. Mechanisms must be incentive compatible (Maskin (2008):4). In the context of data protection's mechanism design, much of the work is directed at answering the three basic questions Maskin (2008):4 lists:

1. When it is possible to design incentive-compatible mechanisms for attaining the desirable outcome?

2. What form might these mechanisms take when they exist?

3. When is finding such mechanisms ruled out theoretically?

Although the three questions appear to be simple, it is not an easy task to answer them solely by legal methods. Nevertheless, mechanism design researchers invented multiple models to address these three fundamental questions. Such models may appear as new and sophisticated policy instruments that can combine with both the requirements for studying CASs and the legal instruments to meet the desirable goal of data protection.

(v) Incentives vs learning

We know that CASs encompass non-linear feedback loops. Thus linear models for direct regulation may easily fail. What might be done

to influence or nudge the PDC's emergent behavior? Part of the answer lies in improved anticipating of responses and outcomes, and part in improved control on hubs.

First, to predict the behavior of a CAS contradicts the finding that even the best efforts of the sharpest minds cannot make accurate long-term forecasts about a CAS (Jervis (1997) Watts (2012)Page (2012)). Nevertheless, I agree with what Page argued that some characteristics of outputs and some institutions could predict better outcomes than others, if proper models are adopted and are interpreted cautiously (Page (2012)). Quite similar arguments may be brought to the fore when considering the models, methods and techniques known as ``mechanism design" and ``game theory." These areas are vast. Maskin (2008) provides a useful introduction, and Page (2012) links the basics of mechanism design to the intricacies of CAS-theory. The problems are huge, certainly for a law student, and wide open to further investigations.[179]

One thing is clear, though. Mechanism design and game theory provide models where both agent incentives and information asymmetries are important for understanding and modeling behavioral strategies. Again there remain issues about assumptions that are at the core of these models, often culminating in what requirements are posed on the consistencies in individual preferences and on the `rationality' considered inherent in individual behavioral choices. Nevertheless, like Markov models, the models of mechanism design may be

[179]Mechanism design and complexity theory may at first act in a way that defeats each other's purposes. As Page pointed:

> The former focuses on the equilibria of systems. The standard mechanism-design perspective on institutions can be summed up as follows: institutions produce equilibria; better institutions produce better equilibria. A complexity perspective, while not denying equilibria, admits other classes of phenomena, such as cycles, randomness, and complex dynamics, that can produce large events such as stock-market crashes and the collapse of markets.(Page (2012))

It is not to negate perspectives, although we link the two theories together. Instead, Page (Page (2012)) Axelrod (Axelrod *et al.* (2000)) and Beinhocker (Beinhocker (2006)) have successfully adopted the mechanism design approach to organize thinking about "how complexity arises, why complexity matters, and what I might do to harness complexity for our betterment" (Page (2012)).

moulded into useful tools for researching aspects of CAS behavior.

Yet I think that legal scholarship needs to establish and protect its own identity boundaries by explicitly defending its proper position as addressing autonomous behavior by responsible agents. Where social scientists are on the look-out for knowledge that will nudge such agents into behaving in a way that they want, often unconsciously, legal scholars are interested in knowledge that will support responsible agents to make autonomous behavioral choices, while aware of law and cultural norms -- of knowledge that can be learned.

And a legislator will presumably be best informed, when both types of knowledge and their interactions are made available.

Summary

The CAS theory may help to improve law, specifically data protection law's ability (in the long run) to regulate the PDC units' behaviors and to manage the outcomes of units' behavior's aggregates. Certainly, many other methods such as case study, qualitative, experimental-sort studies are relevant in the study of a CAS. I just try to propose a posture that takes into consideration the fact that the subject matter of the legal arrangement is a CAS, and, as such, the fact presents significant challenges to the endeavor of arrangement design. The strategies proposed in this section do not aim to create a blueprint for legislative work or to recommend imposing legal order synthesizing these strategies. Rather, the effectiveness offered by these mechanism design models could help policymakers to improve their sense of judgement when trying to solve the problems of data protection law.

Conclusions of Part II

In this Part, I investigated, through combining the PDC with the knowledge and experiences from different classes of CAS, whether data protection law's subject matter, as a network of data users, exhibits the characteristics of a CAS and what these imply for the future of data protection law.

The explorative review in Section 3 has provided indications about which kinds of subjects can be understood as CASs. Subsequently, through using some key CAS-properties and relating them to our PDC and its ecology, we are ``informed" that these characteristics apply to the PDC and that thus the PDC can be understood as a CAS. From the CAS perspective, the human-created PDC is a large and dynamic system of interacting data users networked in a particular pattern of organization from which arises the ability to adapt to internal and external changes by self-organization, emergence and co-evolution/learning (Kim & Mackey (2013); Holland (1995)).

Our findings brought challenges to legal arrangements over data protection issues, since these try to tame a CAS. Evidence taken from case studies published in this issue as well as other sources suggested that data protection law's subject matter is (possibly) quite different from other law's subject matters. It faces critical transitions all the time in practice.[180] Thus -- as we continuously have to regulate situations that the legislature could (and did) not imagine when framing the law[181] -- the purposes of data protection law, the reasons for its existence and the modalities of its regulation are requiring methods quite different from those that focus on the interpretation of material laws.

I suggest that future data protection law may be fruitful implemented, which build on CAS-theory's recommendations, since Ruhl has minded us the problems presented in a CAS only can be addressed unless you think like a complex adaptive system (Ruhl (1997)). Thus, the problem needing attention is to adjust data protection law to tally with its subject matter. But how?

Multidisciplinary CAS-theory can help legal scholarship to better inform the legislature on expected risks and outcomes of legislative interventions that address CAS-``dots." In this Part, I suggested some strategies that can be adopted to help legal researchers capture complex adaptive phenomena in the PDC when arranging or regulatory frameworks. These strategies include: (i) the evaluation of expected benefit of legal intervention, (ii) understanding the environment, (iii) the special functionalities of hubs, (iv) understanding

[180] Some induced by innovative and exploding technical (e.g., The 'Cloud'), social/business (e.g., Google, Wikipedia, Twitter, Facebook, SMS, internet banking) and governmental services (e.g., data retention).

[181] Lessig (2006) considers these situations to be legally inherently ambiguous.

agents' incentives and (v) considering the forces of incentives vs learned behavior.

The picture of the data protection law's subject matter as a CAS is an ongoing rather than completed construction. Notwithstanding that our understandings of CAS theory is in a state of evolution, our efforts thus far have already served to deepen our comprehension of many problems that troubled data protection law. And they have operated as checks against some of the mistakes of current data protection laws. It is against this background that I expect that regulation over data-protection issues stands to benefit from being informed through the lens of CAS theory.

Again: I think that legal scholarship needs to establish and protect its own identity boundaries by explicitly defending its proper position as addressing autonomous behavior by responsible agents. Where social scientists are on the look-out for knowledge that will nudge such agents into behaving in a way that they want, often unconsciously, legal scholars are interested in knowledge that will support responsible agents to make autonomous behavioral choices, while aware of legal and cultural norms -- of knowledge that can be learned. A legislator will presumably be best informed, I think, when both types of knowledge and their interactions can be made available in a coherent framework. Complexity theory is a serious candidate for providing it.

End of Part II

Index

Bibliography

Aiming Qi. 2005. Legal Protection on Personal Data. *Academic Journal of Suzhou University*, **2**, 30--35.

Aiming Qi. 2007. Macro-interpretation of Protective Law of Individual Information. *Journal of the Party School of CPC of Changchun Municipal Committee*, **4**.

Anderson, Philip. 1999. Perspective: Complexity theory and organization science. *organization Science*, **10**(3), 216--232.

Anderson, P.W. 1972. More is different. *Science*, **177**(4047), 393--396.

Andrus, Calvin. 2005. Toward a complex adaptive intelligence community: the Wiki and the blog. *Studies in Intelligence*, **49**(3), 2005--6.

Arthur, W Brian. 1999. Complexity and the economy. *Science*, **284**(2), 107--109.

Article 29 Working Party. 1998. Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. *Article 29 Working Party*, **Working Paper 12**.

Article 29 Working Party. 2009a. The Future of Privacy Joint contribution to the The Future of Privacy: Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. *Working Report*, **WP 168**.

Article 29 Working Party. 2009b. Working Document: Opinion 5/2009 on online social networking. *Article 29 Working Party*, **Working Paper 163**(June).

Article 29 Working Party. 2010a. Opinion 3/2010 on the principle of accountability. *Working Report*, **WP 171**.

Article 29 Working Party. 2010b. Opinion 8/2010 on applicable law. *Working Report*, **WP 179**(December).

Article 29 Working Party. 2011. Opinion 15/2011 on the definition of consent. *Working Report*, **WP187**.

Article 29 Working Party. 2012. Opinion 05/2012 on Cloud Computing. *Working Report*, **WP 196**(July).

Asia-Pacific Economic Cooperation. 2004. *APEC privacy framework*.

Axelrod, Robert. 1986. An evolutionary approach to norms. *American political science review*, **80**(04), 1095--1111.

Axelrod, Robert M, Axelrod, Robert, & Cohen, Michael D. 2000. *Harnessing complexity: Organizational implications of a scientific frontier*. Basic Books.

Barabási, Albert-László, & Albert, Réka. 1999. Emergence of scaling in random networks. *science*, **286**(5439), 509--512.

Barabási, Albert-László, & Frangos, Jennifer. 2002. *Linked: The New Science Of Networks*. Basic Books.

Beckner, Clay, Blythe, Richard, Bybee, Joan, Christiansen, Morten H, Croft, William, Ellis, Nick C, Holland, John, Ke, Jinyun, Larsen-Freeman, Diane, & Schoenemann, Tom. 2009. Language is a complex adaptive system: Position paper. *Language learning*, **59**(Supplement 1), 1--26.

Begun, James W, Zimmerman, Brenda, & Dooley, Kevin. 2003. Health care organizations as complex adaptive systems. *Advances in health care organization theory*, 253--288.

Beinhocker, Eric D. 2006. *The origin of wealth: Evolution, complexity, and the radical remaking of economics*. Boston: Harvard Business School Press.

Bignami, Francesca. 2007. European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining. *Boston College Law Review*, **48**, 609.

BinBin Wang. 1998. Xian Dai Han Yu Zhong De Ri Yu Wen Ti/Modern Chinese which is imported from Japan. *Shanghai Literature*.

Birnhack, M.D. 2008. The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Report*, **24**(6), 508--520.

Bloche, Maxwell Gregg. 2008. The emergent logic of health law. *California Law Review*, **83**(389).

Bobbitt, P. 2002. *The shield of Achilles: War, peace, and the course of history*. Anchor.

Bowles, S. 2006. *Microeconomics: behavior, institutions, and evolution*. Princeton University Press.

Boyd, Robert. 1988. *Culture and the evolutionary process*. University of Chicago Press.

Briscoe, Edward J. 1998. Language as a complex adaptive system: co-evolution of language and of the language acquisition device. *Pages 3--40 of: 8th Meeting of Comp. Linguistics in the Netherlands*. Citeseer.

Brownlee, Jason, *et al.* . 2007. Complex adaptive systems. *Complex Intelligent Systems Laboratory, Centre for Information Technology Research, Faculty of Information Communication Technology, Swinburne University of Technology: Melbourne, Australia*.

Büllesbach, Alfred. 2010. *Concise European IT Law*. Vol. 1. Kluwer Law International.

Capra, Fritjof. 1997. *The web of life: A new scientific understanding of living systems*. Anchor.

Capurro, R. 2005. Privacy. An intercultural perspective. *Ethics and Information Technology*, **7**(1), 37--47.

Cavoukian, Ann. 2000. Should the OECD Guidelines Apply to Personal Data Online? *In: A report to the 22nd international conference of data protection commissioners*.

Chan, Serena. 2001. Complex adaptive systems. *In: research seminar in Engineering Systems, October*.

Cilliers, Paul. 2002. *Complexity and postmodernism: Understanding complex systems*. Routledge.

Clark, Andy. 1999. Leadership and influence: the manager as coach, nanny and artificial DNA. *Pages 47--66 of:* J.Clippinger (ed), *The Biology of Business:De-Coding the Natural Laws of Enterpries*. Jossey-Bass: San Francisco.

Cohen, B. 2010. German Data Protection Authority Imposes 200000 euros Fine for Targeted Advertising Without Adequate Consent. *Hogan Lovells Law Firmer Press Report*.

Council of Europe. 1950. the Convention for the Protection of Human Rights and Fundamental Freedoms) is an international treaty to protect human rights and fundamental freedoms in Europe. *Official Journal of the EC*.

Council of Europe. 1981. For the Protection of Individuals with Regard to Automatic Processing of Personal Data. *the Council of Europe*, **T.S. No. 108.**(Jan. 28,).

Crocker, Lester G. 1968. *Rousseau's social contract: An interpretive essay*. Press of Case Western Reserve University.

Cuijpers, Colette Mathilde Klasina Christina. 2004. Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn.

Davidoff, Steven M. May 31, 2011. Investor Hunger for Foreign Tech Stocks Overrides Risk. *The New York Times.*

DeCew, Judith. 2012. *Privacy*. Fall 2012 edn.

DeHert, P., & Gutwirth, S. 2006. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. *Pages 61--104 of:* Claes, E., Duff, A., & Gutwirth, S. (eds), *Privacy and the criminal law*. Antwerp/Oxford,: Intersentia.

Dehong Ai, & Zhigang Cai. 2001. How to Improve Chinese Personal Credit System: Lessons from abroad. *Journal of Financial Research*, **3**, 106--115.

Dorff, E.N. 1997. Judaism, business and privacy. *Business Ethics Quarterly*, **7**(2), 31--44.

Dutch Data Protection Authority. 2012. Written opinion on the application of the Wet bescherming persoonsgegevens [Dutch Data Protection Act] in the case of a contract for cloud computing services from an American provider.

EC. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L*, **281**(23/11), 0031--0050.

EC. 1997. Directive 97/66/EC concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. *Official Journal L*, **199 (26))7**.

EC. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. *Official Journal L*, **201**(31).

EC. 2006. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. *Official Journal L*, **105**(13), 04.

EC. 2009. Directive 2009/136/EC of the European Parliament and of the Council of of 25 November 2009 amending Directive

2002/22/EC on universal service and users rights relating to electronic communications networks and services. *Official Journal L*, **337 (18) 12**.

ECJ. 2003. Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk. *European Court Reports*, **Joined cases C-465/00, C-138/01 and C-139/01.**(I-04989).

ECJ. 2006 (30 May). *European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04)*. Joined cases C-317/04 and C-318/04 Protection of individuals with regard to the processing of personal data - Air transport.

ECJ. 2008a (16 December). *Heinz Huber v Bundesrepublik Deutschland*. Case C-524/06 Reference for a preliminary ruling: Oberverwaltungsgericht für das Land Nordrhein-Westfalen - Germany.

ECJ. 2008b (16 December). *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*. Case C-73/07 Reference for a preliminary ruling: Korkein hallinto-oikeus - Finland. Directive 95/46/EC - Scope - Processing and flow of tax data of a personal nature - Protection of natural persons - Freedom of expression.

ECJ. 2009 (May). *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands*. C-553/07 Reference for a preliminary ruling: Raad van State - Netherlands. Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Respect for private life - Erasure of data - Right of access to data and to information on the recipients of data - Time-limit on the exercise of the right to access.

ECJ. 2010 (9 March). *European Commission supported by European Data Protection Supervisor v Federal Republic of Germany*. Case C-518/07.

ECJ. 2011 (24 November). *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) , Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado*. Joined cases C-468/10 and C-469/10.

ECJ. judgment of 6 November 2003). Reference for a preliminary ruling from the Göta hovrätt: Bodil Lindqvist. *ECJ Case Reports*, **C-101/01**.

Edmundson, Andrea, & Global, IGI. 2013. *Cases on Cultural Implications and Considerations in Online Learning*. Information Science Reference.

Einstein, Albert. 1918. Principles of research. *In: Ideas and Opinions*. New York: Random House.

European Commission. 2001. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the community institutions and bodies and on the free movement of such data. *OJ L*, **8**(12 January.).

European Commission. 2003. First report on the implementation of the Data Protection Directive (95/46/EC).

European Commission. 2004. Decision of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor). *Official Journal L*, **12 (17) 1**.

European Commission. 2012. 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*, **0011**.

European Union. 1997. Treaty on European Union (Consolidated Version), Treaty of Amsterdam. *Official Journal of the European Communities*, **2 October**.

European Union. 2012. Charter of Fundamental Rights of the European Union. *Official Journal of the European Communities*, **2012/C 326/02**.

Farrall, K. 2008. Global privacy in flux: Illuminating privacy across cultures in China and the US. *International Journal of Communication*, **2**, 993--1030.

Feyerabend, Paul. 1975. *Against Method: Outline of an Anarchistic Theory of Knowledge*. NLB.

Foster, John. 2005. From simplistic to complex systems in economics. *Cambridge Journal of Economics*, **29**(6), 873--892.

Foster, John. 2006. Why is economics not a complex systems science? *Journal of Economic Issues*, **40**(4), 1069--1091.

Foutouchos, M. 2005. The European Workplace: The Right to Privacy and Data Protection. *Accounting Business & the Public Interest*, **4**(1), 35.

Glachant, Matthieu. 1998. The use of regulatory mechanism design in environmental policy: a theoretical critique. *Sustainability and firms: technological change and the changing regulatory environment. Edward Elgar, Cheltenham*, 179--188.

Glancy, Dorothy. 2000. At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet. *Santa Clara Computer & High Tech. LJ*, **16**, 357.

Goel, Vindu, & Somaiya, Ravi. 2014. With New App, Facebook Aims to Make Its Users' Feeds Newsier. *The New York Times.*, FEB. 3.

Greenleaf, G. 2009. Five years of the APEC Privacy Framework: Failure or Promise? *Computer Law & Security Report*, **25**(1), 28--43.

Grilo, António, Caetano, Artur, & Rosa, Agostinho. 2002. Immune system simulation through a complex adaptive system model. *Pages 675--698 of: Soft Computing and Industry*. Springer.

Hailin Hong. 2007. On the Legislation Idea of Personal Information Protection------Between information protection and freedom of information circulation. *Hebei Law Sicence*, 108--113.

Haldane, Andrew G. 2009. Rethinking the financial network. *Speech delivered at the Financial Student Association, Amsterdam, April*.

Hanhua Zhou. 2006. *Research on the Forefront of the Protection of Personal Information*. Law Press.

Hart, Herbert LA. 1994. *The concept of law*. Oxford University Press.

Hofstede, Geert, Hofstede, Gert Jan, & Minkov, Michael. 1997. *Cultures and organizations*. McGraw-Hill New York.

Hogan Lovells Law Firmer. 2011. Upcoming EU Cloud Strategy Announced: Application of Local Privacy Laws Remain an Issue, To Be Explored at IAPP Navigate on September 14. *Hogan Lovells Law Firmer Press Report*, September 1.

Holland, John H. 2012. *Signals and boundaries: Building blocks for complex adaptive systems*. Mit Press.

Holland, John Henry. 1995. *Hidden order: How adaptation builds complexity*. Basic Books.

Holz, Byron. 2007. Chaos Worth Having: Irreducible Complexity and Pragmatic Jurisprudence. *Minn. JL Sci. & Tech.*, **8**, 303--715.

Hon, W Kuan, & Millard, Christopher. 2008. Cloud computing and EU data protection law Part one: Understanding the international issues. *ComputerWorldUK Cloud Vision blog*, **28 Sep**.

Hornby, A.S., & Zhang, F. 1984. *Oxford Advanced Learner's Dictionary of Current English with Chinese Translation: Niu Jin Xian Dai Gao Ji Ying Han Shuang Jie Ci Dian*. 3 edn. Oxford University Press.

Irish Data Protection Commission. 2011. Facebook Ireland Ltd Report Audit. *Official Journal of the EC*.

Jagodzinski, C.M. 1999. *Privacy and Print: Reading and Writing in Seventeenth-Century England*. University of Virginia Press.

Jentzsch, N. 2007. *Financial privacy: an international comparison of credit reporting systems*. Springer Verlag.

Jentzsch, Nicola. 2005. Best world practices in credit reporting and data protection: lessons for China. *In: International Workshop on Household Credit*.

Jervis, Robert. 1997. *System effects: Complexity in political and social life*. Princeton University Press.

Jia Yao. 2008. Analysis on Interim Measures for the Administration of the Basic Data of Individual Credit Information. *Theory And Practice*.

Jian Zhou. 2001. The Privacy Act of USA and the Protection of Personal Information. *Information Sciences*, **6**(10).

JIPDEC. 2008. DSIA and JIPDEC Launch Mutual Recognition Program. *Japan Information Processing Development Corporation Press Report*, 30 Jun.

Johnson, Jeffery L. 1989. Privacy and the judgment of others. *The Journal of Value Inquiry*, **23**(2), 157--168.

Jolls, Christine. 1998. Behavioral economics analysis of redistributive legal rules. *Vand. L. Rev.*, **51**, 1653.

Jones, Gregory. 2008. Dynamical jurisprudence: law as a complex system. *Georgia State University Law Review*, **24**(4).

Katz, D, Stafford, Derek, & Provins, Eric. 2008. Social Architecture, Judicial Peer Effects and the 'Evolution' of the Law: Toward a Positive Theory of Judicial Social Structure. *Georgia State Law Review*, **23**.

Kay, James J, & Schneider, Eric. 1995. Embracing Complexity the Challenge of the Ecosystem Approach. *Pages 49--59 of: Perspectives on ecological integrity*. Springer.

Kim, Rakhyun E, & Mackey, Brendan. 2013. International environmental law as a complex adaptive system. *International Environmental Agreements: Politics, Law and Economics*, 1--20.

Kuhlen, Rainer. 2004. Informationsethik: Umgang mit Wissen und Informationen in elektronischen Räumen. *Konstanz: UVK Verlagsgesellschaft.--[UTB*, **2454**.

Kuhn, Thomas S. 1962. *The Structure of Scientific Revolutions*. University of Chicago Press.

Kuner, Christopher. 2007. *European data protection law: corporate compliance and regulation*. Oxford University Press.

Kuner, Christopher. 2011. *Regulation of transborder data flows under Data Protection and Privacy Law: past, present and future*. Tech. rept. OECD Publishing.

Kuschewsky, Monika. 2013. What does the revision of the OECD Privacy Guidelines mean for businesses? *MLex Press Report*, **22 October**.

Lessig, Lawrence. 2006. *Code Version 2.0*. Basic Books (AZ).

Levin, Simon A. 1998. Ecosystems and the biosphere as complex adaptive systems. *Ecosystems*, **1**(5), 431--436.

Levin, Simon A. 2000. *Fragile dominion: complexity and the commons*. Basic Books.

Li, Ling, *et al.* . 2010. *Legality, discretion and informal practices in China's courts: a socio-legal investigation of private transactions in the course of litigation*. Ph.D. thesis, Van Vollenhoven Institute. Faculty of Law, Leiden University.

Liming Wang, Ming Xu, & Lixin Yang. 1994. *Ren Ge Quan Fa Xin Lun/ Personality Right*. Jilin People Press.

Maguire, Steve, McKelvey, Bill, Mirabeau, Laurent, & Öztas, Nail. 2006. Complexity Science and Organization Studies. *Page 165 of:* Clegg;, Stewart R, Hardy;, Cynthia, Lawrence;, Tom, & Nord, Walter R (eds), *The sage handbook of organization studies*. SAGE.

Marmor, Andrei. 2011. The Nature of Law. *In:* Zalta, Edward N. (ed), *The Stanford Encyclopedia of Philosophy*.

Maskin, Eric S. 2008. Mechanism design: How to implement social goals. *The American Economic Review*, **98**(3), 567--576.

Mattei, Ugo. 1997. Three Patterns of Law: Taxonomy and Change in the World's Legal System. *The American journal of comparative law*, **45**.

Maxwell, Winston, & Souza, Lionel De. 2013. French CNIL Annual Report Shows Increased Complaints, Audits, Sanctions. *Hogan Lovells Law Firmer Press Report*, **APRIL 30TH,**.

McDaniel Jr, Reuben R., Lanham, Holly Jordan, & Anderson, Ruth A. 2009. Implications of Complex Adaptive Systems Theory for the Design of Research on Health Care Organizations. *Health care management review*, **34**(2), 191--199.

McFarland, Michael. 2012. *Information Privacy: A Case Study and Commentary*. http://ethics.iit.edu/eelibrary/biblio/information-privacy-case-study-and-commentary.

Meadows, Donella H. 2008. *Thinking in systems: A primer*. Chelsea Green Publishing.

Merriam-Webster Inc. 2004. *Merriam-Webster's collegiate dictionary*. Merriam-Webster.

Michaels, Ralf. 2005. The functional method of comparative law. *Pages 339--382 of:* Mathias Reimann, Reinhard Zimmermann (ed), *THE OXFORD HANDBOOK OF COMPARATIVE LAW*. Oxford University Press.

Milgrom, Paul R, North, Douglass C, *et al.* . 1990. The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs. *Economics & Politics*, **2**(1), 1--23.

Miller, John H, & Page, Scott E. 2009. *Complex Adaptive Systems: An Introduction to Computational Models of Social Life: An Introduction to Computational Models of Social Life*. Princeton University Press.

Mitchell, M. 2009. *Complexity: a guided tour*. Oxford University Press, USA.

Moerel, Elise Marie Leonore. 2011. *Binding Corporate Rules: Fixing the Regulatory Patchwork of Data Protection*.

Molyneaux, Brian L, & Stone, Peter G. 2004. Privacy and community through medieval material culture. *In: The Presented Past: Heritage, Museums and Education*. Routledge.

Mookherjee, Dilip, & Png, Ivan PL. 1992. Monitoring vis-a-vis Investigation in Enforcement of Law. *The American Economic Review*, 556--565.

National People's Congress. April 12, 1986 and effective as of January 1, 1987. General Principles of the Civil Law of the People's Republic of China. *Order No.37 of the President of the People's Republic of China*.

Newman, M. E. J. 2011. Complex Systems: A Survey. *Am. J. Phys.*, **79**, 800--810.

North, Douglass C. 1993. The new institutional economics and development. *EconWPA Economic History*, **9309002**.

Nunn, Nathan. 2009. The importance of history for economic development. *Annual Review of Economics*, **1**(1), 65--92.

Oakleaf, David. 2005. Review of: Patricia Meyer Spacks: Privacy: Concealing the Eighteenth-Century Self. *Eighteenth-Century Fiction*, **18**(1), 8.

Odlyzko, A. 2004. Privacy, economics, and price discrimination on the Internet. *Economics of information security*, 187--211.

Organization for Economic Cooperation and Development. 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD*, **C(80)58/FINAL**(September 23).

Organization for Economic Cooperation and Development. 2013. Revised guidelines governing the protection of privacy and transborder flows of personal data (the ``Revised Guidelines"),. *OECD Officials*.

Ottino, Julio M. 2003. Complex systems. *AIChE Journal*, **49**(2), 292--299.

Otto, Jan Michiel. 2000. Conclusion: A Comparativist's Outlook on Law-Making in China. *In: Law-Making in the People's Republic of China*. Kluwer Law International.

P Klaus Schwab, Alan MarcusJustin, Rico Oyola, & Hoffma, William. 2011 (January). *Personal Data Ecosystem: The Emergence of a New Asset Class*. World Economic Forum.

Page, Scott E. 2008. *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies (New Edition)*. Princeton University Press.

Page, Scott E. 2012. A complexity perspective on institutional design. *Politics, Philosophy & Economics*, **11**(1), 5--25.

Pagel, Mark. 2012. *Wired for culture: origins of the human social mind*. WW Norton & Company.

Parsons, Mark. 2013 (July). *Briefing: China brings in new rules for online personal data*.

Peltoniemi, Mirva, & Vuori, Elisa. 2004. Business ecosystem as the new approach to complex adaptive business environments. *Pages 267--281 of: Proceedings of eBusiness Research Forum*.

People's Bank Of China. 2005a. Interim Measures for the Administration of the Basic Data of Individual Credit Information. *Order of the People's Bank of China*, **Order No.3**(18 Auguest).

People's Bank Of China. 2005b. PBOC Procedures for Handling Disputes about the Individual Credit Information Database. 1 October.

People's Bank Of China. 2006. Procedures for Searching one's Own Credit Report from the Individual Credit Information.

Phister Jr, Paul W. 2010. Cyberspace: the ultimate complex adaptive system. *The International C2 Journal*, **4**(2), 1--30.

Picker, Randal C. 1997. Simple games in a complex world: A generative approach to the adoption of norms. *The University of Chicago Law Review*, 1225--1288.

Pistor, Katharina, & Xu, Cheng-Gang. 2004. Beyond law enforcement-governing financial markets in China and Russia. *Pages 167--189 of:* Kornai, János, Rothstein, Bo, & Rose-Ackerman, Susan (eds), *Creating Social Trust in Post-Socialist Transition*. Palgrave Macmillan.

Pistor, Katharina, & Xu, Chenggang. 2002a. Fiduciary Duty in Transitional Civil Law Jurisdictions Lessons from the Incomplete Law Theory. *ECGI-Law Working Paper*.

Pistor, Katharina, & Xu, Chenggang. 2002b. Incomplete law. *NYUJ Int'l L. & Pol.*, **35**, 931.

Pistor, Katharina, & Xu, Chenggang. 2006. *The Challenge of Incomplete Law and H ow Diferent Legal Systems respond*.

Post, David, & Eisen, Michael. 2000. How long is the coastline of law? Thoughts on the fractal nature of legal systems. *Journal of Legal Studies*, **29**, 545.

Poullet, Yves, & Gutwirth, Serge. 2008. The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of'reflexive governance'? *Pages 570--610 of:* Asinari, Verónica Perez, & Palazzi, Pablo (eds), *Défis du droit à la protection de la vie privée .Challenges of privacy and data protection law - Challenges of privacy and data protection law*. Bruylant.

Qin Xie. 2006. Legal System of Personal Information Protection In Japan and Its Enlightenment. *Political Sicence and Law*, **6**, 152--156.

Qiong Wang, & Zongxian Feng. 2006. Discussion On Personal Credit System in China. *Business Economics and Administration*, **2**, 011.

Rappaport, John. 2014. Second-Order Regulation of Law Enforcement.

Reding, Viviane. 2012. The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age. *In: Innovation Conference Digital, Life, Design Munich*, vol. 22.

Rettman, Andrew. 2013. *NSA and GCHQ mass surveillance is violation of European law, report finds*.

Rouse, William B. 2008. Health care as a complex adaptive system: implications for design and management. *Bridge Washington National Academy of Engineering*, **38**(1), 17.

Ruhl, JB. 1997. Thinking of environmental law as a complex adaptive system: how to clean up the environment by making a mess of environmental law. *Houston Law Review*, **34**(4).

Ruhl, JB. 2005. Regulation by adaptive management-is it possible. *Minn. JL Sci. & Tech.*, **7**, 21.

Ruhl, J.B. 2008. Law's Complexity: A Primer. *Georgia State University Law Review*, **24**, 885--1097.

Ruhl, JB. 2009. The Co-Evolution of Sustainable Development and Environmental Justice: Cooperation, Then Competition, Then Conflict. *Pages 1998--1999 of: Duke University Law & Policy Forum*, vol. 9.

Ruhl, JB, & Ruhl, Harold. 1997. The Arrow of the Law in Modern Administrative States: Using Complexity Theory to Reveal the Diminishing Returns and Increasing Risks the Burgeoning of Law Poses to Society. *UC Davis Law Review*, **30**.

Ruhl, John B. 1996a. Complexity theory as a paradigm for the dynamical law-and-society system: A wake-up call for legal reductionism and the modern administrative state. *Duke Law Journal*, 849--928.

Ruhl, John B. 1996b. The fitness of law: Using complexity theory to describe the evolution of law and society and its practical meaning for democracy. *Vanderbilt Law Review*, **49**.

Ruhl, John B, Kraft, Steven E, & Lant, Christopher L. 2007. *The law and policy of ecosystem services*. Cambridge Univ Press.

Schelling, T.C. 1969. Models of segregation. *The American Economic Review*, **59**(2), 488--493.

Schneider, Marguerite, & Somers, Mark. 2006. Organizations as complex adaptive systems: Implications of complexity theory for leadership research. *The Leadership Quarterly*, **17**(4), 351--365.

Shi, Xiaohong. 2008. Gong Si Zhi Li Jie Gou De Bi Jiao Lun Shi/Comparative Study on Corporate Governance in China. *Economics in China*, **9**.

Solove, Daniel J. 2006. A brief history of information privacy law. *PROSKAUER ON PRIVACY, PLI,*.

Spacks, P.A.M. 2003. *Privacy: concealing the eighteenth-century self*. University of Chicago Press.

Stefan.S. 2012. German DPAs Issue Rules for Cloud Computing Use. *HLdataprotection*.

Steffen, Will, Sanderson, Regina Angelina, Tyson, Peter D, Jäger, Jill, Matson, Pamela A, Moore III, Berrien, Oldfield, Frank, Richardson, Katherine, Schellnhuber, Hans Joachim, Turner, Billie L, *et al.* . 2006. *Global change and the earth system: a planet under pressure*. Springer.

Swire, Peter. 2012. Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment. *NCL REV.*, **90**, 1371--1395.

Ter Haar, Barend J. 2009. *Het hemels mandaat: de geschiedenis van het Chinese keizerrijk*. Amsterdam University Press.

Tesfatsion, Leigh. 2003. Agent-based computational economics: modeling economies as complex adaptive systems. *Information Sciences*, **149**(4), 262--268.

The Economist. 2007. The long march to privacy. *The Economist*, **January 6**.

the European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights. 2013. *Handbook on European data protection law*. Publications Office of the European Un.

Tribe, Laurence H. 1989. The curvature of constitutional space: What lawyers can learn from modern physics. *Harvard Law Review*, 1--39.

Tussey, Deborah S. 2005. Music at the Edge of Chaos: A Complex Systems Perspective on File Sharing. *Loyola University Chicago Law Journal*, **37**, 147--212.

Van Rooij, Benjamin. 2006. *Regulating land and pollution in China: lawmaking, compliance, and enforcement: theory and cases*. Amsterdam University Press.

Velkley, Richard. 2002. The Tension in the Beautiful: On Culture and Civilization in Rousseau and German Philosophy. *Being after Rousseau: Philosophy and Culture in Question*.

Warren, Samuel D, & Brandeis, Louis D. 1890. The right to privacy. *Harvard law review*, **4**(5), 193--220.

Watts, Duncan J. 2012. *Everything Is Obvious: How Common Sense Fails Us*. Random House LLC.

Watts, Duncan J, & Strogatz, Steven H. 1998. Collective Dynamics of Small-World Networks. *nature*, **393**(6684), 440--442.

Wendell Holmes Jr., Oliver. 1897. The Path of the Law. *Harvard Law Review*, **10**(472), 403--6.

Westin, Alan F. 1968. Privacy and freedom. *Washington and Lee Law Review*, **25**(1), 166.

Whitman, James Q. 2004. The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, 1151--1221.

Widmer, Ursula. 2009. Cloud computing and data protection. *Law Business Research*.

Wikipedia. 2007. *Dalian Software Park*.

Wikipedia. 2010. *Community*. http://en.wikipedia.org/wiki/Community.

Wu, Handong. 2009. Zhong Guo Zhi Shi Chan Quan Zhi Du De Ping Jia He Fan Si (Assessment on China's Interllectual Property Institution). *China's Law*, **1**.

Xi Ai. 2006. *Studies on legal institutions over personal credit report issues*. Ph.D. thesis, China University of Political Science and Law.

Xie, Lingli, & Zhang, Jun. 2010. Zhong Guo Yi Zhi Du Li Dong Shi Zhi Du De Fan Si (Reflecting on China's imported independent director institution. *China's Lawyers*, **8**.

Xinbao Zhang. 1997. *Yin Si Quan De Fa Lv Bao Hu/ Legal Protection over privacy right*. People Press.

Xinbao Zhang. 2007. Ge Ren Shu Ju Li Fa De Xian Zhuang Yu Zhan Wang/ The Present Situation of Data Protection Legislation in China and Proposal for Reform. *Chinese Law*, **3**.

Xiulan Zhang. 2005. Models for web-privacy protection: cases study on Europe and America. *Researches on Library Sicence*, **5**, 86--88.

Xu, Chenggang, & Pistor, Katharina. 2002a. Incomplete Law: Conceptual and Analytical Framework and its Application to the Evolution of Financial Market Regulation". *Journal of International Law and Politics*, **35**, 931--1013.

Xu, Chenggang, & Pistor, Katharina. 2002b. Law enforcement under incomplete law: Theory and evidence from financial market regulation. *Columbia Law and Economic Working Paper*.

Yin, Jiliang. 2002. Lun Zhong Guo Dui Kang Zhi Yi Zhi Shi Bai De Yuan Yin/On the Reason of failure in Transplanting Confrontation System to China. *Journal of Lianniang Administration College Of Police and Justice*, **4**, 46--50.

Yue Wang, & Jian Xiong. 2003. China's Strategies Credit Reporting Industry Against the EU Directive onData Protection. *Commercial Research*, **1**, 037.

Zhang, Kunbei, & Schmidt, Aernout. 2013. Looking at China's Facebook (RenRen) through the Lens of European Data Protection Principles. *Available at SSRN 2257907*.

Zweigert, Konrad, & Kötz, Hein. 1996. *Einführung in die Rechtsvergleichung: auf dem Gebiete des Privatrechts*. Mohr Siebeck.

Zweigert, Konrad, & Kötz, Hein. 1998. An Introduction to Comparative Law, 3. *Aufl., New York*.

Zwenne, Gerrit-Jan. 2013. *Diluted Privacy Law*. Universiteit Leiden.

Summary

Summary of: Can Chinese Legislation on Informational Privacy Benefit from European Experience?

This thesis is concerned with data protection legislation in China. The primary objective is to examine the advisability of cloning European data protection law and transplant it into China. In order to address the issue, I explored it from several perspectives.

In Chapter 2, using documentary evidence and interview results, I compared the material laws over data protection of the European general system with the Chinese credit reporting system, and provided a positivist assessment of the data protection levels in the two regions. In doing so I employed a set of measure sticks that I derived from the 2013 version of the OECD guidelines. I focused on the differences (not on the matches) between the two jurisdictions. These differences are marked. Generally, the comparison reveals that European data protection laws cover the principles of informational privacy as embedded in OECD 2013 far more complete than Chinese data-protection laws do (when available at all). Considering the Chinese credit reporting database CRC in Chapter 2 thus provides evidence that this database, were it operational in Europe, would be in danger of being deemed illegal. I pointed out that the CRC's operations violate three types of privacy guarantees, valid under European data protection law.

The first violation type concerns the data subject's rights. Two elements in the OECD 2013 are recognized by both regions. Yet, the right to object, which can be considered a species of the right to challenge is a peculiarity of European data protection law and is not observed in Chinese laws. The second type of violations concerns the data controllers' obligations. The Directive recognizes all

OECD principles on the data controllers' obligations, while Chinese Credit Reporting Laws miss the collection limitation principle, the use limitation principle, the openness principle and the accountability principles. These omissions are serious indeed. The third violation type concerns the procedural issues. Implementation principles are largely recognized by European data protection law, except the national strategy, which was only incorporated into the OECD guidelines in 2013. Yet, China misses most of the procedural core issues. Only three principles are found in China's system, including "reasonable means for the individual to exercise their rights, adequate sanctions and complementary measures." Again, Chinese positive laws on data protection for credit reporting lag seriously behind Directive 95/46/EC when looked at through the lens of OECD 2013. Therefore, under China's legal arrangements Chinese CRC database use might very well be considered legal. Yet under European law the very same database use would clearly be illegal.

Based on the above comparison, I conclude that if China's policymakers introduce European data protection law, it can upgrade China's legal arrangements, considered from a positivist perspective. Consequently, and assuming the "all other things being equal" assumption, European data protection law can serve as a point of departure for improving China's legal arrangements. But since we know that all other things are not equal between Europe and China, I submit that further investigations are needed. They may suggest improvements to the plan to directly clone and transplant legal texts from Europe into China.

In Chapter 3, I investigated the evolution of privacy and informational privacy in Europe and China as these evolutionary paths have certainly unwound under different conditions. I began the Chapter by showing some considerations on the analogies between languages, cultures and legal systems: like languages, legal systems evolve under the pressures of the cultures they serve and are part of - consequently, by looking at the developments in their cultural environments, how the differences between legal systems may be better understood - both in the book (the positivist perspective) and in action (the realist perspective). Based on the analysis I conclude that differences in culture helped shape differences in data protection law. As the discussion of European data protection law in the Chapter demonstrates, it has

emerged from the (functional) roots of European privacy conceptions that came to flourish under the pressures of contingencies in the environment. These functional roots are there first, and are soon followed by the emergence of the first legal forms of privacy protection by law. Privacy functions and laws kept on co-evolving in Europe and culminated after World War II not only in elaborate functional (and thus instrumental) legislation, but also in the rather Kantian idea of privacy as an intrinsically individualist human value (as expressed in art. 12 of the UDHR). In China, the current legal arrangement over data protection issues grows directly out of China's collectivist culture, which only rewards the instrumental-goods aspect of privacy. The findings in this Chapter suggest that China's policymakers should realize that European data protection law is being transplanted neither from, nor to jurisdictions with culturally blank or neutral slates. Instead, both Europe and China have pre-existing sets of data protection laws and privacy- related cultural norms. The cultures that embed privacy practices are complicated and have far-reaching implications for the ways that data protection laws are and will be understood, and on how they will be received, upheld and enforced. Therefore, I suggest that China will adopt a cautious approach to the realization of the legal transplantation plan.

At the end of Chapter 3, I have established differences between two positive law arrangements and between the two cultures involved. There is a lot that at first sight seems a valid candidate for importation from the EU to China. Yet, there are risks. For instance, both technical innovation and the uptake of social media services are highly dynamic and tend to make adequate legislation difficult. So in order to make an informed choice about what to import and what not to import, it is useful to analyze how the legal systems under discussion support (or undermine) the recipient legal system's resilience in a changing environment.

This very issue is my motivation for Chapter 4's excursion into Incomplete Law theory. In order to impose an interpretation on the phenomenon in question, I deployed the theory of Incomplete Law, created by Xu and Pistor, for the analysis. It showed that European data protection laws, as represented by Directive 95/46/EC, are incomplete. The reasons can be categorized in three ways. First, the generality of the Directive makes it difficult to provide rules that are

specific enough; second, technology, that strongly influences data protection law's subject matter, changes at high speed and therefore renders the Directive more incomplete as it lags further behind; and finally, lawmakers are unable to foresee all future contingencies, also those contingencies that emerge through mass adoption of innovative services. Particularly, technology's changes strongly challenge even the short-term "fit" of the Directive. The Directive 95/46/EC was designed to regulate the data processing technologies a couple of decades ago and thus focused on "old" problems while digital technologies have experienced radical revolutions. New advanced digital technologies were being introduced into public communications networks and in the community. Access to digital mobile networks has become available and affordable for the public at large. These digital networks have huge opportunities for processing personal data. All these changes, thus, required frequent adaptations of the law for it to remain effective. This led to problems with the law's focus and mechanisms to remain connected to reality.

How does Europe arrange to face the resulting incompleteness? European policymakers created a new role, the data protection authority who assumes residual LMLEP (law making and law enforcing powers), in order to make interventions possible for mitigating the problems of incompleteness. In Chapter 4, I focused on the Article 29. Working Party and the national data-protection authorities that take significant roles in regulating and law enforcement for reducing incompleteness. The investigation confirmed that the emergence of data authorities responded to the problem of under-enforcement caused by highly incomplete law. Data authorities are more flexible than legislative agencies on adapting the law to a changed technical environment (although the scope of their lawmaking rights is limited), since their swift reaction time allows them to better keep up with the fast pace of technology. And Data authorities are more proactive than courts, since they can initiate actions to enforce data protection law in situations where courts, by design, have to wait for a file to be suit.

Consequently, the findings in Chapter 4 reject the assumption (which China's policymakers nurse) that European data protection law is complete, and that the transplantation scheme can be confined to material, positive data protection laws. I show that, beyond their expectations, issues of dynamics in technology and in mass use of social media are not trivial and require measures that safeguard the availability of a highly informed and highly responsive authority that has sufficient residual LMLEP to guard the law's incompleteness will not become intolerable. I conclude that legal transplantation as envisaged will not ensue effective consequences unless a competent regulatory authority is in place.

As a follow up to this conclusion, I analyzed in Chapter 5 what gaps between the law in the books and the law in action the EU data authorities have to face when they regulate American Facebook or its Chinese sibling (RenRen). It is clear from the discussion that RenRen's current practices are neither in compliance with European Data Protection principles, nor with EU data protection laws. Consequently, if RenRen would open its EU headquarters in any member state in Europe, the firm may receive multiple complaints about its data protection practices. Regarding Facebook, I conclude that, even though its current practices seem to comply with EU data protection law, they do not fully comply with European Data Protection principles. This leads to the insight that what is acceptable to EU privacy laws needs not be acceptable through the lens of the Working Party's principles. On the one hand, this means that the level of data subjects' protection may increase substantially to a higher level, dependent of the data regulators' performance (as such regulators populate the Working Party). On the other hand, the same finding shows that it is difficult to enforce the law rigorously in order to influence the data protection behavior of a world-leading Social Network Service player like Facebook. In other words, the efficacy of the law in action is complex, and difficult to anticipate by looking at the law and its enforcing officials in isolation.

In China, the tension between the efficacy of law in action and the optimal standard of legal design is mounting, at least at the outset of the data protection transplantation plan. The incompleteness of data protection law in China is more severe than in Europe, as many of such laws simply are not there at all and most of such laws that exist have been enacted recently. The incompleteness is also more severe in China than in Europe, because law enforcement agencies simply lack the experience that accompanies the adjudication in a substantial number and variety of cases. This is particularly relevant to the MIIT's performance. Under such conditions, mechanisms of

law enforcement cannot be expected to work effectively, at least not during the early period of the data protection institution's development. Thus, Chinese legislators face a predicament: they really need to develop a European type of data protection system, and yet they lack the instruments to do so. Worse yet, recipes for law enforcement that have historically worked elsewhere may not help in the short-to-medium term in China.

Now, I can answer my main research question: "Is China's transplantation plan advisable?" My approach concludes that it is not feasible to solely transplant EU data protection law (as China's transplantation proposal suggests), unless an equivalent to the EU data authorities is included. Chinese Data protection law is less strong than EU privacy law (Chapter 2). However, cultural differences (Chapter 3) and inherent incompleteness of the EU law (Chapter 4), coupled with the fact that institutional arrangements in the EU that reduce incompleteness will not work in China (Chapter 5) make me conclude that of the effectiveness of the an imported European data protection law cannot be expected too much.

In the Second Part of my research project I explore what additional opportunities can be discerned when adopting the perspective offered by complexity theory, and when considering the subject matter of data-protection regulation to be a complex adaptive system (hereinafter CAS). This change of perspective is because the phenomena that I encountered in Chapters 3-5 and that characterize the subject matter for personal-data protection can be summarized with six characteristics: they are networked/connected, they lead to emergent interdependencies, now and then showing path dependent, dynamic, complex and adaptive behavior.

In this Second Part, I first identified the subject matter of data protection law to be a Personal Data Community (PDC). Then, I investigated, through 4 combining the PDC with the knowledge and experiences from different classes of CAS, whether data protection law's subject matter, as a network of data users, exhibits the characteristics of a CAS and what these imply for the future of data protection law. Through using some key CAS-properties and relating them to our PDC and its ecology, we are "informed" that these characteristics apply to the PDC and that thus the PDC can be understood as a CAS. From the CAS perspective, the human-created PDC is a large

and dynamic system of interacting data users networked in a particular pattern of organization from which arises the ability to adapt to internal and external changes by self-organization, emergence and co-evolution/learning.

My findings brought challenges to legal arrangements over data protection issues, since these try to tame a CAS. Evidence taken from case studies published in this book as well as other sources suggested that data protection law's subject matter is (possibly) quite different from other law's subject matters. It faces critical transitions all the time in practice. Thus - as we continuously have to regulate situations that the legislature could (and did) not imagine when framing the law - the purposes of data protection law, the reasons for its existence and the modalities of its regulation are requiring methods quite different from those that focus on the interpretation of material laws.

I suggest that future data protection law may fruitfully build on CAS- theory's recommendations: as Ruhl (1997) minded us, the problems presented in a CAS only can be addressed unless you think like a complex adaptive system. Thus, the problem needing attention is to adjust data protection law to tally with its subject matter. But how?

Multidisciplinary CAS-theory can help legal scholarship to better inform the legislature on expected risks and outcomes of legislative interventions that address CAS-"dots." In this Second Part, I suggested some strategies that can be adopted to help legal researchers capture complex adaptive phenomena in the PDC when arranging or regulatory frameworks. These strategies include: (i) the evaluation of expected benefit of legal intervention, (ii) understanding the environment, (iii) the special functionalities of hubs, (iv) understanding agents' incentives and (v) considering the forces of incentives vs learned behavior. I think that legal scholarship needs to establish and protect its own identity boundaries in multidisciplinary settings by explicitly defending its proper position as addressing autonomous behavior by responsible agents. Where social scientists are on the look-out for knowledge that will nudge such agents into behaving in a way that they want, often unconsciously, legal scholars are interested in knowledge that will support responsible agents to make autonomous behavioral choices, while aware of legal and cultural norms -- of knowledge that can be learned. A legislator will presumably be best informed, I think, when both types of knowledge and their inter-

actions can be made available in a coherent framework. Complexity theory is a serious candidate for providing it.

The picture of the data protection law's subject matter as a CAS is an ongoing rather than completed construction. Notwithstanding that our understandings on CAS theory is in a state of evolution, our efforts thus far have already served to deepen our understanding of many problems that troubled data protection law. And they have operated as checks against some of the mistakes of current data protection laws. It is against this background that I expect that regulation over data-protection issues stand to benefit from being informed through the lens of CAS theory.

Nederlandse Samenvatting

Samenvatting van: Kan Chinese wetgeving betreffende informationele privacy profiteren van de Europese ervaring?

Dit proefschrift gaat over regelgeving ten aanzien van de bescherming van persoonsgegevens in China. Het primaire doel van mijn onderzoek was om te onderzoeken of het is aan te raden dat China de Europese wetgeving inzake de gegevensbescherming overneemt en implementeert. Ik heb dit onderzoek gedaan vanuit verschillende perspectieven.

In hoofdstuk 2 heb ik, gebruikmakend van relevante documentatie en interviewresultaten, de Europeesrechtelijke materiële persoonsgegevensbeschermingswetgeving vergeleken met het Chinese systeem van kredietregistratie, en heb, vanuit een positivistisch perspectief, van beide het beschermingsniveau beoordeeld. Daarbij heb ik meetinstrumenten gehanteerd die ik heb afgeleid uit de OESO-richtlijnen (versie 2013). De focus lag op de verschillen tussen de twee betreffende rechtsgebieden (en niet op de overeenkomsten). Deze verschillen zijn typerend. Over het algemeen blijkt uit de vergelijking dat de Europese wetgeving betreffende de persoonsgegevensbescherming de beginselen van de informationele privacy zoals ingebed in OESO 2013 veel vollediger dekt dan de Chinese wetten (voor zover die er überhaupt zijn). Er bestaat, aldus beschouwd, een grote kans dat de databank van het Chinese *Credit Reporting Center* (CRC), ware deze operationeel in Europa, illegaal zou worden

bevonden. Ik vestig er de aandacht op dat het CRC met zijn activiteiten drie soorten privacywaarborgen schendt, die alle drie wel zijn opgenomen in de Europese wetgeving. De eerste soort schending betreft de rechten van de betrokkene. Twee elementen uit OESO 2013 zijn vastgelegd in beide rechtsregelingen. Maar daarentegen is het recht om bezwaar te maken, dat kan worden beschouwd als een species van het recht om iets aan te vechten - typerend voor de Europese wetgeving inzake gegevensbescherming - niet opgenomen in de Chinese regelingen. De tweede soort schending betreft de verplichtingen van de voor de verwerking verantwoordelijken. Zo erkent de EU-Richtlijn wel alle OESO-beginselen inzake de verplichtingen van de voor de verwerking verantwoordelijken, terwijl de Chinese Credit Reporting regelgeving de beginselen van gelimiteerd verzamelen, van gelimiteerd gebruik, het transparantiebeginsel en het aansprakelijkheidsbeginsel missen. Dit zijn echt ernstige omissies. De derde soort schending betreft procedurele aspecten. Implementatiebeginselen zijn grotendeels erkend door de Europese gegevensbeschermingswetgeving, met uitzondering van de nationale strategie, die alleen was opgenomen in de OESO-richtlijnen 2013. China echter mist het grootste deel van de procedurele kernaspecten. Er zijn maar drie beginselen te vinden in het Chinese systeem, te weten: "redelijke middelen voor het individu om hun rechten uit te oefenen, adequate sancties en aanvullende maatregelen". Nogmaals, in het licht van OESO 2013 loopt Chinees positief recht inzake gegevensbescherming voor de krediet registratie serieus achter bij Richtlijn 95/46/EG. Daarom kan het gebruik van de Chinese CRC-database vanuit het Chinese rechtssysteem heel goed worden beschouwd als legaal. Vanuit het Europese recht zou datzelfde gebruik echter duidelijk illegaal zijn. Op basis van de bovenstaande vergelijking, concludeer ik dat als de Chinese beleidsmakers Europese gegevensbeschermingswetgeving invoeren, dit vanuit een positivistisch perspectief een verbetering is van de juridische regelingen daarvan in China. Daarom, en uitgaande van de *ceteris paribus* aanname, kan Europese gegevensbeschermingswetgeving dienen als uitgangspunt voor het verbeteren van juridische regelingen in China. Maar aangezien we weten dat *ceteris* niet *paribus* zijn

in Europa en China, merk ik op dat verder onderzoek nodig is waar het gaat om de onderbouwing van de gedachte dat de wetgeving vanuit Europa in China direct kan worden overgenomen en geïmplementeerd.

In hoofdstuk 3 heb ik onderzoek gedaan naar de evolutie van de persoonlijke levenssfeer en de informationele privacy in Europa en in China, aangezien deze verschillende paden hebben gevolgd onder uiteenlopende omstandigheden. Ik begon dit hoofdstuk met een aantal overwegingen over analogieën tussen talen, culturen en rechtssystemen: evenals talen, evolueren juridische systemen ook onder druk van de culturen die ze dienen en waarvan ze deel uitmaken. Door te kijken naar de ontwikkelingen in hun culturele omgeving, kunnen de verschillen tussen de rechtsstelsels beter worden begrepen - zowel het recht in de boeken (*law in the books*, het positivistische perspectief) als het recht in actie (*law in action*, het realistische perspectief). Op basis van mijn analyse concludeer ik dat cultuurverschillen van invloed zijn geweest op de verschillen in gegevensbeschermingswetgeving. Zoals de discussie over Europese wetgeving inzake gegevensbescherming in dit hoofdstuk laat zien, is deze opgekomen vanuit de (functionele) wortels van het Europese privacy-idee dat tot bloei kwam onder de druk van gebeurtenissen in de omgeving. Deze functionele wortels zijn er het eerst, en worden al snel gevolgd door de opkomst van de eerste juridische vormen van wettelijke privacybescherming. Privacyfuncties en -wetten bleven in Europa co-evolueren en culmineerden na de Tweede Wereldoorlog niet alleen in gedetailleerde functionele (en dus instrumentele) wetgeving, maar ook in het tamelijk Kantiaanse idee van privacy als een intrinsiek individualistische menselijke waarde (zoals uitgedrukt in art. 12 UVRM). In China, komt de huidige wettelijke regeling op het gebied van gegevensbeschermingsaangelegenheden rechtstreeks voort uit de Chinese collectivistische cultuur, die alleen het instrumentele aspect van privacy (h)erkent. De bevindingen in dit hoofdstuk ondersteunen de stelling dat de Chinese beleidsmakers zich moeten realiseren dat de Europese gegevensbeschermingswetgeving geenszins wordt overgezet vanuit, noch naar cultureel blanco of neutrale jurisdicties. Zowel Europa als China hebben reeds be-

staande wetgeving inzake gegevensbescherming en hebben reeds gevormde privacy-gerelateerde culturele normen. De culturen waarin de praktijk van de privacy is ingekaderd zijn ingewikkeld en hebben verstrekkende gevolgen voor de manier waarop de wetgeving inzake gegevensbescherming wordt en zal worden begrepen, en voor hoe deze zal worden ontvangen, nageleefd en gehandhaafd. Daarom stel ik voor dat China een voorzichtige benadering volgt waar het gaat om de realisatie van het plan om wetgeving over te nemen.

Aan het einde van hoofdstuk 3 heb ik de verschillen vastgesteld tussen de twee positiefrechtelijke regelingen en de twee betrokken culturen. Er is veel dat op het eerste gezicht een geldige kandidaat lijkt om te worden ingevoerd uit de EU naar China. Maar er zijn ook andere dan culturele risico's. Bijvoorbeeld, zowel technische innovatie als de toepassing van sociale media-diensten zijn zeer dynamisch en hebben de neiging om adequaat wetgeven te bemoeilijken. Om een weloverwogen keuze te maken aangaande wat over te nemen en wat niet, is het nuttig om te analyseren hoe in de betreffende jurisdicties de veerkracht van het ontvangende rechtssysteem wordt ondersteund (of ondermijnd) in een veranderende omgeving. Het is dit punt in het bijzonder dat voor mij de motivatie vormt voor de aandacht die ik in hoofdstuk 4 geef aan de Incomplete Law Theorie.

Teneinde een interpretatie vast te stellen van het fenomeen in kwestie, heb ik voor de analyse de Incomplete Law Theorie van Xu en Pistor benut. Daaruit kwam naar voren dat Europese gegevensbeschermingsregelgeving, zoals Richtlijn 95/46/EG, onvolledig (incomplete) is. De redenen daarvoor vallen in drie categorieën uiteen: ten eerste: de algemeenheid van de richtlijn bemoeilijkt het geven van regels die specifiek genoeg zijn; ten tweede: de technologie, die sterk van invloed is op het onderwerp van de gegevensbeschermingswetten, verandert pijlsnel en maakt daardoor de richtlijn incompleter omdat deze hier ver bij achterblijft; en tenslotte: wetgevers zijn niet in staat om alle mogelijke toekomstige ontwikkelingen te voorzien, ook niet die onvoorziene ontwikkelingen die ontstaan door de massale acceptatie en het gebruik van innovatieve diensten. De technologische veranderingen zijn met name een groot probleem voor de toepasselijkheid op de korte termijn van de richtlijn. Richtlijn 95/46/EG is enige decennia terug ontworpen om gegevensverwerkingstechnologieën te reguleren en is dus gericht op de "oude" problemen, terwijl zich op het vlak van de digitale technologieën radicale omwentelingen hebben voorgedaan. Nieuwe geavanceerde digitale technologieën hebben hun intrede gedaan in publieke communicatienetwerken en in de samenleving. Toegang tot digitale mobiele netwerken is beschikbaar en betaalbaar geworden voor het grote publiek. De digitale netwerken bieden enorme mogelijkheden voor de verwerking van persoonsgegevens. Al deze veranderingen vereisen daarom frequente aanpassingen van de wet wil deze effectief blijven. Dit heeft geleid tot problemen met het aan blijven passen van de focus en werkbaarheid van de wet aan de realiteit.

Wat deed Europa aan de hieruit voortkomende onvolledigheid? Europese beleidsmakers creëerden een nieuwe functie, die van een "autoriteit voor gegevensbescherming" die aanvullende regelgevende- en rechtshandhavingsbevoegdheden (LMLEP, law making and law enforcing powers) kreeg toebedeeld, om te kunnen ingrijpen bij het terugdringen van problemen die worden veroorzaakt door de onvolledigheid. In hoofdstuk 4 ga ik nader in op de Artikel 29 Werkgroep en de nationale autoriteiten voor gegevensbescherming die zo een belangrijke rol spelen bij de regulering en rechtshandhaving met het oog het verminderen van de onvolledigheid. Het onderzoek bevestigde dat de komst van deze autoriteiten een reactie vormde op het handhavingsprobleem dat werd veroorzaakt door het zeer onvolledige recht. De gegevensbeschermingsautoriteiten zijn flexibeler dan de wetgevers bij het kunnen aanpassen van de wet aan een veranderde technische omgeving (alhoewel de omvang van hun wetgevingsbevoegdheid beperkt is), omdat de korte tijd die zij nodig hebben om te reageren hen beter in staat stelt om het snelle tempo van de technologie bij te houden. En gegevensbeschermingsautoriteiten zijn meer pro-actief dan rechters, omdat ze acties kunnen initiëren om de gegevensbescherming te handhaven in situaties waarin rechters nu eenmaal moeten wachten tot er een geding wordt aangespannen. Op basis van de bevin-

dingen van hoofdstuk 4 wordt dan ook de veronderstelling (die Chinese beleidsmakers koesteren) verworpen dat de Europese wetgeving inzake gegevensbescherming volledig zou zijn en dat het ontwerp beperkt kan blijven tot de overname van de positieve materiële rechtsregels inzake gegevensbescherming. Ik toon aan, anders dan de verwachtingen daaromtrent, dat de problemen van de technologische dynamiek en het massale gebruik van sociale media niet triviaal zijn en dat deze om maatregelen vragen die garanderen dat er een uitstekend geïnformeerde en zeer toegankelijke "autoriteit" beschikbaar is met toereikende LMLEP om in de gaten te houden dat de onvolledigheid van de wet niet onhoudbaar wordt. Ik concludeer dat de juridische overname, zoals wordt beoogd, geen effectieve gevolgen zal hebben, tenzij er ook ruimte wordt gecreëerd voor een competente regelgevende autoriteit.

Als follow-up van deze conclusie heb ik in hoofdstuk 5 geanalyseerd met welke verschillen tussen law in the books en law in action de gegevensbeschermingsauthoriteiten van de EU worden geconfronteerd wanneer ze te maken krijgen met het Amerikaanse Facebook en met RenRen, het Chinese broertje daarvan. Het blijkt overduidelijk dat de huidige praktijken van RenRen niet in overeenstemming zijn de beginselen van de Europese gegevensbescherming, en ook niet met de EU gegevensbeschermingswetgeving. Dit betekent dat als RenRen zijn EU-hoofdkwartier in enige lidstaat in Europa zou openen, de onderneming meervoudige klachten over de gegevensbescherming kan verwachten. Wat Facebook betreft concludeer ik dat - ook al lijken de huidige praktijken de EU-wetgeving inzake gegevensbescherming na te leven – dit niet helemaal opgaat wat betreft de beginselen van de Europese gegevensbescherming. Dit leidt tot het inzicht dat wat aanvaardbaar is gezien de EU-privacywet niet aanvaardbaar behoeft te zijn vanuit de visie van de beginselen van de Artikel 29 Werkgroep. Aan de ene kant betekent dit dat het niveau van de bescherming van betrokkenen kan stijgen naar een aanzienlijk hoger niveau, afhankelijk van de uitvoering door betreffende autoriteiten (als die autoriteiten zitting hebben in de Werkgroep). Aan de andere kant toont dezelfde bevinding aan dat het moeilijk is strikte naleving van de wet af te dwingen

met het doel om het gedrag inzake de gegevensbescherming van een wereldwijd toonaangevend Social Network Service speler als Facebook te beïnvloeden. Met andere woorden, de effectiviteit van de law in action is complex en moeilijk te voorspellen door de wet en degenen die de wet handhaven geïsoleerd te bekijken. In China, wordt de spanning tussen de effectiviteit van de law in action en de optimale kwaliteit van juridische constructies groter, althans bij de aanvang van het plan tot overname van de gegevensbeschermingsregels. De onvolledigheid van de wetgeving inzake gegevensbescherming is in China erger dan in Europa, omdat veel van dergelijke wetten er eenvoudigweg helemaal niet zijn en de meeste van dergelijke wetten die wel bestaan onlangs pas zijn ingevoerd. De onvolledigheid is ook ernstiger in China dan in Europa, omdat wetshandhavingsinstanties eenvoudigweg de ervaring missen van het rechtspreken met aanzienlijke aantallen en verscheidenheid van de gevallen. Dit is met name relevant voor de uitvoering onder de auspiciën van het *Ministry of Industry and Information Technology*, het MIIT. Om verschillende redenen kan van het MIIT qua rechtshandhaving geen effectiviteit worden verwacht, althans niet in de beginfase van de ontwikkeling van de gegevensbeschermingsinstituties. Zo worden de Chinese wetgevers geconfronteerd met een uiterst lastige situatie: ze moeten echt nodig een Europese soort van gegevensbescherming ontwikkelen, en toch missen ze het instrumentarium om dat te doen. Erger nog, een pasklaar recept voor rechtshandhaving zoals dat in het verleden elders heeft gewerkt, kan China op de korte en middellange termijn niet helpen.

Ik ben op een punt aangekomen dat ik in staat ben om mijn onderzoeksvraag: "Is China's overnameplan aan te raden?" kan beantwoorden. Met mijn benadering kom ik tot de conclusie dat het niet haalbaar is om uitsluitend de EU-wetgeving inzake gegevensbescherming over te nemen (zoals voorgesteld in het overnameplan van China), tenzij een equivalent van de EU-gegevensbeschermingsautoriteiten in dat plan wordt meegenomen. Chinees gegevensbeschermingsrecht is minder krachtig dan het EU-privacyrecht (hoofdstuk 2). Echter, culturele verschillen (hoofdstuk 3) en inherente onvolledigheid van het

EU-recht (hoofdstuk 4), in combinatie met het feit dat institutionele EU-regelingen die de onvolledigheid verminderen niet zullen werken in China (hoofdstuk 5) doen me besluiten dat de effectiviteit van een geïmporteerde Europese gegevensbeschermingswetgeving niet te veel kan worden verwacht.

In het tweede deel van mijn onderzoek verken ik welke extra mogelijkheden kunnen worden gevonden vanuit het perspectief dat wordt geboden door de complexiteitstheorie, als het onderwerp van de gegevensbeschermingsregelgeving wordt beschouwd als een complex adaptief systeem (hierna: CAS). Voor deze verandering van perspectief is gekozen omdat de fenomenen waarmee ik geconfronteerd werd in de hoofdstukken 3-5 die kenmerkend zijn voor de rechtsbescherming van persoonsgegevens kunnen worden samengevat met behulp van zes karakteristieken. Wie persoonsgegevens gebruiken (produceren en benutten) vormen een netwerk, worden onderling afhankelijk, en vertonen zo nu en dan pad-afhankelijk, dynamisch, complex en adaptief gedrag. In dit tweede deel, identificeer ik eerst het onderwerp van de wetgeving inzake persoonsgegevensbescherming als een PDC (Personal Data Community). Daarna onderzoek ik via het combineren van de PDC met de kennis en ervaringen uit verschillende klassen van CAS, of het onderwerp van de wetgeving inzake gegevensbescherming als een netwerk van gebruikers van de gegevens de kenmerken vertoont van een CAS en wat dit betekent voor de toekomst van de wetgeving inzake gegevensbescherming. Met behulp van enkele belangrijke CAS-eigenschappen en door deze te relateren aan onze PDC en de daarbij bijbehorende ecologie, stel ik vast dat deze eigenschappen gelden voor de PDC en dat dus de PDC kan worden opgevat als een CAS. Vanuit het CAS-perspectief is de door de mens geschapen PDC een groot en dynamisch systeem van interactieve gegevensgebruikers in een netwerk met een bepaald organisatiepatroon van waaruit het vermogen ontstaat tot aanpassing aan interne en externe veranderingen door zelf-organisatie, emergentie en co-evolutie/leren. Mijn bevindingen daagden mij uit tot het maken van juridische constructies op het gebied van gegevensbescherming, en zo te proberen een CAS te "temmen". Bewijs ontleend uit case studies weergegeven in dit boek, even-

als in andere bronnen veronderstellen dat de materie van de wetgeving inzake gegevensbescherming (mogelijk) erg verschilt van dat van andere rechtsgebieden. Het kijkt namelijk op voortdurende kritische overgangssituaties in de praktijk. Zodoende – nu we voortdurend situaties moeten reguleren, die de wetgever zich niet kon voorstellen en zich ook niet heeft voorgesteld toen hij de wet ontwierp – vereisen de doelstellingen van de wetgeving inzake gegevensbescherming, de redenen van haar bestaan en de modaliteiten van deze regelgeving methoden die nogal verschillen van die met een focus op de interpretatie van het materiële recht zoals bij de andere rechtsgebieden. Ik stel voor dat de toekomstige wetgeving inzake gegevensbescherming met vrucht kan worden geconstrueerd op de aanbevelingen van de CAS-theorie: zoals Ruhl (1997) ons leert, kunnen de problemen die zich in een CAS voordoen alleen worden aangepakt, tenzij je denkt als een complex adaptief systeem. Dus het probleem dat aandacht vereist is om ervoor te zorgen dat de wetgeving inzake gegevensbescherming is afgestemd op wat het is.

Maar hoe?

De multidisciplinaire CAS-theorie kan de rechtswetenschap helpen om de wetgever beter te informeren over te verwachten risico's en resultaten van wetgevende activiteiten die naar CAS-elementen verwijzen. In het tweede deel stel ik een aantal strategieën voor die kunnen worden ingezet om juridische onderzoekers te helpen om regulerende kaders te vinden voor complexe adaptieve fenomenen in de PDC. Deze strategieën omvatten onder meer: (i) de voortdurende en herhaalde evaluatie van feitelijke en verwachte effecten van wetswijzingingen; (ii) aandacht voor de culturele en economische omgeving; (iii) begrip voor de functionele betekenissen van "hubs," (iv) kennis van en aandacht voor al dan niet bewuste menselijke drijfveren en (v) aandacht voor de wijzen waarop drijfveren en aangeleerde normen op elkaar reageren.

Ik denk dat de rechtswetenschap de eigen identiteit en de begrenzingen ervan in multidisciplinaire verbanden expliciet moet maken en verdedigen door erop te hameren dat voor de rechtswetenschap het autonome keuzegedrag van verantwoordelijke individuen centraal staat – gedrag waarbij rekening kan

worden gehouden met juridische en culturele normen, kortom gedrag dat bewust is en moet zijn aangeleerd. Dit is bijvoorbeeld anders voor de sociale wetenschappen waarin veelal gezocht wordt naar kennis over mechanismen die het menselijk keuzegedrag (ook onderbewust) kunnen sturen. Ik meen dat een wetgever vanuit beide wetenschappelijke perspectieven moet worden geïnformeerd, liefst consistent ingekaderd. Ik meen dat complexiteitstheorie zo'n inkadering kan bieden.

Het beeld van het onderwerp van de wetgeving inzake gegevensbescherming als een CAS is een voortdurende in plaats van een voltooide constructie. Ondanks het feit dat onze inzichten in de CAS-theorie zich in een staat van evolutie bevinden, hebben de inspanningen tot nu toe al gediend om het begrip te verdiepen van de vele problemen die de wetgeving inzake gegevensbescherming bemoeilijken. En zij hebben gewerkt als kritische factor op een aantal fouten van de huidige gegevensbeschermingswetten. Het is tegen deze achtergrond dat ik verwacht dat de regulering van gegevensbeschermingsitems kan gaan profiteren van de informatie die kan worden verkregen door te kijken door de bril van de CAS-theorie.

Acknowledgements

Foremost, I would like to thank my supervisors Prof. Aernout Schmidt and Prof. Gerrit-Jan Zwenne for providing me with the opportunity to complete my Ph.D thesis at Leiden University. Aernout is one of the smartest people I know. His way of research is driven by pure curiosity of the real world. In these years, he has devoted most of his energy to explore the CAS-theory, never being dictated by outside forces. I learn a lot from him, not only knowledge, but also the scientific attitude: to be an independent intellectual and to enjoy being an autonomous explorer of the truth. I hope that I could be as lively, enthusiastic and energetic as you.

I especially want to thank Prof. Zwenne, whose support and guidance made my thesis work possible. I am very grateful for his patience, motivation, enthusiasm and immense knowledge in data protection that, taken together, make him a great supervisor.

I further thank the members of my defense Committee for their direction, dedication, and invaluable advice along this project. I especially express my deep appreciation to Prof. van der Hof and Dr. Schermer for sharing their knowledge with me.

I want to thank present and past members of eLaw: Franke, Jan Jaap, Martijn, Ramona, Carl and all others for helping me to get used to the Dutch culture, for sharing their knowledge, for providing a great work environment, and for their help and chats. I will forever be thankful to Franke for being supportive throughout my time here. Thank you all. For the non-scientific side of my thesis, I want to thank Ye Dan, YuanYuan, Yi Fan, Xiao, Xiang, Ting, Si Jie, Wei, Yajie and all others. Your constant and unwavering supports are the sunshine which helps me to overcome the bad weather in the Netherlands.

I am especially thankful to my parents, they are the ultimate rea-

son for finishing this project. There are no words to convey how much I love them and appreciate their unconditional love and understanding. These past several years have not been an easy ride, both academically and personally. I truly thank them for sticking by my side, even when I was irritable and depressed. Thank you mom and dad for showing faith in me and giving me liberty to choose what I desired. I consider myself the luckiest in the world to have such a loving and supportive family standing around and behind me.

Propositions

[**1**] Data protection laws aim to domesticate a complex adaptive system (Chapter 7 of this dissertation).

[**2**] Data protection laws are highly incomplete (Chapter 4 of this dissertation).

[**3**] A Data Authority with regulatory agency could help overcome the incompleteness of data protection law. (Chapter 4 of this dissertation)

[**4**] History and culture help shape data protection laws (Chapter 3 of this dissertation).

[**5**] Traditional perspectives like legal positivism and legal realism are important but insufficient to explore incomplete data protection laws (Chapters 1 and 4 of this dissertation).

[**6**] When considering a legal transplantation proposal, cultural embeddings of norms, of policymaking and of enforcing institutions should be carefully investigated and assessed (Chapters 2-4 of this dissertation).

[7] To make the law successfully co-evolve with the dynamics of its subject matter requires the existence of conditional feedback loops between them. To domesticate the behavioral deviations from the law's goals that then may emerge becomes a complex affair. Effective domestication depends on the efforts, the wisdom and the capabilities of policymakers. When policymakers operate with the instrumentation of traditional democracies, and the volatility of the subject matter outpaces traditional democratic responsiveness, regulatory agency (e.g., with regulating authorities) becomes an option (Chapters 4, 5 and 7 of this dissertation).

[8] Proposition 7 also covers the co-evolution of EU data protection laws with the dynamics of its subject matter (Chapters 4, 5 and 7 of this dissertation).

[9] To re-search is shorthand for to search, search, search, search and search again.

[10] "The conditions of conquest are always easy. We have but to toil a while, endure a while, believe always, and never turn back"[182]

[11] "In the beginner's mind there are many possibilities, but in the expert's there are few"[183]

[182] Simms, William Gilmore. 1853. *Egeria: Or Voices of Thought and Counsel, for the Woods and Wayside.* E.H. Butler.

[183] Suzuki, Shunryu. 2010. *Zen mind, beginner's mind.* Shambhala Publications.

Curriculum Vitae of Kunbei Zhang

Kunbei Zhang was born in China on 31 December 1983. After completing her Bachelor Degree in Law at the Southwest University of Political Science and Law in 2006, she worked as a lawyer in the Guo Hong Electronic Company. In 2007, she continued her legal studies at the Trinity College in Dublin. She graduated with a LLM degree in 2008. In October, 2008, she joined elaw@Leiden of Leiden University as a PhD researcher. She currently has several publications under review, among which ``Incomplete Data Protection Law" (which is an adaptation of this book's Chapter 4) will be published in the September 2014 issue of the German Law Review. For the immediate future, Kunbei Zhang decided to pursue her scientific career in China.

Proof

Printed By Createspace

Digital Proofer