Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

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.