Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

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.