Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Chapter 3

Do History and Culture Matter?

Introduction

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

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

on context (Johnson (1989)).

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

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

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

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

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

Cultural value patterns on privacy

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

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

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

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

Cultural value patterns in Europe

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

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

least not in Europe:

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

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

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

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

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

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

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

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

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

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

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

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

Cultural value patterns in China

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

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

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

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

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

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

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

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

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

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

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

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

[41]Hornby & Zhang (1984).

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

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

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

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

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

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

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

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

[45]Hornby & Zhang (1984).

privacy;

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

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

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

Diverse cultural value patterns and data-protection laws

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

The right to informational privacy in Europe

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

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

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

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

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

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

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

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

[50]Article 13. Exemptions and restrictions

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

(a) national security;

(b) defense;

(c) public security;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[53] Capurro (2005): 42

Chinese material laws

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[60]Id.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[70]JIPDEC (2008).

[71]Id.

[72]Id.

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

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

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

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

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

Different laws and cultural value patterns

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

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

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

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

Conclusion

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

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

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

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

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

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

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

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

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

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