Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Chapter 6

Conclusion of Part I

Summary

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

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

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

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

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

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

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

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

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

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

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

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

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

and yet they lack the instruments to do so.

Considering China's transplantation plan

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

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

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

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

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

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

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

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

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

Challenges ahead

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

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

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

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

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

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

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

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

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

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

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

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

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