Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Chapter 5

Compliance With Law

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Regulatory institutions and company behavior

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

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

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

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

The case of RenRen

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

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

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

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

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

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

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

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

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

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

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

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

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

Figure 5.1: Example of a RenRen screenshot

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The case of Facebook

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

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

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

Preliminary evaluation: Facebook vs. RenRen

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

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

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

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

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

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

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

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

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

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

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

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

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

[115]Chapter 1

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

Chapter conclusion

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

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

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

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

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