Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Chapter 4

Incomplete Data Protection Law

Introduction

In previous two chapters, I explored the differences between two regions' privacy laws and between two regions' privacy cultures involved. I have a basic understanding of what to import and what not to import. Yet, what I do not know is how to import or how to arrange the candidate law in China? That is an issue related to legal importation strategy.

This Chapter considers the issue. As I presented in Chapter 1, China's policymakers maintain that European data protection law is complete and therefore beneficial (Hanhua Zhou (2006)). Thus, their transplantation plan, based on that assumption, reproduces the contents about data subjects' rights and data controllers' responsibilities in European law. However, if instead the assumption cannot stand up and the targeted data protection law cannot unambiguously stipulate all relevant applications, China's policymakers need to re-adjust past legal transplantation strategy.

In this Chapter, I will find whether the EU data protection law is not as complete as China policymakers' expects? If not, how do European policymakers attempt to compensate for the defects of the incompleteness? In order to do the examination, I deploy an analytical tool from 'The Theory of Incomplete Law' (Hereafter ILT). The

theory is contributed by Katharina Pistor and Chenggang Xu. In fact, it is not a novelty to claim that law is incomplete. For instance, Hart argued that law is indeterminacy (Hart (1994):128). But what makes the ILT different from other ones, which establish the incompleteness of law is that the ILT addresses the problems brought by incomplete law. As Xu and Pistor suggest,

> *"Law is inherently incomplete which implies that it is impossible to write a law that can unambiguously specify all potentially harmful actions. Because law is incomplete, law enforcement by courts may not always effectively deter violations. Rather than attempting the impossible task of completing the law, the effectiveness of law enforcement may be enhanced by reallocating lawmaking and law enforcement powers."*[75]

The incomplete law theory is inspired by the incomplete contract theory (Xu & Pistor (2002a):933). Xu and Pistor develop the incomplete contract theory to cover the profound incompleteness problem in law when they assessed the governance functions in financial market (Xu & Pistor (2002a):937). The theory is of wide interest to legal research which not only can be used to compare legal systems, but also to analyze lawmaking and law enforcement in diverse jurisdictions (Xu & Pistor (2002a):966). In this Chapter, the application of the ILT is extended into a new field: data protection law.

This chapter is organized as follows: first, I will outline the characteristics of incomplete law theory (2). In Section (3), I will apply the framework to the European legal system over data protection issues. I analyze the legislative responses to challenges posed by the development of technology. Then, I explore the European institutional arrangement on data protection issues(section 4). In Section 5, I draw conclusions on the strategy to import European data protection law.

[75] Xu & Pistor (2002a):931.

The Incomplete Law Theory

In this Section, I amplify the analytical framework of incomplete law theory. Most of the contents in this section are concluded from a series of paper wrote by Xu and Pistor (such as Pistor & Xu (2002a, 2004, 2006); Xu & Pistor (2002b,a)). The purpose of this Section is to provide a complete picture about the theory.

Law is intrinsic incomplete

My first question when I met the ILT is: What is a complete law and what is an incomplete law? According to Xu and Pistor, completeness means that obligations *can be unambiguously stipulated in the law and the law can be enforced literally provided that evidence is established* (Xu & Pistor (2002a):938) In the enforcement process, completeness requires that *the law is self-explanatory, i.e., that every addressee agrees to the meaning of the law and, by implication, that there is no need for interpreting the law* (Xu & Pistor (2002a):938). If not, the law is incomplete. The two authors argue that laws cannot be complete since they have in their `genes' some characteristics that make them designed to *serve a large number of addressees for long periods of time and to cover a great variance of cases* (Xu & Pistor (2002a):939).

According to Xu and Pistor, it is questionable to create an intrinsic complete law (even though legislators try to avoid this energetically), since legislators *cannot foresee all future contingencies, nor can they correctly predict their probabilities*" (Pistor & Xu (2004):9). Of course, sometimes, a law can remain complete for a period of time when sufficient expertise is assembled (Pistor & Xu (2004):8). Nevertheless, it is difficult, even for a carefully designed law, to remain complete for a long time. New conditions, which lawmakers have not yet contemplated before, will arise over time to challenge the completeness of law and therefore its incompleteness is increased (Pistor & Xu (2004):8). Whatever happens, legislators can neither predict nor shape the future. As legal philosopher H.L.A. Hart argued, it is *a feature of the human predicament* that lawmakers simply cannot *regulate, unambiguously and in advance, some sphere of conduct by means of general standards to be used without further official direc-*

tion on particular occasions(Hart (1994):128). The world is simply too complex (Hart (1994):128).[76]

Moreover, some laws are enacted to be incomplete by the legislator's *deliberate design* (Xu & Pistor (2002a):932). In order to provide general guidance for helping others to *structure their relations* or to remain applicable to future disputes, laws may be created in a way that can *serve a large number of addressees for long periods of time and to cover a great variance cases* (Xu & Pistor (2002a):939). The positive side of the strategy is that a law can apply *equally all conditions described in the law, irrespective of the class, social status, or other attributes of individuals subject to the law* (Xu & Pistor (2002a):939). But the flip side is that law becomes too general to provide specific standards and procedures for each case. This can *affect the outcomes for a variety of cases that may arise in the future* (Xu & Pistor (2002a): 939).

Two types of incompleteness

Xu and Pistor classify incomplete laws into two categories based on the causes of incompleteness.

Type 1 *An incomplete law of Type I is one that broadly circumscribes outcomes without identifying particular actions or enumerating only a few actions* (Xu & Pistor (2002a):941). The example of Type I incomplete law is tort law (Xu & Pistor (2002a)).

> ``*General tort principles typically stipulate that damage to property, life, and liberty gives rise to a liability claim against the person responsible. Note that no single action is defined, only the broad outcome of damages to life, liberty, and property. Requiring intent or negligence or imposing strict liability can further circumscribe the scope of liability, but this still leaves open the question of what form actions might take that will trigger liability under the law.*"(Xu & Pistor (2002a):941)

[76]In the words of Hart, "If the world in which we live were characterized only by a finite number of features, and these together with all the modes in which they could combine were known to us, then provision could be made in advance for every possibility." He adds, "Plainly this world is not our world."

Type 2 *An incomplete law of Type II is a law that specifies the actions that shall be prevented but that fails to capture all relevant actions. To categorize laws based on types of incompleteness brings forth new ideas for legal study* (Xu & Pistor (2002a):941). The authors think Criminal Law offers an excellent example for incomplete laws in this type. As they state, Criminal Laws

> ``*usually contain a number of provisions aimed at protecting property rights, but each designed to cover a particular action, such as theft, embezzlement, damage to property, and the like. Closer inspection of these provisions reveals that the law has not captured all possible actions that could violate property rights*." (Xu & Pistor (2002a):941)

Institutional mechanisms for incompleteness.

When a law is incomplete, some new powers have to arise in order to decide how to deal with new cases through either interpreting or developing existing laws. Xu and Pistor name the new powers to be 'residual lawmaking and law enforcement powers' (Xu & Pistor (2002a):938) (hereafter *residual LMLEP*). The residual LMLEP is ``*the power to adapt or extend the range of existing laws to new cases that arise in changing circumstances*" (Xu & Pistor (2002a):933). Correspondingly, ``*the power to make new law from scratch*" is the original LMLEP (Pistor & Xu (2006):7). When law is complete, merely allocating the original LMLEP (in most cases, courts are naturally to grant with original LMLEP) is sufficient to achieve efficient levels of deterrence (Xu & Pistor (2002a):946). But when law is incomplete, it is insufficient. In this case, the residual LMLEP needs to be allocated explicitly (Xu & Pistor (2002a):964). The two authors claim that incompleteness can, to a large extent, be reduced when the residual LMLEP is allocated appropriately (Xu & Pistor (2002a):935).

Generally, residual LMLEP can be allocated to two different agents: courts and regulators (Xu & Pistor (2002a):946).[77] The two

[77]The agencies which are qualified to exercise the residual LMLEP are not limited to the two agents. For instance, self-regulators may be allo-

agents both have merits and demerits. The ILT offer a criteria to help policymakers to decide which one is preferred under certain conditions and constraints (Xu & Pistor (2002a):961). Herein lies a significant contribution of the theory to link the expected needs of the (incomplete) law on institutional LMLEP competence with competences already in place.

Courts

Courts could be allocated with substantive residual LMLEP. When law is incomplete, courts step in to clarify the incompleteness if it is required in the process of addressing a case. Through interpretation and further development of existing laws, courts decide how to enforce an 'old' law to new cases. This is the way how courts exercise residual LMLEP. Every case reflects courts' efforts to optimize the completeness of the law.

There is big difference between the two major legal families in the world on how residual LMLEP has been allocated to courts (Xu & Pistor (2002a):946). In Common Law countries, *courts commonly hold extensive residual LMLEP* (Xu & Pistor (2002a):947),[78] while in Civil Law countries, courts are constrained in and to exercising residual LMLEP (Xu & Pistor (2002a):947).

Yet overall and traditionally, courts are the natural agents to exercise residual LMLEP. However, courts have a weakness in exercising the residual LMLEP. That is courts do not ``have the power to take action *sua sponte* even when such an intervention might be desirable." In other words, courts enforce laws *ex post, ``after harm has occurred*." Judges cannot take action unless parties bring in motions.[79] Xu and Pistor are concerned that it may be insufficient to ensure optimal law enforcement of incomplete laws to solely allocate the residual LMLEP to courts (Xu & Pistor (2002a):949, Milgrom *et al.* (1990)).

cated to exercise residual LMLEP. In the data protection area, it is widely believed that self-regulators, from the incomplete law's perspective, are allocated with these residual powers in the USA. But when the theory was first established, the authors limited their analysis to regulators generically defined. In the following years, the two authors also analyze the efficacy of the approach to grant residual powers to agencies beyond courts and regulators. In my research, I also limit my analysis to regulators generically defined.

[78]The two authors mentioned that there is a substantial debate whether common law judges actually "make" law or whether they "find" the law based on legal principles. See, e.g., Jack G. Day, *Why Judges Must Make Law*, 26 CASE W. RES. L. REV. 563, 563-65 (1994). Incomplete law theory remains neutral to the debate. The authors consider that what judges in Common Law countries do is to make legally binding precedents, which fills in some gaps in the law. This lawmaking power is one of their major functions.

Regulators

It is an alternative approach to grant residual LMLEP to regulators. Regulators exercise residual LMLEP in a different way from courts, since regulator can adapt and enforce the completeness of laws proactively through various means (Xu & Pistor (2002a):948). For instance, a regulator can control *entry to markets and access to assets, monitor activities, initiate investigations, enjoin actions, and initiate the administration of sanctions against violators* (Xu & Pistor (2002a):948). The police, illustrated by the authors, is an example of a regulator (Xu & Pistor (2002a):948). The police can *monitor behavior and seek to prevent damages by enjoining actions that are likely to cause harm* (Xu & Pistor (2002a):948). Additionally, the supervisory authorities in stock markets or the banking industry, which are the main objects of observation for Xu and Pistor, also regulators that exercise substantive LMLEP.

Different from courts, regulators can exercise the powers both *ex post* and *ex ante* (Xu & Pistor (2002a):949). Regulators can exercise residual LMPEP to respond to incompleteness more freely (but within the scope of their lawmaking rights) (Xu & Pistor (2002a):950). Regulators also can *correct past errors on their own initiative and in a flexible and responsive manner* (Xu & Pistor (2002a):951). Therefore, regulators enjoy a comparative advantage over courts in exercising residual LMLEP more flexible and in a wider range of situations (Xu & Pistor (2002a):1012).

[79]Citations in this paragraph are from (Xu & Pistor (2002a):948-49). The two authors noticed that courts can also be asked to prevent harmful actions from taking place, for example to file a motion for preliminary injunction. But this procedure is still based on someone other's motion.

Nevertheless, regulators are superior to courts only under certain conditions and constraints,[80] since they are subject to infirmities in exercising residual LMLEP (Xu & Pistor (2002a):961). Typically, over- or under- regulation is the mistakes which could be seen frequently. *Over-regulation occurs when a regulation imposes costs that outweigh the benefits of proactive law enforcement by courts* (Xu & Pistor (2002a):951).[81] Over-regulation also occurs when it chills *too many potentially beneficial actions or when well-intended regulation stifles economic activities in other ways* (Xu & Pistor (2002a):951). According to Xu and Pistor, *Regulators may also under-enforce because they face resource constraints, mis-allocate their resources, or fail to detect risks of harmful actions* (Xu & Pistor (2002a):951).

Hence, the question turns to under which conditions it may be optimal to allocate the exercise of residual LMLEP to courts, and under which conditions to allocate them to regulators? Xu and Pistor suggest two important factors for consideration: standardization and the level of expected harm (externality) (Xu & Pistor (2002a)).

Standardization:

> *refers to the ability to describe actions and outcomes at reasonable cost so that regulators can exercise their proactive law enforcement powers effectively. The effectiveness of proactive law enforcement hinges on the ability of regulators to monitor the market and identify types of actions and outcomes that reasonably may be expected to result in harmful outcome. The assessment of which actions or outcomes fulfill these conditions may change over time. Yet it is essential that regulators be able to identify and standardize in order to use their resources effectively and avoid the pitfall of over-enforcing (Xu & Pistor (2002a):952)*

The level of expected harm:

> *The constraints of ex post lawmaking and reactive law enforcement may be tolerable when the expected level of harm is low, for example, when the harm victims might suffer is small or when only a few victims are affected by harmful actions [...] If, however, the level of expected harm is substantial, [...] court enforcement will not be effective. It will typically come too late, after harm has been done. Shifting to a proactive law enforcement regime that seeks to prevent the occurrence of harm through entry barriers, continuous monitoring, and investigation, will therefore be superior* (Xu & Pistor (2002a):952)

Accordingly, regulators are only the superior option to be allocated with the residual LMLEP, when these two factors are met. The cost of proactive law enforcement by regulators can be justified only when actions can be standardized and when these actions are likely to create substantial harm which cannot be fully remedied by reactive law enforcement (Xu & Pistor (2002a)).[82]

Section Summary

The ILT can be summarized into three propositions:

1. all law is intrinsically incomplete;
2. the optimal approach to incompleteness is to allocate residual LMLEP;

[80] On the tradeoff between monitoring and investigating and the cost implications of these regulatory enforcement mechanisms, see Dilip Mookherjee & I. P. L. Png, Monitoring vis-á-vis Investigation in Enforcement of Law, 82 AM. ECON. REV. 556, 557 (1992). Using a formal model to compare the tradeoffs, Mookherjee and Png conclude that the use of these alternative enforcement devices should be tailored to the severity of the offense. Smaller offenses should not be investigated, merely monitored. Larger offenses should be investigated in accordance with their severity, and fines should be maximized (Mookherjee & Png (1992)).

[81] The two authors illustrate that the direct costs of regulation include the funds needed to hire monitors and investigators, to maintain filing systems, and to launch lawsuits. The indirect costs of regulation are comprised of the costs market participants incur because they have to comply with regulations and that society incurs when regulators either over- or under-enforce the law.

[82] Of course (yet for my research questions off-topic), the deployment of residual LMLEP competencies must be monitored and exercised within the constraints as set by the legal system that erect the regulator, as all powers have to respect checks and balances.

3. regulators conditionally have advantages over courts for holding and exercising residual LMLEP -- *i.e.*, when actions can be standardized and when substantial harm is likely to be created.

The first proposition lies the foundation of the theory, and the other two supply an analytical framework to help researchers assess the design of legal institutions as well as the efficacy of law enforcement.

Incomplete Law: Examples from Directive 95/46/EC

In this section, European data protection law is observed through the lens of ILT. The purpose of the observation is not to illustrate how good or bad drafting the Directive is. Instead, what I am interested in is the European legal system's abilities to deal with ``unforeseen contingencies." Since issues related to data protection are too broad for a compact analysis, the analysis is limited to the scope of Directive 95/46/EC.

Directive 95/46/EC is intrinsically incomplete

The Directive 95/46/EC is intrinsically incomplete because it is a general law to ``*serve a number of addressees for long periods of time and to cover a great of variance of cases*" (Xu & Pistor (2002a):938-939). Hence, the Directive could not cover all possible situations. As I analyzed above, the feature of generality determined the Directive, from the first beginning, has accompanied with "incompleteness". Moreover, the Directive 95/46/EC tries to regulate a field which is closely linked with technology. According to (Xu & Pistor (2002a):932), the law which is affected by a high pace of technological changes, is more incomplete than others, because ``*such change constantly challenges legal solutions designed to solve "old" problems and thus requires frequent adaptations of the law if it is to remain effective."* The challenges caused by technological changes will be further presented in Section 4.3. Therefore, through the lens of ILT, Directive 95/46/EC is incomplete and it is even more incomplete than other areas which may not be featured by continuously exogenous changes.

A key aspect of incomplete law is both data subjects and data processors may trouble to determine whether an action falls within the forbidden scope (Xu & Pistor (2002a):949). Data processors may find it difficult to anticipate the consequences of actions within a particular situation. If they are careless, and assume that their action will not by punished by law, harms may be resulted in (Xu & Pistor (2002a):949). Xu and Pistor point under this situation law under-deters since data subjects may be harmed (Xu & Pistor (2002a):949). If data processors are too cautious to do what otherwise would be considered legitimate business, the over-deterrence are unfavorable to the development of economics (Xu & Pistor (2002a):949). In either case, the incomplete law could not prevent damages.

Courts' efforts to address incompleteness

In order to address the incompleteness, courts, as the natural agents to grant with residual LMLEP, step in to fill the gaps left by laws. In this section, I will moreover do some research based on cases that were decided by the European Court of Justice in Luxembourg (hereafter ECJ)[83] that are also referring to Directive 95/46/EC. The reading on the case law is in order to answer: Whether the Courts adequately remedy the incompleteness of Directive 95/46/EC through exercising residual LMLEP?

The ECJ is allocated with substantial residual LMLEP. The ECJ plays an important role in shaping the common 'character' of data protection in Europe (Kuner (2007):7).[84] The ECJ involves in data protection issues through two ways: first, a member state or the Commission may bring an action before the Court, and the other one is a Member State's national court may refer questions to the ECJ for interpretation (Kuner (2007):7). For the second way, a major part of the ECJ's judicial reasoning are to determine whether Directive 95/46/EC

[83] The information about the ECJ is harvested from its official website. Readers can get access to more details about the ECJ through the following link: http://europa.eu/about-eu/institutions-bodies/court-justice/

[84] According to European data protection officer, case law decided by ECJ is a significant building block of the legal framework for data protection law in Europe. See:
http://ec.europa.eu/dataprotectionofficer/legal_framework_en.htm

and its companion directives or cases laws could extend to new cases. In this situation, the ECJ exercises the residual LMLEP through settling legal disputes (or answering prejudicial questions addressed to it by member-state courts, deciding a case).

Following, I pay attention to case study. How the ECJ exercises their LMLEP is at the center of my analysis. The background and legal contents are cited from the ECJ's judgement.

Joined Cases C-465/00, C-138/01 and C-139/01 Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk[85] *ECJ (2003)*

- Directive 95/46/EC includes a provision that the purpose of the Directive is to ensure the personal data flow freely from one Member State to another (EC (1995). The dispute referring to the prejudgement sent to the ECJ is to answer: whether Directive 95/46/EC is applicable to issues, which seems to have no relation with the issue of internal market harmonization (ECJ (2003)).
- The ECJ's response: In this judgement, the ECJ held that the Directive should apply to cases which are no link with the issue of harmonizing internal market (ECJ (2003)).
- The outcome of the preliminary ruling: The Type I incompleteness was reduced. ECJ's judgement extended the scope of the applicability to cover any actions which are different from the expression of principles and criteria laid down in the Directive 95/46/EC (*ECJ (2003)*).

Case C-101/01 Criminal Proceedings against Lindqvist[86] ECJ (judgment of 6 November 2003))

[85]ECJ, Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof, Judgment of 20 May 2003. The judgement of the case could be get access to through the following link: http://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en

[86]http://eur-lex.europa.eu provides more information about the case.

- The Directive 95/46/EC has provisions referring to the scope of its applicability (Article 3); prohibited processing categories (Article 8); restrictions and exemptions of its applicability (Article 13) and cross-border data flow (Article 25). The disputes referred to the preliminary rulings include: whether " the act of referring on an Internet page to various persons and identifying them by name or by other means" falls into the scope of the Directive's applicability (ECJ (judgment of 6 November 2003)))? whether ``processing data such as giving their telephone number, or information regarding their working conditions and hobbies constitutes is covered by one of the exceptions in Article 3 (2)"? what kind of information concerns health (ECJ (judgment of 6 November 2003)))? whether ``a transfer of data to a third country includes the occasion that load personal data onto a page stored on a server which is hosted by a natural or legal person established in a Member State and thereby making those data accessible to anyone who connect the Internet including people from third country" (ECJ (judgment of 6 November 2003)))? And if no one from third country is accessed that data (ECJ (judgment of 6 November 2003)))? Whether ``the provisions in Directive 95/46/EC bring about a restriction which conflicts with the general principle of freedom of speech" (ECJ (judgment of 6 November 2003)))? whether it is permissible for the member state to ``provide for greater protection for personal data than required by Directive 95/46/EC" (ECJ (judgment of 6 November 2003)))?
- The ECJ's response: First, information on an internet page which could identify data subjects by any means falls into the scope of the Directive; second, the information about "injured foot" in this case is concerning health; third, there is no 'transfer of data to a third country' within the meaning of Article 25 of Directive 95/46 by loading personal data onto an internet page which is stored in a server hosted by legal or natural persons in another Member State, even though it is accessible by people from third country; fourth, there is no restriction on the principle of freedom of speech and it is the national authorities and courts' responsibilities to balance these general principles; fifth,

member states' legislators must ensure to comply with the provisions of Directive 95/46/EC but are not restricted to extend the protective scope above the Directive. (ECJ (judgment of 6 November 2003)))

- The outcome of the preliminary ruling: Type I incompleteness was largely reduced. However, the Type II incompleteness was increased. Each new extended scope will eventually give rise to new litigation, as technological development would go beyond the scope of its applicability. Since courts are limited by its reactive and ex post features, they cannot easily and quickly adjust laws in response to observed changes. Before they catch up with new developments via exercising LMLEP, there is always sharp learning and waiting curve.

Joined Cases C-468/10 and C-469/10 - Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/ 10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado ECJ (2011)[87]

- Directive 95/46/EC has a provision (Article 7 (b)-(f) referring to conditions relating to legitimate interest in data processing without the data subject's consent (EC (1995)). The dispute referred for preliminary rulings is about whether Member States' national laws are entitled to add extra conditions to those required by Directive 95/46/EC?

- The ECJ's response: "*Article 7(f) must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalized way, any processing of data not appearing in such sources*" (ECJ (2011)).

- The outcome of the preliminary ruling: Type I incompleteness of Directive 95/46/EC was reduced.

[87] In the case, Spain's Royal Decree 1720/2007 which was believed to impose the extra conditions relating to the legitimate interest in data processing without the data subject's consent, which does not exist in Directive 95/46, to the effect that the data should appear in public sources. The Tribunal Supremo (Supreme Court, Spain) asked the ECJ to interpret Article 7(f) of Directive 95/46. The contents in this section are cited from the judgement. The complete version of the judgement could be access following the link http://curia.europa.eu/juris/liste.jsf?num=C-468/10&language=en

C-518/07 European Commission supported by European Data Protection Supervisor v Federal Republic of Germany ECJ (2010)

- Directive 95/46/EC includes a provision (Article 28) that the data protection authorities must be able to exercise their entrusted functions independently (EC (1995)). The dispute in the case is: how "independent" should independent agencies should be?

- ECJ's Decision: *"by making the authorities responsible for monitoring the processing of personal data by non-public bodies and undertakings governed by public law which compete on the market (öffentlich-rechtliche Wettbewerbsunternehmen) in the different Länder subject to State scrutiny, and by thus incorrectly transposing the requirement that those authorities perform their functions 'with complete independence', the Federal Republic of Germany failed to fulfill its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"* (ECJ (2010));

- Outcome of the decision: The Type I incompleteness of Directive 95/46/EC was reduced.

C-553/07 College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands [88]

- Directive 95/46/EC includes a provision (Article 12) to entrust data subjects the right to access (EC (1995)). However, the provision does not indicate ``any time period within which it must be possible for those rights to be exercised'' (ECJ (2009)). The dispute referred to the preliminary ruling is about whether Member States could impose a time restriction in their national law (ECJ (2009)).
- The ECJ's response: It is not in-proportional for Member States to fix a time-limit for storage of that information and to provide for access to that information (ECJ (2009)). Nevertheless, the storage period must take consideration of both data subjects' interests and the burden on data controllers for storage (ECJ (2009)).
- The outcome of the preliminary ruling: Type II incompleteness of the Directive is reduced since the preliminary ruling specifics a situation that shall not be prevented. But Type I incompleteness is increased.

C-524/06 Heinz Huber v Bundesrepublik Germany

- Directive 95/46/EC has a provision that requires data processing for a task carried out in the public interest or in the exercise of official authority (EC (1995)). The dispute refereed to the preliminary ruling is about whether the provision could be enforced on the grounds of nationality (ECJ (2008a)).
- The ECJ's response: According to the ECJ's judgement,[89] "*Article 7(e) is interpreted in the light of the prohibition on any discrimination on grounds of nationality, unless: 1) it contains only the data which are necessary for the application by those authorities of that legislation, and 2) its centralized nature enables the legislation relating to the right of residence to be more effectively applied as regards Union citizens who are not nationals of that Member State*" (ECJ (2008a)).
- The outcome of the preliminary ruling: The Type I incompleteness of Directive 95/46/EC was reduced. But Type II incompleteness may be increased.

[88]The contents in this section are cited from ECJ (2009).

[89]The contents in this section are cited from the judgement.

C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy(ECJ (2008b))

- Directive 95/46/EC provides exemptions for processing personal data for journalistic purposes (EC (1995)). The dispute referred to the preliminary rulings is about in which circumstances the activities at issue may be regarded as the processing of data carried out solely for journalistic purposes could exempt or derogate from data protection (ECJ (2008b)).
- The ECJ's response:[90] the notion of "journalistic activities" should encompass " *all activities whose object is the disclosure to the public of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper or radio waves or an electronic medium such as the internet) and of the nature (profit-making or not) of those activities*" (ECJ (2008b))
- The outcome of the preliminary ruling: the way the ECJ response to Type I incompleteness might increase Type II incompleteness to the Directive 95/46/EC. The interpretation aimed at broadly encompassing all journalistic activities, but each conditions the ECJ designed covered particular situation, such as medium, format of data, nature of those activities.

[90]The contents in this section are cited from the judgement.

Joined Cases C-317/04 and C-318/04 (judgment of 30 May 2006/ European Parliament v Council of the European Union ECJ (2006)

- Directive 95/46/EC has a provision (Article 26) referring to non Member States' data protection level (EC (1995)). The dispute in the case is about: whether the Commission could validly adopt the decision on adequacy on the basis of Directive 95/46/EC (ECJ (2006))?
- The ECJ's judgement: "*the transfer falls within a framework established by the public authorities that relates to public security. The Court thus concluded that the decision on adequacy does not fall within the scope of the directive because it concerns processing of personal data that is excluded from the scope of the directive. Consequently, the Court annulled the decision on adequacy*" (ECJ (2006)).
- The outcome of the judgement: The Type I incompleteness of the Directive 95 was not reduced.

The ECJ's efforts enhanced the efficiency of lawmaking, if compared with depending on legislators to update law. But, whether the ECJ's reactive enforcements adequately remedy this incompleteness? My reading of the judgements does demonstrate that the ECJ's efforts do largely remedy the incompleteness of the Directive 95/46/EC. Nevertheless, in some cases (including C-101/01, C-553/07, C-524/06, C-73/07), I also witness that ECJ's judgments create new incompleteness to the Directive. This is not a satisfactory result.

A weakness in courts' action range

Data protection law is closely related with technology. How do Courts, the reactive law enforcement agency, overcome the challenges brought by technological changes? In this Section, I focus on the challenges presented by cloud computing for regulating transnational data flow.

Currently, cloud computing raises some unique law enforcement concerns regarding, for example, the location of potential digital evidence, its preservation, and its subsequent forensic analysis.[91] The transnational data flow agreement, the U.S. -- EU Safe Harbor Framework, is also tested in a cloud computing context. In European law aspect, the Framework is to facilitate personal data to be transferred under a presumption of adequacy to U.S-based companies that agree to be bound by the system (Kuner (2007):180).

Cloud computing technology threatens to render the Framework unsafe for ``the cloud." The Dutch Data Protection Authority (hereafter CBP) highlighted three personal data-related concerns surrounding the Framework: transfer, security and processing by sub-processors of personal data in the cloud.[92] The CBP observed that sole self-certification with Safe Harbor Framework may not be sufficient in a cloud environment. It is the controllers/data clients' responsibilities to ensure that the principles (from Safe Harbor principles, from the Dutch Data Protection Act and from other additional requirements) are complied with by safe-harbor companies (Dutch Data Protection Authority (2012)). Thus Cloud Computing practices challenge the conviction that the Safe Harbor Framework provides a viable compromise.

In fact, the three personal data-related concerns not only plague the Framework, but also test the limitation of Directive 95/46/EC. Article 25 and article 26 limit the flow of data to countries located

[91] http://www.dfinews.com/articles/2013/08/cloud-computing-presents-unique-forensic-challenge#.UpUc9pEUHlU

[92] The CBP presented the three challenges when proceeding to answer the questions posed by SURFmarket. SURFmarket is a Dutch organization that undertakes joint investments nationally and internationally in IT-driven innovations. The SURFmarket submitted three questions to the CBP:

1. Does the self-certification by the American provider to the Safe Harbor Framework offer sufficient safeguards for the transfer of personal data to the United States (U.S.)?
2. Does the Statement on Auditing Standards no. 70 (SAS 70) standard offer sufficient certainty regarding the security of the processed personal data, or are the International Standards for Assurance Engagements (ISAE) 3402 and Statement on Standards for Attestation Engagements (SSAE) 16 standards better equipped for this purpose?
3. Is the self-certification of the American provider to the Safe Harbor Framework sufficient to safeguard that sub-processors engaged by the provider satisfy a comparable suitable level of protection (Dutch Data Protection Authority (2012))?

outside the EEA when such countries (or the recipients) can not provide an adequate level of personal data protection (Article 29 Working Party (2012):17). These articles evoke discussion. The premise underlying them is that the location of personal data is clear. This premise is in step with the technology of the time when the Directive was enacted. Generally, the specific technological horizon was featured by relational databases and `island' computing, and by the business practices that these features supported for personal data processing. It may have been common sense at the time of enactment, that the location of personal data was easily identified: where the data is at a certain moment and by whom and how it is being processed. However, through the lens of current tech-level optics, this perspective has become obsolete for a growing collection of business practices. Against the diversity of cloud computing services, the cloud client[93] is rarely in a position to know in real time where the data are located, stored or transferred (Article 29 Working Party (2012):17). As the 'International Association of Privacy Professionals' described, ``*data are stored and processed remotely, or in places far away, often in multiple places with different jurisdictions and legal regimes*" (Hogan Lovells Law Firmer (2011)). And Widmer (2009) submits concerning e-mail services based on cloud computing: ``*the customer's data can be stored anywhere in the world, depending on where the servers are located*." Hence, it is impossible, both for the cloud clients/controllers and for the cloud providers/processors to say where the data are at a certain moment and by whom and how it is being processed. Thus employing the cloud computing platform for ICT services even further[94] tests in practice the efficacy of the Articles 25 and 26.

Moreover, data flows within Europe also test the limitations of the applicability principle in the Directive. The applicability principle is governed by Article 4.[95] According to Article 4, the applicability of national laws is determined either by the location of the establishments of controllers or by the location of the means or equipment being used when the controller is established outside the EEA (Article 29 Working Party (2010b):17). As Moerel concluded, ``the connecting factor for applying the Data Protection Directive is based on the territoriality principle and limited to situations where foreign controllers use processing 'equipment' located within the EU" (Moerel (2011):91). However, the complexity of applicability issues is multiplied by cloud computing. Personal data may be transferred within the cloud provider's proprietary cloud, which can cover several Member States. As a result, it is no longer quite certain who is the controller that ``*determines the purposes and means of processing personal data*" (EC (1995): Article 2). Moreover, Hon & Millard (2008) correctly warn in their blog that ``*cloud users who process personal data in the cloud will be controllers unless an exemption applies, e.g. private use only, as with purely personal webmail. Cloud service providers are generally treated as processors. But the roles taken by cloud service providers are not limited to being processors, but may also and concurrently, in some situations, turn into being controllers*." This feature blurs the demarcation lines between data controllers and non controllers, which might easily turn into another[96] force that works towards the dilution of EU privacy law.

[93]The "cloud client" is the W.P.'s equivalent for the Directive's controller where personal data protection "in the cloud" is concerned (see Hogan Lovells Law Firmer (2011):5 and Article 29 Working Party (2012)).

[94]As many expect to be the case, considering the growing success of the cloud servicing business model.

[95]Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

[96]Zwenne (2013) discusses the problems of privacy-law dilution that result from over-expanding the conceptual demarcations of "personal data."

The three arguments illustrate how cloud computing questions Directive 95/46/EC. Distinctions can be made between the technologies that are regulated by law and the technologies that are not (and that need to be regulated). These distinctions do cause problems for the Directive to provide clear formulations. Incompleteness of both types comes to the fore. As a matter of fact, the emergence of new technology like cloud-computing services has set the EU legislature more incomplete.

Naturally, cloud computing should not become a technology that can evade data protection requirements. However, the significant limitations of courts for exercising LMLEP are highlighted in this case. As the ``ultimate arbiter'' (Kuner (2007):7), the ECJ is passive and can only exercise their LMLEP after a motion has been filed. I do believe that the judges in the ECJ are aware of the data-protection problems under cloud computing business models. But they do not have the power to take action, since no case is brought to the ECJ (until now). The ECJ has to remain passive until others bring actions, even though judges may have designed a strategy on how to exercise their LMLEP. Thus, although it is possible that the ECJ would stretch the scope of Directive 95/46/EC to encompass cloud computing, uncertainties remain for the personal data processing industry about what actions would lead to liability in practice. This situation does, in fact, undermine the effectiveness of the law.

Legislators nor courts offer complete solutions

In this section, I used the example of Directive 95/46/EC to exemplify the proposition that the European legal system over data protection is intrinsically incomplete. The incompleteness is determined by the feature of generality, since it was designed to serve general cases. Moreover, legislators can not foresee unambiguously all future changes, developments and obstacles related to data protection issues, and therefore they can not write a law to regulate unambiguously all future contingencies. In fact, legislators have paid and are paying significant efforts (such as amendments) to prevent and to remedy incompleteness. Nevertheless, Directive 95/46/EC was written prior to the developments of and changes in the (in the ICT sector highly volatile) exogenous environment, independent of when or how it is

drafted. It is highly unlikely that it will always be able to offer clear answers to new cases and it is very probable that it will increasingly become incomplete with the life cycles of technological innovations becoming shorter, while concurrently the mechanisms that prepare adaptations of the law require more time.

In this situation, the ECJ steps in and tries to offset the incompleteness. The Court is quite capable of, as the Incomplete Law theory expected, ``adapting existing legal principles to the changing environment'' (Xu & Pistor (2002a):979). In each case, courts, as the theory worried, ``faced the dilemma of adhering to well-established legal principles or extending them to fit the needs of the new types of cases before them'' (Xu & Pistor (2002a):989). But in most cases, judges re-identified the scope of laws to include the new issues. Thus, the scope of the Directive becomes more and more extensive.[97]

However, the analysis above also demonstrates the limitation of courts' rulings when exercising the residual LMLEP. First, in some cases, the amendments even lead to new incompleteness, as each new development creates new questions. Second, the amendments can only come *ex post* and reactive to the specific exogenous change (and, of course, within the bandwidth provided by a reasonable interpretation of the Directive). In this section, I focus on the challenges presented to regulate personal data flow by cloud computing technologies. The analysis showed that prior to the current `big' developments in ICT technology (*e.g.,* cloud computing, mobile internet and telephone converging, etc.), the concept of data protection had been well defined and was in harmony with the current of the time. But along with the exogenous changes that happened in the environment, the existing law lost its clarity on some relevant issues and became ambiguous, especially when facing new ICT. However, the courts, constrained by their reactive enforcement mechanism, cannot help but watch the emergence of a growing protection gap.

The above discussion signaled that Courts do not offer fully satisfactory solutions in the ICT-related area, as it is subject to considerable exogenous changes in very limited time spans. It also signaled

[97] This might be an analogous mechanism as the one Zwenne brings to the fore. He argues, as hinted earlier, that the broader definition of "personal data" may lead to the indefinite expansion of the scope of the Directive, and consequentially, to a complete loss of foreseeability (Zwenne (2013)).

that the resulting ambiguities will decrease the law's effectiveness. Thus, that it is very difficult, perhaps even impossible, to address incompleteness of data protection law solely by depending on courts.

An alternative strategy: the regulator

In response to the problem, rather than frequently changing laws or solely depending on courts' reactions, European policymakers created a unique institutional mechanism, the "data protection authority," to take up the functions required. From the vantage point of the theory of incomplete law, the most important contribution of the Directive 95/46/EC is the creation of a multiple-layered regulatory system that combines *ex ante* rule-making with proactive enforcement powers. This does not mean that court enforcement has been replaced by regulators. Instead, regulators are vested with residual LMLEP to complement court enforcement. In the subsequent analysis, I will analyze the European data regulator's responses to the challenges posed by the incompleteness of Directive 95/46/EC.

The multiple-layered regulators' System

A multiple-layered regulators' system that combines *ex ante* rule making with proactive enforcement powers was created in order to ensure the compliance of data protection law in both European level and National level.

European Data Protection Supervisor (Hereafter: EDPS) is a significant supervisory agent at European level. It is an independent supervisory authority and responsible for making sure compliance of the EU institution and bodies with data protection law (Kuner (2007):7). The EDPS was established in accordance with Article 286 of the Treaty of Amsterdam[98] and Regulation 45/2001.[99] And the status of the EDPS and general conditions for governing were further clarified by Decision 1247/2002 (Kuner (2007):8).[100] EDPS is

[98] European Union (1997)

[99] European Commission (2001)

[100] European Commission (2004)

equipped with legal authority to exercise residual LMLEP. It has substantial influences on policymaking at EU level since it could advise European Commission, European Parliament and the Council on proposals for new legislation or amending (Kuner (2007):9).[101] And the EDPS could intervene ex ante since it could monitor the processing of personal data through prior checking processing operations likely to present specific risks, handling complaints and conducting enquiries (Kuner (2007):9).[102] In each EU institution, a Data Protection Officer is appointed to ensure the internal application of the Regulation in close cooperation with the EDPS.[103]

The EDPS is significant to cooperate national data authorities. The central platform for the cooperation is Article 29 Working Party. The Article 29 W.P. is established in accordance with Article 29 of Directive 95/46/EC. It is an independent advisory body comprised of representatives of national data protection authorities (Kuner (2007):9). The Article 29 W.P. publishes a large amount of opinions and recommendations on various data protection topics, for instance Article 29 Working Party (2009b) which will be analyzed in Chapter 5. Although the documents published by Article 29. W.P. do not have legal binding forces, the documents tend to be quite influential and in effect represent a sort of crystallization of legal opinion (Kuner (2007):9).

Moreover, at the European level, there are some other institutions which play the role of supervisory authority. For instance, the Article 31 Committee which is established in accordance with Article 31 of Directive 95/46/EC could take decisions for which Member

[101] e.g. Opinion of the European Data Protection Supervisor regarding a joint communication by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace

[102] e.g. Several cases before the General Court on the relationship between public access to documents and data protection: Cases T-170/03 (British American Tobacco v. Commission), T-161/04 (Valero Jordana v. Commission), T-194/04 (Bavarian Lager v. Commission) and the subsequent appeal before the Court of Justice, C-28/08 P, T-3/08 (Suárez v. Council), T-82/09 (Dennekamp v. Parliament) and T-190/10 (Egan and Hackett v. Parliament);

[103] The Information is cited from European Commission's official website about the Data Protection Officer, available at: http://ec.europa.eu/justice/data-protection/bodies/ officer.

State approval is necessary (Kuner (2007):10); and the European Ombudsman which is appointed by the European Parliament could investigate complaints from natural and legal persons (Kuner (2007):12).

At the national level, a Data Protection Authority (Hereafter: DPA) must be established and responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive (EC (1995): art.28). These authorities shall act with complete independence in exercising the functions entrusted to them (EC (1995): art.28). National DPAs are granted with substantial powers, although there are many differences in the powers granted by national legislation (Kuner (2007):15). The National DPAs are in charge with, but not limited to, investigating powers, powers of access to files and filing systems, intervention powers, the power to order the blocking, erasure and destruction of data, the power to impose a ban on the processing, the power of warning or admonishing the controller and the powers of sanctions. (European Commission (2003):39-41)

Regulators exercise LMLEP

This section explores the functions of data regulators in Europe, in particular in the deployment of residual LMLEP, both at the European and at the national levels.

The Regulators at European Level

Residual LMLEP are granted to regulators at the European level. In this Section, I focus on the role of Article 29. W.P. in mitigating the incompleteness of data protection law. The Working party is an unique event within the European institutional landscape since no similar agency can be found at European level (Poullet & Gutwirth (2008):2).

Since Article 29. W.P. does not involve in investigating and monitoring data processors' practice, the main efforts that it pays to mitigate the incompleteness of law is to adapt the European data protection legislative framework in accordance with the changing society, especially the new technologies which continuously create new privacy threats (Poullet & Gutwirth (2008):2), which can be seen as

ways to support the development of more complete laws (or law interpretations) to deal with data protection issues. For instance, with the emergence of Facebook, data protection in social networking services became the center of attention. The Working Party has not hesitated to intervene the topic. In 2009, the Article 29 W.P. delivered "*Opinion 5/2009 on online social networking*"(Article 29 Working Party (2009b)), to react the social-network issues at stake. WP 163 sets up very general standards for social networking service providers to comply with. Then the standards are employed by national data regulators to assess different cases. According to the Irish Data Protection Commissioner's audit report (Irish Data Protection Commission (2011)), the national regulators can adapt these rules and shape them to their special needs.[104] However, I could not find any actions that legislators do to adjust the rules in response to observed risks. This is a typical case to show how the Working Party exercises its residual LMLEP to adapt rule-interpretation in response to these technological changes. This reflects the flexibility of regulators on exercising LMLEP at multiple levels. As Xu and Pistor argue, "*regulators need not go through a lengthy lawmaking process, but may, within the scope of their lawmaking rights, adapt and change the law in a simplified procedure...*"(Xu & Pistor (2002a):950), *"...independent of whether violations have occurred, or when others have brought problems to their attention...*"(Xu & Pistor (2002a):954).

What is remarkable is that the Article 29 W.P. is just an advisory body. This means the opinions issued by the Working Party do not have binding legal character (Kuner (2007):10). Nevertheless, according to its rule of procedure, any of its issued documents will be automatically forwarded to EU Commission, to the European Parliament and other related alliances, even though the legislators do not have any motivation to amend any data protection legislative framework (Poullet & Gutwirth (2008):6). Through this way, they do help prepare law for legislators and they do influence law enforcement activities. Although it is one step removed from lawmaking and law enforcement, it thus combines important functions that I have associated with an agent which exercise residual LMLEP. In the light of

[104]Irish Data Protection Commissioner adopted the standards set by the Article 29. W.P. to evaluate Facebook's data protection level.

this performance, Article 29 W.P. bridges the gap left by legislators.

National Data Protection Authority

The National DPAs largely mitigate the incompleteness of data protection law when they exercise the residual LMLEP granted to them. The substantial residual LMLEP are taken up by national DPAs, as the ILT expected, ``in response to the problem of existing law's underdeterrence and the resulting widespread violations of data subjects' rights" (Pistor & Xu (2002b):996). It is not difficult to find cases which national DPA exercises its LEP. For instance, in Germany:

> *On November 23, 2010, the data protection authority (DPA) of the German Federal State of Hamburg imposed a €200,000 fine against the Hamburg-based savings & loan Hamburger Sparkasse due to violations of the German Federal Data Protection Act (the BDSG) for, among other reasons, using neuro marketing techniques without customer consent. The case – which attracted much negative publicity in Germany, including page 1 headlines and "top spots" in television news – may very well influence the assessment of neuro marketing techniques under data protection laws beyond Germany (Cohen (2010))*

Through the enforcement of residual LMLEP, national regulators link the standards and responsibilities for data protection compliance with provisions of Directive 95/46/EC in practice.

The national regulators also exercise extensive residual LMLEP to adapt rules in incomplete law when it deems necessary. Normally, national regulators engage in lawmaking activities proactively and promulgated industrial guidelines. For instance:

> *The German data protection authorities on September 26, 2011 adopted an "Orientation guide – cloud computing." The guide sets out mandatory and recommended content for any agreement between German users of cloud computing services ("customers") and cloud computing service providers. It highlights the customer's responsibility for full compliance with German data protection requirements for the cloud. Based on this orientation guide, customers and providers will have to review existing agreements in the German market.*
>
> *Privacy and data protection compliance has been a challenging and unclear issue for cloud computing customers and service providers. The new German "orientation guide", adopted by the Munich conference of the German data protection authorities gives clear guidance to cloud computing service providers and their customers in the German market. Privacy practitioners can expect that German DPAs will refer to this guide when addressing situations that raise close questions about the application of data protection laws to cloud computing (Stefan.S (2012))*

The lawmaking activities of national regulators enhance overall protection for citizens and increase the visibility of national authorities in society.

Summary:

The current brief overview demonstrates that data regulators are given extensive residual LMLEP. The story in Europe offers important insights into the benefits of a system that offered not only reactive but also proactive enforcement. Similar as regulators in financial, environmental and other areas, data regulators work differently from legislators and courts. Data regulators react to technical development much quicker than legislators who are constrained by procedures. Data regulators also exercise their residual LEP proactively rather than courts who can only apply their residual LEP reactively. Generally, data regulators exert the flexibility of the rules in Directive 95/46/EC. Although the original reason of the emergence of data regulators is not in response to the functional problems of incomplete law, the introduction of regulators can be seen as a successful shift from reactive to proactive law enforcement and reallocation of some lawmaking powers to regulators (Xu & Pistor (2002a)).

Limitation of study

In this Chapter, I have analyzed the problems that confront European laws over data protection issues as example. The analysis used the established framework of incomplete law theory.

The most obvious limitation of the study is its cross-sectorial application of the incomplete law theory. In fact, the incomplete law theory was created to explain/address the legal problems in financial market. The result of my experimental application thus was difficult to foresee. Indeed, Xu and Pistor believe their theory's basic principles are not limited to financial issues, but do apply to any field that "needs to consider the allocation of lawmaking and law enforcement powers"(Pistor & Xu (2002b):936).[105] Nevertheless, the framework has never been applied beyond corporate-law and financial-market regulations. Moreover, the uncertainties of the results increase since the theory is basically derived from the study of legal economy. Incomplete law theory is exploratory in itself. The theory is equally incomplete as incomplete laws are.

Second, when they established and analyzed the theory, Xu and Pistor "*downplay incentive problems different lawmakers and law enforcers may face, including problems of regulatory capture or corruption, in order to highlight the central issues associated with incomplete law*" (Pistor & Xu (2002b):935) Although they recognize that these issues are of great importance, Xu and Pistor do not analyze them and their relations to incomplete law theory.

Third, Xu and Pistor's study used samples of UK, US and German experiences over financial market's development. However, this selection led to a problem for generalization, which may be limited by contextual differences in policy, governance, culture, and history as well as other potential differences in regimes which were not selected in this study. For instance, the analysis in '*Beyond law enforcement-governing financial markets in China and Russia*' shows that the intervention by financial regulators which is recommended by incomplete law theory works less well in transition economies (Pistor & Xu (2004)) Moreover, incomplete law theory can not explain the divergent experiences of Russia and China in developing financial markets

[105]The two authors illustrate that *environmental, safety, food and drug regulation* are fitting fields to adopt this analytical framework.

and the standard enforcement practices (Pistor & Xu (2004)). These findings show us that incomplete law theory is not always relevant (or complete).

Further work is needed to validate the applicability and relevance of the theory and the implications for different legal regimes. Here, I will leave these questions open. On methodological ground, I argue that the theory provides a useful conceptual analysis model for my research where it concerns EU data protection regulation. It produces a useful model for the design of effective enforcement. And it offers me a fresh perspective to peer into the European legal system over data protection issues. My analysis suggest, that the theory is both appropriate and useful as a framework for guiding our analysis.

Conclusion

The chapter deploys the theory of Incomplete Law, which is created by Xu and Pistor. The theory includes three propositions: 1) law is intrinsically incomplete, since lawmakers are unable to foresee all future contingencies and thereby they cannot write a complete law; 2) when a law is incomplete, law enforcement that relies exclusively on courts which enforce laws reactively is not sufficient; 3) regulators, which are vested with proactive law enforcement and residual lawmaking powers, is the optimal solution in an incomplete legal world in order to achieve optimal deterrence effects, given specific conditions (Xu & Pistor (2002a)). Regulators can better respond to the problem of ineffective enforcement caused by incomplete law, since they perform their functions flexible and reactively (Xu & Pistor (2002a):1012).

In this chapter, I applied the theory to the European legal system over data protection issues. The analysis shows that, in Europe (i) lawmakers can not formulate all relevant issues in data protection laws and (ii) courts could not offer satisfactory solutions to incompleteness of law. But the problem caused by incompleteness of law is largely mitigated by an unique European creation: a multiple layered data authorities. I paid attention to the Article 29 W.P. and to the national data authorities (DPAs) that take significant roles in keeping the regulation in step with technologic innovation. My finding is that data regulators are vested with substantial LMLEP. Data regula-

tors are more flexible in adapting law over time than legislatures are. Many challenges brought by technical developments do not make the legislator modify laws because regulators preemptively fill the gaps. Regulators determine the flexibility of these rules by clarifying the conditions that companies should comply with in order to respect the right to personal data keeping up with exogenous changes. As proactive law enforcers, they can initiate actions and exercise enforcement rights in situations where courts, by design, must be passive and wait for others to bring action. Many potentially harmful actions do not make it to the ECJ, because they are caught preemptively by regulators. Regulators enforce laws to recover or prevent injuries caused by harmful actions.

The story in Europe offers important insights into the benefits of a system that not only offers reactive but also offers proactive enforcement. 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 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 ensure effective consequences unless a competent regulatory authority is in place. The lessons drawn from this Chapter call for a rethink of China's legal transplantation strategy.

Until now, the previous three Chapters, from Chapter 2 to Chapter 4, focus on legal design from a positivism perspective. However, this is not enough since there is an underlying tension between performance of law and design of law which requires a binary treatment (Rappaport (2014):7). Without an exploration on the performance of law from a realism perspective, it is unlikely to realize the competences of law which will not be achieved in performance. This would influence China's policymakers to anticipate the effectiveness of imported law. The following Chapter is stressed by this need.