Articles

Incomplete Data Protection Law

By Kunbei Zhang[*]

A. Introduction

The European legal system governing data protection issues is widely regarded as an adequate blueprint for late developers to follow. According to this position, host countries will benefit from receiving the ready-made data protection law because it has already gone through a process of trial and error in Europe. For example, China follows the traditional civil law measures on data protection, such as contractual and tort liability. No Chinese legislation deals specifically with the right to protection of personal data. In China, researchers paid attention to the European legal system, which is regarded as the milestone for data protection. Some vigorously suggest that China should quickly move to enact data protection law based on the model provided by European law.

When Chinese researchers strongly promote the European legal system over data protection issues, they send an underlying message that the quality of European laws is good enough to sufficiently deter violations: Individuals would be prohibited from carrying out harmful actions as soon as the expected law is transplanted to China. From a Chinese perspective, our country could quickly move to enact a similar law following the tone of Europe in order to enhance the efficiency of data protection. But is this a compelling position? Will European data protection laws indeed regulate unambiguously and prospectively? Will European data protection laws provide clear guidance to Chinese judges for resolving data protection-related cases? And will the court-enforced laws sufficiently solve the broad spectrum of problems on data use? Understanding the European enforcement mechanism covering data protection issues, and thereby assessing its efficacy on deterrence, is vital to answering these questions.

In this paper, I attempt to answer these issues from the incomplete law perspective. I focus on the development of the European legal system governing data protection issues and its enforcement system. I deploy an analytical tool from "The Theory of Incomplete Law," contributed by Katharina Pistor and Chenggang Xu, in order to complete this examination. This theory provides a framework for "analyzing the relation between basic features of statutory and case law and the design and functioning of institutions that enforce this

[*] Ph.D. student at eLaw@Leiden, Leiden University's Centre for Law in the Information Society. This paper is part of the author's Ph.D. research at Leiden University. Its title is: "Can Chinese Legislation on Privacy Benefit from Western Experience?" and it is currently under review.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

law."[1] Pistor and Xu developed the theory when analyzing the regulation on financial markets and the need for optimal levels of regulation. They suggest:

> Law is intrinsically 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.[2]

Through the lens of incomplete law theory, I argue that European data protection law is highly incomplete, and its deterrence effect weakens as the development of technology increases the level of incompleteness. When these occasions arise, courts step in to reduce the incompleteness while resolving new cases. But courts can only react to cases that are brought to them, and potential litigants often lack the initiative and resources to effectively address new problems. Therefore, the European legal system regarding data protection issues remains highly incomplete as new and "nasty surprises"[3] continue to challenge Directive 95/46/EC. However, the Regulator, a unique agent in Europe, has emerged to improve law enforcement, and thereby mitigates its incompleteness. I suggest that the construction of a "regulatory agent," beyond legislators and courts, is the "secret recipe" to make the European legal system covering data issues the best practice for data governance.

In this paper, I begin to apply the incomplete law theory to data protection regulations. This paper is organized as follows: First, I will outline the characteristics of incomplete law theory in Section B. In Section C, I will apply the framework to the European legal system over data protection issues. I attempt to analyze the legislative responses to challenges posed by the development of technology. Then, in Section D, I explore the European regulatory framework governing data protection, as it added proactive law enforcement by

---

[1] Katharina Pistor & Chenggang Xu, *Incomplete Law*, 35 N.Y.U. J. INT'L L. & POL. 931, 931 (2002–2003).

[2] Katharina Pistor & Chenggang Xu, *Beyond Law Enforcement: Governing Financial Markets in China and Russia*, *in* BUILDING A TRUSTWORTHY STATE: PROBLEMS OF POST-SOCIALIST TRANSITION 167, 176 (Janos Kornai et al. eds., 2004).

[3] I take this phrase from Jeff Howard's paper, *Environmental Nasty Surprise, Post-Normal Science, and the Troubled Role of Experts in Sustainable Democratic Environmental Decision Making*, 43 FUTURES 182, 182 (2011). The phrase is rather commonly used in papers exploring environmental law issues such as Daniel Farber, *Probabilities Behaving Badly: Complexity Theory and Environmental Uncertainty,* 37 U.C. DAVIS L. REV. 145, 146 (2003). Although there are differences, the surprises happening in data protection are equally nasty as what happens in environmental law.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

regulators to the classic reactive law enforcement by the courts. Finally, I draw conclusions about the efficacy of European data protection laws and the possibility of their legal transplantation to China.

B. The Incomplete Law Theory

The incomplete law theory is inspired by the incomplete contract theory. Xu and Pistor believe that: "[N]ot only contracts but law is inherently incomplete—indeed that the incompleteness problem is more profound for law than for contracts."[4] In fact, the claim that law is incomplete is not a novelty to most lawyers.[5] It has long been recognized in legal literature. The main task of the theory is to address the problems brought by incomplete law, rather than to establish that laws are inherently incomplete.

The incomplete law theory is used primarily in assessing governance functions in financial markets. Xu and Pistor wrote several companion papers analyzing the role of the Regulator in the financial market in order to illustrate the incompleteness of the law.[6] In my analysis, I extend the application of the theory into a new field: Data protection law. First, I will amplify the analytical framework of incomplete law theory. Most of this section's content is concluded from a paper series written by Xu and Pistor. My aim is to draw a picture of the theory, explaining why law is inherently incomplete, and arguing, given incomplete law, how legal institutions intended to reduce enforcement problems may be designed.

I. Law Is Intrinsically Incomplete

Since the theory is called incomplete law, naturally the first questions to arise are: What is a complete law, and what is an incomplete law? To Xu and Pistor, completeness means that obligations "are unambiguously stipulated in the law and the law can be enforced literally provided that evidence is established."[7] 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."[8] If not, the law is incomplete.

---

[4] Pistor & Xu, *supra* note 1, at 937.

[5] The phenomenon that law is incomplete has been long recognized. For instance, Hart argues that law is indeterminate. In fact, indeterminacy of law and incomplete law are different in expression, but equal in argumentation. *See* HERBERT HART, THE CONCEPT OF LAW 128 (1994); Xu & Pistor, *supra* note 1, at 957.

[6] *See, e.g.*, Katharina Pistor & Chenggang Xu, *Fiduciary Duty in Transitional Civil Law Jurisdictions: Lessons from the Incomplete Law Theory* (ECGI Law, Working Paper No. 01/2002, 2002); Katharina Pistor & Chenggang Xu, *Law Enforcement Failure Under Incomplete Law: Theory and Evidence from Financial Market Regulation* (LSE STICERD, Working Paper No. TE/02/442, 2002).

[7] Pistor & Xu, *supra* note 1, at 938.

[8] *Id.*

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

Nevertheless, Xu and Pistor argue that laws cannot be complete since they have in their "genes" 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."[9] For legislation, incompleteness is the norm.

Precluding bad drafting, most of the time incompleteness is caused by this "gene" in the law-making process, which universally contributes to its intrinsic incompleteness. Normally, legislators give their best effort in designing a law: An extensive amount of time is spent on consultation, appraisal, assessment, preparation, modification, and so on. However, "Even the best, social welfare maximizing, lawmaker cannot write law that is fully complete, because lawmakers cannot foresee all future contingencies," nor can they correctly predict their probabilities.[10]

Of course, I cannot definitely preclude the possibility of writing more complete law when legislators are well equipped with the necessary resources and render their best efforts. For instance, legislators can be asked to provide legislative changes in order to make an incomplete law more complete. Indeed, a thus-modified law may remain complete for some time when sufficient expertise is assembled.[11] Nevertheless, it is difficult for an even carefully designed law to remain complete for a long time. The reason is simple but fundamental (and implied in the foregoing): Legislators can neither predict nor shape the future. As legal philosopher H.L.A. Hart argues, "it is a feature of the human predicament that we simply cannot regulate, unambiguously and in advance, some sphere of conduct by means of general standards to be used without further official direction on particular occasions."[12] The world is simply too complex.[13] This determines the "destiny" of any law: Incompleteness cannot be escaped. As time goes on, new conditions that revise the law's efficacy, which the legislator did not, or could not, contemplate will undoubtedly arise, increasing its incompleteness once more.[14]

---

[9] *Id.* at 938–39.

[10] Pistor & Xu, *supra* note 2, at 170.

[11] *See id.* at 175.

[12] HART, *supra* note 5, at 128.

[13] 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.

Id.

[14] *See* Pistor & Xu, *supra* note 2, at 175.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

Moreover, some incomplete laws are enacted to be incomplete by the legislator's "deliberate design."[15] 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 of cases."[16]

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."[17] Yet on the other hand, this contributes to incomplete law, since law becomes too general to provide specific standards and procedures for each case. This can "affect the outcome for a variety of cases that may arise in the future."[18]

II. Two Types of Incompleteness

Xu and Pistor classify incomplete laws into two categories based on the motives that triggered incompleteness. They stipulate that categorizing laws based on types of incompleteness brings forth new ideas for legal study.[19]

1. Type I

Type I incomplete law refers to one that "broadly circumscribes outcomes without identifying particular actions, or enumerates only a few actions."[20] The most representative incomplete law in Type I, according to Xu and Pistor, is tort law. The authors state:

> 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

[15] Pistor & Xu, *supra* note 1, at 932.

[16] *Id.* at 938–39.

[17] *Id.* at 939.

[18] *Id.*

[19] *See id.* at 941.

[20] *Id.*

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

> open the question of what form actions might take that will trigger liability under the law.[21]

2. Type II

Type II incomplete law refers to one that "specifies the actions that shall be prevented but fails to capture all relevant actions."[22] As Xu and Pistor 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."[23]

III. Different Institutional Mechanisms Respond to the Incompleteness

When a law is incomplete, it is required to interpret and develop existing laws in order to deal with new, not yet covered cases. According to Xu and Pistor, in this situation, new powers must arise, such as "residual lawmaking and law enforcement powers," [24] (hereinafter residual LMLEP). Xu and Pistor further suggest that incompleteness can, to a large extent, be reduced when the residual LMLEP is appropriately allocated.[25]

The residual lawmaking power (hereinafter residual LMP) is "power to interpret existing law, to adapt it to changing circumstances, and to extend its application to new cases."[26] The original lawmaking power (hereinafter original LMP) is "the power to make new law from scratch."[27] Universally, original LMP is granted to legislators, while original LEP is granted to courts. Xu and Pistor argue that it is sufficient to allocate original LMLEP to legislators and courts if law is complete.[28] This is because legislators made a law permanently efficient enough to guide conduct and deter violations. In such a case, courts could decide any case by just following the contents in the permanently complete law. However, Xu and Pistor have proven that law is permanently incomplete, rather than

---

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.* at 938.

[25] *See id.* at 935.

[26] *Id.* at 933.

[27] Katharina Pistor & Chenggang Xu, *The Challenge of Incomplete Law and How Different Legal Systems Respond to It*, *in* BIJURALISM: AN ECONOMIC APPROACH 71, 78 (Andre Breton & Anne des Ormeaux, eds., 2006).

[28] *See* Pistor & Xu, *supra* note 1, at 946.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

complete. When law is incomplete, it is insufficient to merely allocate the original LMLEP. Residual LMLEP arises and must be allocated explicitly.

In most cases, residual LMLEP can be allocated to two different agents: Courts and regulators.[29] In fact, agencies qualified to exercise residual LMLEP are not limited to regulators. For instance, self-regulators may be allocated to exercise residual LMLEP. In the realm of data protection, it is widely believed that self-regulators, from the Theory of Incomplete Law's perspective, are allocated with these residual powers in the United States. But when the theory was first established, the authors limited their analysis to regulators generically defined. In the following years, Xu and Pistor also analyze the efficacy of the approach to grant residual powers to agencies beyond courts and regulators. In my research, I limit my analysis to regulators generically defined.

These two institutions both have merits and demerits. How can policymakers decide which institution to choose? Herein lies a significant contribution of the theory. The incomplete law framework helps us determine which institution is to be preferred, under certain conditions and constraints.[30]

1. Courts

Courts are allocated with substantive residual LMLEP. When law is incomplete, courts step in to clarify the incompleteness while addressing a case. Through interpretation and further development of existing laws, courts decide how to enforce "old" law to new cases, thus exercising residual LMLEP. Each case decided reflects effort by courts to optimize the relative completeness of the law. In fact, there is a significant difference between the two major legal families in the world concerning how residual LMLEP has been allocated to courts.[31] In Common Law countries, "[J]udges not only hold extensive residual lawmaking powers; they are also vested with original lawmaking powers,"[32] while in Civil Law countries, courts are constrained to exercising residual LMLEP.[33] Yet overall, and traditionally, courts are the natural institutions to hold and exercise residual LMLEP. However, as an enforcement agent, courts have a weakness, which leads to inefficient enforcement; courts

[29] *See id.*

[30] *See id.* at 961.

[31] *See id.* at 946.

[32] *Id.* at 947. The two authors mentioned that there is a substantial debate on 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 (1976). 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 fill in some gaps in the law. This lawmaking power is one of their major functions. *See* Pistor & Xu, *supra* note 1, at 947.

[33] *See* Pistor & Xu, *supra* note 1, at 947.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

do not "have the power to take action *sua sponte* even when such an intervention might be desirable." [34] Shortly, courts enforce laws reactively. Thus, their range of action is insufficient to ensure optimal law enforcement of incomplete laws, and the insufficiency worsens as the expected damages from harmful actions increase.[35]

2. Regulators

A regulator represents an alternative institutional approach to addressing problems brought on by incomplete law. The manner in which regulators exercise residual LMLEP is very different from the way courts do: Regulators can adapt and enforce the completeness of laws proactively through various means,[36] including, but not limited to, "controlling entry, monitoring activities, initiating investigations, enjoining actions, and initiating the administration of sanctions against violators."[37] Police officers, as illustrated by Xu and Pistor, are an example of regulators. Police can "monitor behavior and seek to prevent damages by enjoining actions that are likely to cause harm."[38] It is better for police to intervene before harm has occurred, for they need not wait until harm has actually occurred in order to act.[39] Supervisory authorities in stock markets and the banking industry are also regulators that exercise substantive LMLEP. They are the main objects for observation by Xu and Pistor.

Xu and Pistor argue: When law is highly incomplete and violations of the law may result in substantial harm, it is optimal to allocate law enforcement rights to regulators rather than courts.[40] This argument is based on the fact that regulators can exercise the powers both *ex post* and *ex ante*, unlike courts, which in most cases "make and enforce the law ex post, that is, after harm has occurred."[41] Also, judges must wait for parties to bring motions. Otherwise, judges cannot take action at all.[42]

---

[34] *Id.* at 948.

[35] *See id.* at 949; Paul R. Milgrom, Douglass C. North & Barry R. Weingast, *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs*, 2 ECON. & POL. 1, 5–6 (1990).

[36] *See* Pistor & Xu, *supra* note 1, at 948.

[37] *Id.*

[38] *See id.*

[39] This relates to the problem of legitimate pro-active regulatory behavior, which is resolved in the practice in politics (both Europe and China), a topic beyond this paper's scope.

[40] *See* Pistor & Xu, *supra* note 1, at 951–952.

[41] *Id.* at 949.

[42] The two authors note that courts can also be asked to prevent harmful actions from taking place: For example, to file a motion for preliminary injunction. However, this procedure is still based on another party's motion. *See id.*

In contrast, regulators can trigger enforcement processing *ex ante* and can exercise residual LMP to respond to observed changes more directly (within the scope of their lawmaking rights),[43] and thereby, an incomplete law's efficacy can be enhanced. Therefore, some believe that regulators can exercise residual LMLEP more flexibly and in a wider range of situations than courts are able to.[44] Regulators also can "correct for past errors on their own initiative and in a flexible and responsive manner."[45] Based on the foregoing comparison, it is more advantageous to let the Regulator as an institution hold and exercise residual LMLEP than the court.

But are these advantages visible in all situations? In fact, regulators may make mistakes by either over- or under-enforcing the law. "Over-regulation occurs when a regulation imposes costs that outweigh the benefits of proactive law enforcement [by courts]."[46] Over-regulation also occurs when it chills "too many potentially beneficial actions or when well-intended regulation stifles economic activities in other ways."[47] According to Xu and Pistor, "Regulators may also under-enforce because they face resource constraints, misallocate their resources, or fail to detect [risks of] harmful actions."[48] Thus, regulators are relatively superior to courts only under certain conditions and constraints.[49]

We then turn to the issue of 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). These concepts support the analytical framework of incomplete law theory.

---

[43] *See id.* at 950.

[44] *See id.* at 1012.

[45] *Id.* at 951.

[46] *Id.* 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 the costs society incurs when regulators either over- or under-enforce the law. *See id.*

[47] *Id.*

[48] *Id.*

[49] *See id.* at 961. On the tradeoff between monitoring and investigating, and the cost implications of these regulatory enforcement mechanisms, see Dilip Mookherjee & Ivan 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, but merely monitored. Larger offenses should be investigated in accordance with their severity, and fines should be maximized. *See id.*

Standardization:

> [R]efers 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.[50]

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.[51]

According to Xu and Pistor, regulators are only the superior option to allocate residual LMLEP when these two factors are considered and their conditions 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.[52]

---

[50] Pistor & Xu, *supra* note 1, at 952.

[51] *Id.* at 953–54.

[52] Of course (yet, off-topic for my research), 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.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

IV. Summary

The Incomplete Law Theory can be summarized in three propositions: (1) All law is intrinsically incomplete; (2) the optimal approach to incompleteness is to allocate residual LMLEP; and (3) regulators conditionally have advantages over courts for holding and exercising residual LMLEP—for example, when actions can be standardized, and when substantial harm is likely to occur.

The first proposition lays the foundation of the theory, and the following two supply an analytical framework that can help researchers to assess the design of legal institutions, as well as the efficacy of law enforcement. Xu and Pistor believe their theory is of wide interest to legal research. They stipulate that it can be used to compare legal systems (such as the authors' comparison of courts' residual LMLEP in the Civil Law and Common Law systems) and to analyze lawmaking and law enforcement in diverse jurisdictions (as demonstrated in their companion paper "Beyond law enforcement-governing financial markets in China and Russia," through which the theoretical framework is employed to analyze the financial regulation mechanism in Russia and China).[53]

In the remaining section of this paper, I will analyze the European legal system governing data protection issues through the lens of the Incomplete Law Theory. I seek to explore the effectiveness of lawmaking and law enforcement in the data protection field—a field that was, and remains, highly susceptible to technological changes. This assessment aims to discover whether the European legal arrangement indeed provides the high level of protection widely attributed to it.

C. Incomplete Law Theory and the Data Protection Field: Examples from Directive 95/46/C

In this section, I take the "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" (hereinafter "Directive 95/46/EC") as a representative piece of law-making that assesses resilience to incompleteness.[54] I do not select this Directive to illustrate the quality of the Directive's drafting, but to illustrate the European legal system's abilities to deal with "unforeseen contingencies."

[53] *See* Pistor & Xu, *supra* note 2.

[54] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

I. Directive 95/46/EC Is Intrinsically Incomplete

Since it was released, Directive 95/46/EC has been long assumed an engine for the emergence of a global data protection regime.[55] This Directive addresses the protection of personal data from a number of different perspectives and covers multiple situations. Nevertheless, it has not captured "all possible actions" that can violate a data subject's rights. The Directive is incomplete.

Fundamentally, the incompleteness of Directive 95/46/EC does not mean the European legislators have drafted the law badly. Rather, the intrinsic feature of this Directive causes it: It is a general law. A general law means this Directive was designed to "serve a larger number of addressees and to cover a much greater variance of cases," and typically have much longer duration.[56] Directive 95/46/EC was not a "single-case-law," which aimed to apply to a specific case in a short time.[57] As I analyzed above, the feature of generality determined that this Directive, from the first beginning, has been accompanied with "incompleteness."

Moreover, Directive 95/46/EC tries to regulate a field which is closely linked with technology. According to Incomplete Law Theory, data protection law may be more incomplete than others, since it is affected by a high pace of technological change:[58] "The reason is that 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."[59] Consequently, it is even more incomplete than other areas that are not featured by continuously "exogenous changes."

When a Directive is incomplete, it cannot effectively deter all situations not encompassed within it. This may trouble both individuals and law enforcers to determine—as the two authors pointed—"whether these actions fall within the scope of the relevant laws."[60] For example, data-users may find it difficult to determine punishments or to foresee the level of punishments when contemplating actions. If they are too careless, and proceed on the assumptions that the law will not apply to them, actions resulting in harm, similar to the harm that the incomplete law aims to protect against, may occur. Alternatively, they may

[55] *See* Michael Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SECURITY REP. 508 (2008).

[56] Pistor & Xu, *supra* note 1, at 938.

[57] *See id.* at 939.

[58] *See id.* at 933.

[59] *Id.*

[60] *Id.* at 949.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

worry their actions fall within the scope of Directive 95/46/EC and refrain from doing what otherwise would be considered perfectly legitimate business. In either case, the deterrence effect of the law is not optimal. In the first case, the law under-deters;[61] in the second, it over-deters.[62]

To law enforcers, the trouble is to decide whether Directive 95/46/EC can be applied to a specific "new" case. In fact, the worries about the incompleteness of Directive 95/46/EC include uncertainties about some of its particulars remaining in force in a world where their enjoinment could concern potential harmful actions (and not their prevention).

Under such conditions, it becomes important to address incompleteness in order to ensure clear levels of punishments. Courts have to step in and fill the gaps left by incomplete Directive 95/46/EC. I will also do some research based on cases that were decided by the European Court of Justice in Luxembourg (hereinafter ECJ)[63] that are also referring to Directive 95/46/EC. The analysis of the case law is to answer the question: Can the courts reactive enforcement adequately remedy this incompleteness?

II. Legal Enforcement by Courts Cannot Achieve Optimal Levels

The case law created by the ECJ plays an important role in shaping the character of data protection in Europe.[64] The ECJ tries to cope with challenges of rapid technological changes, since a major part of judicial reasoning is to determine whether Directive 95/46/EC, and its companion directives or cases law, could extend to new cases. From the perspective of Incomplete Law Theory, substantial LMLEP has been allocated to the ECJ; it can interpret and adapt community laws to make sure they are applied in the same way in all EU countries. The ECJ exercises these powers when settling legal disputes or answering prejudicial questions addressed to it by member-state courts. It establishes the standardized interpretation of Directive 95/46/EC that member state's courts must take into account when applying national law.

I now explore how courts exercise their LMLEP, which is at the center of our analysis. The background and legal contents are cited from the ECJ's judgment.

[61] *See id.*

[62] *See id.*

[63] The information about the ECJ is harvested from its official website. *See* European Union, *Court of Justice of the European Union*, http://europa.eu/about-eu/institutions-bodies/court-justice/.

[64] According to a 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* European Comm'n, *Data Protection Officer* (Nov. 4, 2012), http://ec.europa.eu/dataprotectionofficer/legal_framework_en.htm.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

1. 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[65]

(a) Directive 95/46/EC includes a provision that its purpose is to ensure free personal data flow from one Member State to another.[66] The dispute referring to the prejudgment sent to the ECJ questioned whether Directive 95/46/EC is applicable to issues that have no relation with the issue of internal market harmonization.[67]

(b) In this judgment, the ECJ held that Directive 95/46/EC should apply to cases, even those that have no link with the issue of harmonizing internal market.[68]

(c) The outcome of the preliminary ruling reduced Type I incompleteness. ECJ's judgment extended the scope of the applicability to cover any actions, which differs from the expression of principles and criteria laid down in the Directive 95/46/EC.[69]

2. Case C-101/01: Criminal Proceedings Against Lindqvist[70]

(a) 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, whether processing data such as "giving their telephone number, or information regarding their working conditions and hobbies" is covered by one of the exceptions in Article 3(2), what kind of information concerns health, whether a transfer of data to a third county includes the occasion that load personal data onto a page stored on a server…established in a Member State and thereby making those data accessible to anyone who connect the Internet including people from third country, whether the provisions in Directive 95/46/EC bring about a restriction which conflicts with the general

[65] Joined Cases Rechnungshof v. Rundfunk, CJEU Case C-465/00, Neukomm v. Rundfunk, CJEU Case C-138/01, and Lauermann v. Rundfunk, CJEU Case C-139/01, 2003 E.C.R. I-04989 [hereinafter Joined CJEU Cases C-465/00, C-138/01, and C-139/01].

[66] *See* Council Directive 95/46, *supra* note 54, at para. 3.

[67] *See* Joined CJEU Cases C-465/00, C-138/01, and C-139/01, *supra* note 65, at paras. 31–47.

[68] *Id.* at paras. 48–101.

[69] *See id.* at para. 100.

[70] Lindqvist, CJEU Case C-101/01, 2003 E.C.R. I-12971. Reference for a preliminary ruling from the Göta hovrätt in the criminal proceedings against Bodil Lindqvist.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

principle of freedom of speech, whether it is permissible for the Member State to provide for greater protection for personal data than required by Directive 95/46/EC.[71]

(b) The ECJ ruled: (1) information on an Internet page which could identify data subjects by any means falls into the scope of the Directive; (2) the information about "injured foot" is information concerning health; (3) there is no transfer of data to a third country within the meaning of Article 25 of Directive 95/46/EC 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; (4) 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; and (5) a member state could extend the scope of data protection law.[72]

(c) The outcome of the preliminary ruling largely reduced Type I incompleteness, but increased Type II incompleteness. Each new extended scope will eventually give rise to new litigation, as technological development will 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.

3. Joined Cases C468/10 and C469/10: Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C469/10) v. Administración del Estado[73]

(a) 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. The dispute referred for preliminary rulings concerns whether Member States' national laws are entitled to add extra conditions to those required by Directive 95/46/EC.

[71] *Id.* at paras. 12–17.

[72] *Id.* at paras. 19–99.

[73] Joined Cases Asociación Nacional de Establecimientos Financieros de Crédito v. Administración del Estado, CJEU Case C-468/10, and Federación de Comercio Electrónico y Marketing Directo v. Administración del Estado, CJEU Case C-469/10, 2011 E.C.R. I-12181. In the case, Spain's Royal Decree 1720/2007 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 judgment.

(b) The ECJ responded:

> Article 7(f) of Directive 95/46 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 generalised way, any processing of data not appearing in such sources.[74]

(c) The outcome of the preliminary ruling reduced the Type I incompleteness of Directive 95/46/EC.

4. C-518/07 European Commission Supported by European Data Protection Supervisor v. Federal Republic of Germany[75]

(a) Directive 95/46/EC includes a provision (Article 28) that the data protection authorities must be able to exercise their entrusted functions independently.[76] The dispute in the case is how "independent" independent agencies should be.

(b) The ECJ ruled:

> [B]y 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

[74] *Id.* at para. 49.

[75] European Comm'n v. Fed. Republic of Ger., CJEU Case C-518/07, 2010 E.C.R. I-01885.

[76] *See* Council Directive 95/46, *supra* note 54.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

> obligations under the second subparagraph of Article 28(1) of Directive 95/46.

(c) The outcome reduced the Type I incompleteness of Directive 95/46/EC.

5. C-553/07 College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer Netherlands[77]

(a) Directive 95/46/EC includes a provision (Article 12) to entrust data subjects the right to access.[78] However, the provision does not indicate "any time period within which it must be possible for those rights to be exercised."[79] The dispute referred to the preliminary ruling concerns whether member states could impose a time restriction in their national law.[80]

(b) The ECJ ruled that 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.[81] Nevertheless, the storage period must consider both a data subject's interests and the burden on data controllers for storage.[82]

(c) The outcome of the preliminary ruling ruled the Type II incompleteness of the Directive, but increased Type I incompleteness.

6. C-524/06 Heinz Huber v. Bundesrepublik Germany[83]

(a) Directive 95/46/EC has a provision (Article 7 (e)) that requires data processing for a task carried out in the public interest or in the exercise of official authority.[84] The dispute

[77] College van burgemeester en wethouders van Rotterdam v. Rijkeboer, CJEU Case C-553/07, 2009 E.C.R. I-03889 [hereinafter *Rijkeboer*, CJEU Case C-553/07].

[78] Council Directive 95/46, *supra* note 54.

[79] *Rijkeboer*, CJEU Case C-553/07, *supra* note 77, at para. 28.

[80] *See id.*

[81] *Id.* at para. 70.

[82] *See id.*

[83] Huber v. Bundesrepublik Deutschland, CJEU Case C-524/06, 2008 E.C.R. I-09705 [hereinafter *Huber*, CJEU Case C-524/06].

[84] Council Directive 95/46, *supra* note 54.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

referred to in the preliminary ruling concerns whether the provision could be enforced on the grounds of nationality.[85]

(b) The ECJ ruled:

> [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.[86]

(c) The outcome of the preliminary ruling reduced the Type I incompleteness of Directive 95/46/EC, but may increase Type II incompleteness.

7. C-73/07 Tietosuo javaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy[87]

(a) Directive 95/46/EC provides exemptions for processing personal data for journalistic purposes.[88] The dispute referred to in the preliminary rulings concerns which circumstances the activities at issue may be regarded as the processing of data carried out solely for journalistic purposes and thus exempt or derogate from data protection.[89]

(b) The ECJ ruled that the notion of journalistic activities should encompass all activities whose "object is the disclosure to the public of information, opinions or ideas, irrespective 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.[90]

(c) The way the ECJ ruled concerning Type I incompleteness might increase Type II incompleteness of Directive 95/46/EC. The interpretation broadly encompassed all

[85] *See Huber*, CJEU Case C-524/06, *supra* note 83, at para. 2.

[86] *Id.* at para. 82.

[87] Tietosuojavaltuutettu v. Oy, CJEU Case C-73/07, 2008 E.C.R. I-09831 [hereinafter *Tietosuojavaltuutettu*, CJEU Case C-73/07].

[88] Council Directive 95/46, *supra* note 54.

[89] *See Tietosuojavaltuutettu*, CJEU Case C-73/07, *supra* note 87, at para. 2.

[90] *Id.* at para. 61.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

journalistic activities, but each of the conditions the ECJ designed covered a particular situation, such as medium, format of data, nature of those activities.

8. Joined Cases C-317/04 and C-318/04 (judgment of 30 May 2006/European Parliament v. Council of the European Union)[91]

(a) Directive 95/46/EC has a provision (Article 26) referring to non-Member States' data protection level.[92] The dispute in the case concerns whether the Commission could validly adopt the decision on adequacy on the basis of Directive 95/46/EC.[93]

(b) The ECJ ruled: "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.[94]

(c) The outcome of the judgment did not reduce the Type I incompleteness of the Directive 95/46/EC.

If compared with solely depending on legislators to update law, the ECJ's efforts enhanced the efficiency of lawmaking. Still, do the ECJ's reactive enforcements adequately remedy this incompleteness? My reading of the case law does not suggest that the problems of incomplete law can be adequately remedied through the courts' reactive enforcement. Rather, I found that in some cases, the recoveries offered by the ECJ even lead to further incompleteness. Additionally, technological innovations challenge court enforcement. I analyze this below.

III. The Weakness of the Courts' Enforcements: Challenges Brought by Cloud Computing

From the analysis above, courts' efforts largely reduced the incompleteness of Directive 95/46/EC. Nevertheless, courts present a weak exercise of residual LMLEP. Particularly, problems may arise with the invention of new technologies. At the time, cloud computing strongly challenged courts' enforcement.

---

[91] Joined Cases European Parliament v. Council of the European Union, CJEU Case C-317/04, and European Parliament v. Comm'n of the European Cmtys., CJEU Case C-318/04, 2006 E.C.R. I-04721 [hereinafter Joined CJEU Cases C-317/04 and C-318/04].

[92] Council Directive 95/46, *supra* note 54.

[93] *See* Joined CJEU Cases C-317/04 and C-318/04, *supra* note 91, at para. 2.

[94] *Id.* at para. 57.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

The challenges are mainly brought by the premise underlying the Directive's focus. The obligations established by the Directive mainly apply to the "controller," who "determines the purposes and means of processing personal data."[95] In the Directive, "processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[96]

The premise underlying this definition, as Ursula Widmer identified, is that there is always a clear location of where personal data presents itself, by whom it is processed, and who is responsible for the processing.[97] As formed by Article 4 of Directive 95/46/EC, data controllers are the ones who process personal data on the territory of the Member State or the territory of several Member States; or in a place where member states' "national law applies by virtue of international public law," or who are not "established" in any member state but, for purposes of processing personal data, make use of equipment (or "means," in some languages) situated in the member state.[98] The definition was sufficiently complete to cover data controllers that existed at the time of the Directive's enactment. When facing the technology of the time, the Directive's technological horizon, based on location, fitted business practices and the environment it generated for personal data-processing, which was featured by relational databases and "island" computing.

However, Directive 95/46/EC's perspective has proven to be technologically quite narrow, particularly, from the perspective of cloud computing that emerged later. Cloud computing strongly challenges Directive 95/46/EC. As International Association of Privacy Professionals' announcement described, "Cloud computing involves data and data applications stored and processed remotely, often in places far away, sometimes in multiple places, and in places with differing legal regimes."[99] This feature blurs the demarcation lines between data users, collectors and processors. As stated, "Generally, cloud users who process personal data in the cloud will be controllers unless an exemption

[95] Council Directive 95/46/EC, art. 2(d), 1995 O.J. (L 281) (EC).

[96] *Id.* at 2(b).

[97] *See* Ursula Widmer, *Cloud Computing and Data Protection*, LAW BUSINESS RESEARCH LTD. (July 2009), http://whoswholegal.com/news/features/article/18246/.

[98] *See* Council Directive 95/46/EC.

[99] *Upcoming EU Cloud Strategy Announced: Application of Local Privacy Laws Remain an Issue, To Be Explored at IAPP Navigate on September 14*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Sept. 1, 2011), http://www.hldataprotection.com/2011/09/articles/international-eu-privacy/upcoming-eu-cloud-strategy-announced-application-of-local-privacy-laws-remain-an-issue-to-be-explored-at-iapp-navigate-on-september-14/ [hereinafter *Upcoming EU Cloud Strategy Announced*].

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

applies, e.g. private use only, as with purely personal webmail. Cloud service providers are generally treated as processors." [100] But the roles taken by cloud service providers are not limited to being processors, they may also and concurrently, in some situations, turn into controllers.[101]

Second, the operational principles of cloud computing fundamentally conflict with the premise formed by Article 4. As described, "If a customer uses an e-mail service based on cloud computing, the customer's data can be stored anywhere in the world, depending on where the servers are located,"[102] and without an explicit chain of contractual transfers of data-protection responsibilities. In the cloud-computing era, it is no longer possible to say where the data is at a certain moment, and by whom and how it is being processed. Thus, distinctions can be made between the technologies regulated by law and the technologies are not—and that need to be regulated. These distinctions cause problems for Directive 95/46/EC to provide clear formulations. Incompleteness of both types comes to the forefront. As a matter of fact, the emergence of new technology like cloud-computing services has set the EU legislature buzzing.

According to the types of incompleteness as categorized by Xu and Pistor, Type II incompleteness results. This leaves open the question of the scope of applicability.

Naturally, cloud computing should not become a technology that can evade data protection requirements. However, Directive 95/46/EC does not include any statement about the irrelevance of location. Indeed, the European Commission, which is vested with substantial original LMP, proclaimed that an essential pillar of EU citizens' privacy rights is "protection regardless of location" which has obvious implications for the cloud.[103] Still, messages from the European Commission stated that it would take more time for the legislatures to complete current laws.[104] The message inherently signaled to the ECJ that it should reconsider the applicable scope of the Directive 95/46/EC in a preliminary ruling,[105] as it is not to be expected that the legislature will fill the gap by quickly promulgating a more complete law. Therefore it is provisionally left to the ECJ to determine whether the

[100] For example, when they determine the "means" of processing. W Kuan Hon & Christopher Millard, *Cloud Computing and EU Data Protection Law, Part One: Understanding the International Issues*, COMPUTERWORLDUK (Sept. 28, 2011), http://www.computerworlduk.com/blogs/cloud-vision/-cloud-computing-and-eu-data-protection-law--3570958/.

[101] For example, when they determine the "means" of processing. *See id.*

[102] Widmer, *supra* note 97.

[103] *See* Viviane Reding, Vice-President, Eur. Comm'n & EU Justice Comm'r, Review of the EU Data Protection Framework (Mar. 16, 2011).

[104] *See* Windmer, *supra* note 97. *See also, Upcoming EU Cloud Strategy Announced*, *supra* note 99.

[105] *See* Windmer, *supra* note 97.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

existing standards of conduct formed by Directive 95/46/EC can be understood so as to support a more adequate realization of data protection under cloud computing.[106]

This highlights significant limitations of courts for exercising LMLEP. As a neutral arbiter, the ECJ is passive and can only exercise its LMLEP after a motion has been filed. 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 has been brought to the ECJ (until now). ECJ has to remain passive until others bring actions, even though judges may have designed a strategy on how to exercise LMLEP. Thus, although it is possible that the ECJ would stretch the scope of Directive 95/46/EC to encompass cloud-computing, uncertainties remain about what actions would lead to liability. This situation does, in fact, undermine the deterring effects of the law.

IV. Summary: Neither Legislators nor Courts Offer Fully Satisfactory Solutions in this Area

The case studies show us that the scope of Directive 95/46/EC's applicability has changed over time. This is the natural result of continuous, exogenous innovations and related changes in the availability and ubiquity of ICT functionality. In fact, prior to the current "big" developments in ICT technology (e.g., cloud computing, mobile internet, and telephony converging, etc.), the concept of data protection had been well-defined and was relatively complete. But along with the exogenous changes that happened in the environment, the existing law lost its clarity on some relevant issues and became ambiguous. This demonstrates that, as Xu and Pistor argued, "[t]echnological change may render incomplete laws that were fairly complete before."[107]

This incompleteness, as in Directive 95/46/EC, does not serve to illustrate errors or poor drafting by the legislature. In fact, legislators have made and are making significant efforts to prevent and to remedy incompleteness. Nevertheless, from the perspective of Incomplete Law Theory, data protection law exists prior to the developments of—and changes in—the highly volatile, exogenous environment in the ICT sector, independent of when or how it is drafted. It is highly unlikely that it will always offer clear answers to new cases and highly probable that it will increasingly become incomplete with the life cycles of technological innovations becoming shorter, while the mechanisms that prepare adaptations of the law still require more time.

In this situation, the ECJ steps in and tries to offset the incompleteness. As the discussed cases show, courts proved quite capable of, as the Incomplete Law Theory expected, "adapting existing legal principles to the changing environment."[108] In each case, courts—

[106] *See id.*

[107] Pistor & Xu, *supra* note 1, at 943.

[108] *Id.* at 979.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

as the theory worried—"faced the dilemma of adhering to well-established legal principles or changing them to fit the needs of the new types of cases before them."[109] In most cases, judges re-identified the scope of laws to include the new issues. Thus, the scope of the Directive becomes more extensive than previous.

Nevertheless, the analysis above also demonstrates the limitation of courts when exercising the residual LMLEP. As the theory stated, the courts only can respond ex post and to the specific exogenous change within the bandwidth provided by a reasonable interpretation of a law.[110] The recoveries provided by courts always come, as the theory pointed, when "the alleged actions have taken place and resulted in harmful outcomes."[111] In some cases, the recoveries even lead to new incompleteness, as each new development creates new questions. In some other cases, for example in the case of cloud-computing, if no case is brought, the ECJ cannot help but watch harmful actions damaging the right to personal data protection, supposedly established in accordance with Directive 95/46/EC.

The above discussion signaled that courts do not offer fully satisfactory solutions in the ICT-related area, as is subject to considerable exogenous changes in very limited time spans. It also signaled that the resulting ambiguities in the law would decrease its deterring effect. Thus, it is very difficult, perhaps even impossible, to address incompleteness solely based on the courts.

D. The Alternative Strategy to Overcome Deterrence Failure: Data Regulators[112]

I found that the data protection area is subject to continuously-occurring technical changes. It is difficult to get rid of incompleteness despite efforts to adjust. The discussion above has shown that neither legislators nor courts offer satisfactory solutions to incompleteness.

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 Incomplete Law Theory, 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 is a unique phenomenon in Europe. This does not

[109] *Id.* at 989.

[110] *Id.*

[111] *Id.* at 949.

[112] In this paper, what seems to me to be the most important aspect of the "data regulator" concept is that parts of the regulatory powers as identified in incomplete law theory are delegated by the legislator and the administration to institutions that have thus gained regulatory agency that allows them to react more adequately, quickly, and with expertise to emerging (mal)practices.

mean that regulators have replaced court enforcement. 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. I seek to explore the effectiveness of lawmaking and law enforcement in the hands of regulators in an area highly susceptible to exogenous changes.

I. The Multi-Layered Regulators' System

A multi-layered regulators' system that combines ex ante rulemaking with proactive enforcement powers was created in order to ensure the compliance of data protection law in both European level and national level.

At the European level, regulators include European Data Protection Supervisor (EDPS).[113] It is an independent regulatory body and responsible for making sure compliance of the EU institution and bodies with data protection law.[114] According to the EDPS, its general objective is to ensure that the European institutions and bodies respect the right to privacy when they process personal data and develop new policies. Generally, the EDPS's main fields of work include supervision,[115] consultation,[116] and cooperation.[117]

The EDPS is significant to cooperate national data authorities. The central platform for the cooperation is the Article 29 Working Party (hereinafter Article 29 W.P.) The Article 29 W.P. was established in accordance with Article 29 of Directive 95/46/EC. It is an independent advisory body comprised representatives of national data protection authorities.[118] The Article 29 W.P. publishes a large amount of opinions and recommendations on various data protection topics. 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

[113] The position was set up according to the Article 286 of the Treaty of Amsterdam and Regulation (EC) No 45/2001 of the European Parliament. *See* Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, Oct. 2, 1997, 1997 O.J. (C 340) art. 286.; Commission Regulation 45/2001, 2001 O.J. (L 8/1).

[114] *See* Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* 7, OECD (Dec. 8, 2011), http://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en.

[115] *See Members & Missions*, EUROPEAN DATA PROTECTION SUPERVISORS (Sept. 15, 2014) https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Membersmission.

[116] *See id.*

[117] *See id.*

[118] *See* Kuner, *supra* note 114, at 9.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

sort of "crystallization" of legal opinion.[119] The Article 29 W.P. congregates the Member state data protection authorities and seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.[120]

Moreover, at the European level, there are some other institutions which play the role of supervisory authority. For instance, the Data Protection Officer of the EU (DPO) is also a position set up by the Regulation No. 45/2001.[121] According to the Regulation, every EU institution must appoint a DPO to independently ensure the internal application of the Regulation in close cooperation with the EDPS.[122]

At the national level, a Data Protection Authority (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.[123] These authorities shall act with complete independence in exercising the functions entrusted to them. The DPA must be granted several tools with which to exercise its powers within member-state jurisdiction: Investigative powers, intervention powers, powers to engage in legal proceedings, powers of audit, and so on.[124]

II. Regulators Exercise LMLEP to Enhance the Efficacy of Incomplete Law

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

1. The Regulators at the European Level

In the multi-layered regulatory system, Article 29 W.P. is significant for exercising LMLEP.[125] The Article 29 working group was set up under Directive 95/46/EC.[126] It is

[119] *See id.*

[120] *See Article 29 Working Party*, EUROPEAN COMM'N (Aug. 6, 2014) http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[121] *See* Commission Regulation 45/2001, 2001 O.J. (L 8/1).

[122] *See Data Protection Officer of the EU*, EUROPEAN COMM'N (July 16, 2013), http://ec.europa.eu/justice/data-protection/bodies/officer/index_en.htm.

[123] *See* Council Directive 95/46/EC, art. 28, 1995 O.J. (L 281) (EC).

[124] *See id.*

[125] The Article 29 working group has a well-organized website: *Article 29 Working Party*, *supra* note 120.

[126] *See* Council Directive 95/46/EC, art. 29.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

composed of representatives of different national DPAs, representatives from the authorities established for the EU institutions and bodies, and a representative of the European Commission.[127] The Article 29 W.P. cooperates with the European Commission, but acts independently.[128]

The Article 29 W.P.'s responses are expressed in the form of advice and recommendations to the European institutions on specific data protection issues.[129] Its domain is identified by Directive 95/46/EC stating in which situations the Article 29 W.P. can issue its opinions, recommendations, and solutions, for instance by giving advice to any new proposal related to data-protection issues submitted by European Commission.[130] The Directive gives substantive discretion to the working group for issuing opinions on any matters or topics related to data protection.[131] In fact, the opinions, recommendations, and solutions reflect the views only of the Article 29 W.P. They do not reflect the position of the European Commission. In short, the materials created by Article 29 W.P. do not formally have legal effect.[132] Nevertheless, based on the Article 29 W.P.'s Rules of Procedure, any of its issued documents will be forwarded to EU Commission, to the European Parliament, and other related institutions. The documents adopted by the Article 29 W.P. have strong influence on European legislators and on Member State DPAs. Thus the Article 29 W.P. is de facto granted with residual LMLEP. Instead of amending rules, these powers allow the Article 29 W.P. to regularly adapt the understanding and application scope of rules in Directive 95/46/EC in response to technological changes they observe. The Article 29 thereby enhances law enforcement, both proactive and reactive. The Article 29 W.P. working group can consequently be seen as a unique institution within the European institutional landscape because at the European level, no similar institution has been established—or has established itself.[133]

---

[127] *See id.*

[128] *See id.* art. 30.

[129] As Pollute concluded, "Since 1996, more than 120 documents on different but important topics have been issued by the Art 29 W.P., which testifies tremendous and intense activities." Yves Poullet & Serge Gutwirth, *The Contribution of the Article 29 Working Party to the Construction of a Harmonized European Data Protection System: An Illustration of "Reflexive Governance"*? *in* CHALLENGES OF PRIVACY AND DATA PROTECTION LAW 570, 575 (Verónica Perez Asinari & Pablo Palazzi eds., 2008).

[130] *See* Council Directive 95/46/EC, art. 30, 1995 O.J. (L 281) (EC).

[131] *See id.* The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community. As Pollute and Gutwirth analyzed, this provision could be "underlined insofar that the Article 29. W.P. could not only advise, but also could intervene and de facto intervenes very freely and broadly about any topic related to data protection. Even the matters that are not covered by data protection directive may be included." Pollute & Gutwirth, *supra* note 129, at 576.

[132] *See* Kuner, *supra* note 114, at 7.

[133] *See* Poullet & Gutwirth, *supra* note 129.

The Article 29 W.P. has an efficient working mechanism. It develops a comprehensive set of rules for compliance toward different topics. Of course, these rules are strictly construed according to Directive 95/46/EC.

Take Article 25 as an example.[134] The Article contains general principles, which are highly ambiguous, open-ended provisions. The Article suffers from Type I incompleteness. In practice, it is difficult to predict whether and how involved actors will exercise the principles in Article 25. Therefore, further interpretation is required. Article 29 W.P. stepped in to interpret the provision in order to, as Incomplete Law Theory described, record legislators' intentions in a more precise manner.[135] Article 29 W.P. delivered the Working Paper 12 Working Document *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (WP12).[136]

The Article 29 W.P. has devised a comprehensive and well-articulated testing system for "evaluating and ensuring the requirement of 'adequate protection' in trans-border data flow,"[137] which is suggested by Pollute as the major contribution of the Article 29 W.P.[138] The standards imposed by Article 29 W.P. surpass Directive 95/46/EC, since they are based both on the content of the protection afforded by the third country's substantive or procedural system in a legal sense and upon the efficacy of these principles enacted.[139] From the perspective of Incomplete Law Theory, the Article 29 W.P. exercised its LMLEP order to mitigate the incompleteness of existing law. With the help of the Article 29 W.P., enforcers can easier decide how to deal with new cases. Since 1997, several such countries have been tested by the Working Party on the issues of data protection. These tests included New Zealand,[140] the Eastern Republic of Uruguay,[141] the Principality of Andorra,[142]

---

[134] *See* Council Directive 95/46/EC, art. 25, 1995 O.J. (L 281) (EC).

[135] Pistor & Xu, *supra* note 1, at 933.

[136] *See* Article 29 Data Protection Working Party, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (European Comm'n, Working Paper No. 12, DG XV D/5025/98, 1998).

[137] Poullet & Gutwirth, *supra* note 129, at 585.

[138] *See id.*

[139] *See id.*

[140] *See* Article 29 Data Protection Working Party*, Opinion 11/2011 on the Level of Protection of Personal Data in New Zealand* (European Comm'n, Working Paper No. 182, 2011).

[141] *See* Article 29 Data Protection Working Party, *Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay* (European Comm'n, Working Paper No. 177, 2009).

[142] *See* Article 29 Data Protection Working Party, *Opinion 7/2009 on the Level of Protection of Personal Data in the Principality of Andorra 2009* (European Comm'n, Working Paper No. 166, 2009).

Israel,[143] Faroer Islands,[144] Jersey,[145] the Isle of Man,[146] Guernsey,[147] Argentina,[148] Australia,[149] Canada,[150] Hungary,[151] and Switzerland.[152]

Regarding challenges brought by continuously changing technology, the Working Party has not hesitated to frequently intervene on topics directly related to issues linked to the growth of the technology.[153] The Article 29 W.P. exercises its residual LMLEP to adapt rule-interpretation in response to these technological changes. For example, both legislators and the Article 29 W.P. have observed the privacy risks brought by social networking.[154] However, legislators face higher procedural constraints and costs in changing the law and therefore cannot easily adjust, or extend the rules in response to observed changes.

[143] *See* Article 29 Data Protection Working Party, *Opinion 6/2009 on the Level of Protection of Personal Data in Israel* (European Comm'n, Working Paper No. 165, 2009).

[144] *See* Article 29 Data Protection Working Party, *Opinion 9/2007 on the Level of Protection of Personal Data in the Faroe Islands* (European Comm'n, Working Paper No. 142, 2007).

[145] *See* Article 29 Data Protection Working Party, *Opinion 8/2007 on the Level of Protection of Personal Data in Jersey* (European Comm'n, Working Paper No. 141, 2007).

[146] *See* Article 29 Data Protection Working Party, *Opinion 6/2003 on the Level of Protection of Personal Data in the Isle of Man* (European Comm'n, Working Paper No. 82, 2003).

[147] *See* Article 29 Data Protection Working Party, *Opinion 5/2003 on the Level of Protection of Personal Data in Guernsey* (European Comm'n, Working Paper No. 79, 2003).

[148] *See* Article 29 Data Protection Working Party, *Opinion 4/2002 on Adequate Level of Protection of Personal Data in Argentina* (European Comm'n, Working Paper No. 63, 2002).

[149] *See* Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000* (European Comm'n, Working Paper No. 40, 2000); *See* Article 29 Data Protection Working Party, *Opinion 1/2004 on the Level of Protection Ensured in Australia for the Transmission of Passenger Name Record Data from Airlines* (European Comm'n, Working Paper No. 85, 2004).

[150] *See* Article 29 Data Protection Working Party*, Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act* (European Comm'n, Working Paper No. 39, 2001); Article 29 Data Protection Working Party, *Opinion 1/2005 on the Level of Protection Ensured in Canada for the Transmission of Passenger Name Record and Advance Passenger Information from Airlines* (European Comm'n, Working Paper No. 103, 2005); Article 29 Data Protection Working Party, *Opinion 1/97 on Canadian Initiatives Relating to Standardization in the Field of Protection of Privacy* (European Comm'n, Working Paper No. 2, 1997).

[151] *See* Article 29 Data Protection Working Party, *Opinion 6/99 Concerning the Level of Personal Data Protection in Hungary* (European Comm'n, Working Paper No 24, 1999).

[152] *See* Article 29 Data Protection Working Party, *Opinion 5/99 on the Level of Protection of Personal Data in Switzerland* (European Comm'n, Working Paper No 22, 1999).

[153] *See* Poullet & Gutwirth, *supra* note 129, at 580.

[154] In 2009, the Article 29 W.P. published Opinion 5/2009 on Online Social Networking to clarify SNS issues. *See* Article 29 Working Party, *Opinion 5/2009 on Online Social Networking* (European Comm'n, Working Paper No. 163, 2009).

Conversely, the Working Party can exercise its LMLEP more flexibly. In 2009, the Article 29 W.P. delivered "Opinion 5/2009 on online social networking,"[155] to react to the social-network issues at stake. The opinion 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,[156] the national regulators can adapt these rules and shape them to their special needs.[157]

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 . . . . [They may do this] independent of whether violations have occurred, or when others have brought problems to their attention."[158]

Based on the above analysis, I conclude that the Article 29 W.P. adopts an active enforcement policy.

The findings also confirmed Poullet's statement that the agency "has an unique role to play in the process of ensuring the *acquis* of Directive 95/46/EC."[159] And the agency develops into an active regulator "when it comes to progressively adapt the legislation framework and its effective application to the real needs of society in a changing context which still creates new privacy threats."[160] The Working Party's operations do not render Directive 95/46/EC more onerous, but improve its clarity. In the light of this performance, Article 29 W.P. has adapted the 'dying' principles in Directive 95/46/EC to get alive again.

2. National Data Protection Authority

The problem of under-enforcement is partly mitigated by national data protection authorities too. According to Article 28 of the Data Protection Directive, the national DPA is endowed with the powers to investigate, to intervene, to hear claims, and to engage in legal proceedings, and so on.[161]

---

[155] *See id*.

[156] *See* Irish Data Protection Commission, *Facebook Ireland Ltd. Report Audit*, 2011 O.J. (EC).

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

[158] Pistor & Xu, *supra* note 1, at 950 to 954.

[159] Poullet & Gutwirth, *supra* note 129, at 572.

[160] *Id.*

[161] *See* Council Directive 95/46/EC, 1995 O.J. (L 281) (EC).

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

It is not difficult to find cases in which national DPA exercises its LEP. For instance, in Germany:

> On November 23, 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 neuromarketing 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 neuromarketing techniques under data protection laws beyond Germany.[162]

Through the enforcement of 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. These powers allow the national regulators to regularly adapt rules in incomplete Directive 95/46/EC 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.

[162] Stefan Schuppert, German *Data Protection Authority Imposes 200000 Euros Fine for Targeted Advertising Without Adequate Consent,* HOGAN LOVELLS (Dec. 7, 2010). http://www.hldataprotection.com/2010/12/articles/international-compliance-inclu/german-data-protection-authority-imposes-a200000-fine-for-targeted-advertising-without-adequate-consent/index.html.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

> 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.[163]

The lawmaking activities of national regulators can enhance overall protection for citizens and increase the visibility of national authorities in society. Therefore, the substantial residual LMLEP are taken up by the national DPAs, as the Incomplete Law Theory expected: "[I]n response to the problem of existing law's under-deterrence."[164]

III. Summary

This 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 to regulators in financial, environmental, and other areas, data regulators work differently than legislators and courts. Data regulators react to technical development much more quickly than legislators, who are constrained by procedures. Data regulators also exercise their residual LMLEP proactively rather than courts who can only apply their residual LMLEP 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 was 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 a reallocation of some lawmaking powers to regulators.[165]

---

[163] Stefan Schuppert, *German DPAs Issue Rules for Cloud Computing Use*, HOGAN LOVELLS (Oct. 13, 2011), http://www.hldataprotection.com/2011/10/articles/international-eu-privacy/german-dpas-issue-rules-for-cloud-computing-use/.

[164] Pistor & Xu, *supra* note 1, at 996.

[165] *See id.* at 968.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

E. Limitations of this Study

In this paper I have analyzed the problems that confront data protection laws, using the European legal system over data protection issues as example. The analysis used the established framework of incomplete law theory because in data protection law the frequency of technical innovations has a serious effect on its completeness.

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 and address the legal problems in the 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."[166] Nevertheless, the framework has never been applied beyond corporate-law and financial-market regulations. Moreover, the uncertainties of our results increase because this theory is basically derived from the study of the legal economy. Incomplete law theory is exploratory in itself. The theory is equally incomplete as incomplete laws are.

First, 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."[167] The two authors recognize that these issues are of great importance, but they do not analyze them and their relations to incomplete law theory.

Second, Xu and Pistor's study used samples of UK, US, and German experiences of financial market development.[168] However, this selection led to a generalization problem, which may be limited by contextual differences in policy, governance, culture, and history, as well as other potential differences in regime, which were not selected in this study.[169] 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.[170] Moreover, incomplete law theory cannot explain the divergent experiences of Russia and China in developing

[166] The two authors illustrate that environmental, safety, food, and drug regulation are fitting fields to adopt this analytical framework. *See id.* at 936.

[167] *Id.* at 935.

[168] *See id.* at 966–1011.

[169] *See id.*

[170] *See id.*

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

financial markets.[171] These findings show that incomplete law theory is not always relevant—or complete.

In fact, further work is needed to validate the applicability and relevance of the theory and the implications it carries for different legal regimes. Here, I will leave these questions open. Methodologically, I argue that the theory provides a conceptual analysis model for my research where it concerns EU data protection regulation. It produces a useful model for the design of effective enforcement. It also offers a fresh perspective to peer into the European legal system regarding data protection issues. My analysis suggests that the theory is both appropriate and useful as a framework for guiding our analysis.

F. Conclusion: Regulatory Agencies are Necessary to Enhance Law Enforcement

This paper analyzes the Incomplete Law Theory created by Xu and Pistor. The theory includes three propositions: (1) Law is intrinsically incomplete because 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, who are vested with proactive law enforcement and residual lawmaking powers, are the optimal solution in an incomplete legal world in order to achieve optimal deterrence effects, given specific conditions.[172] Xu and Pistor focus on the functions performed by regulators. Regulators can better respond to the problem of ineffective enforcement caused by incomplete law because they perform their functions ex post and reactively.[173] As the two authors conclude, "While the scope of their lawmaking rights is limited, they are more flexible in adapting law over time than legislatures are. 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."[174]

In this paper, I applied the theory to the European legal system with respect to data protection issues. The analysis shows that, even in Europe where a jurisdiction with a well-recognized legal system over data protection issues, (1) lawmakers cannot formulate all relevant issues in data protection laws and (2) courts face severe problems in ensuring effective enforcement of data protection. But the problems of incompleteness and under-deterrence are largely mitigated by a unique European creation: Data protection regulators. They assume residual LMLEP. Article 29 W.P. and national data authorities—DPAs—play significant roles in keeping the regulation in step with technological innovation. Normally,

[171] *See id.*

[172] *See id.*

[173] *See id.* at 1012.

[174] *Id.*

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press

the emergence of data regulators in Europe is regarded as a requirement for harmonization. But my analysis suggests that this kind of argument cannot fully explain the functions that the regulators have taken on.

My finding is that data regulators are vested with substantial LMLEP. As agents granted with limited LMLEP regulators are more flexible in adapting law over time than legislatures are. Many challenges brought by technical developments do not require the legislator to modify laws because regulators preemptively try to 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 while 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 regulators catch them preemptively. Regulators enforce laws to recover or prevent injuries caused by harmful actions.

Therefore, the substantial residual LMLEP has to be taken up by the multi-layered regulators in response to the problem of the laws under-deterrence and the resulting danger of widespread violations of data subject's right to personal data. The story in Europe offers important insights into the benefits of a system that not only offers reactive but also proactive enforcement.

Based on the findings in this paper, it is urgently suggested that introducing a regulator may improve law enforcement of incomplete law. No attempt, however, will be made to propose any well-organized road map for legal arrangements to that effect because it is too complicated and big a question for a single person to address. But, the fundamental principle is this: In the data protection field, not only is a legal system addressing data protection issues required to deter violations, but a data regulatory institution is also necessary.

https://doi.org/10.1017/S2071832200019271 Published online by Cambridge University Press