The 'Internal Morality' of European Data Protection Law

Christopher Kuner*

One of the seminal documents of legal philosophy in the 20th century was the February 1958 issue of the *Harvard Law Review*, which featured a debate between Oxford professor H.L.A. Hart and Harvard professor Lon Fuller on the merits of legal positivism (championed by Hart) versus those of natural law theory (championed by Fuller),[1] and also resulted in classic books on jurisprudence being written by each.[2] The ideas of these two scholars raise fundamental issues about the nature of law, the characteristics of a successful and efficient legal order, and the role of enforcement in ensuring that the law functions correctly. These are precisely the types of questions that need to be raised about European data protection law, which even European government ministries and data protection authorities (DPAs) have described as 'far too comprehensive and complicated'[3] and 'increasingly out-dated,…not

* Partner, Hunton & Williams LLP, Brussels, Belgium, e-mail: ckuner@hunton.com. Chairman, Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce (ICC), and member of the Data Protection Expert Group (GEX PD) of the European Commission. This article is written in the author's personal capacity, and does not necessarily reflect the views of any organization.

[1] H.L.A. Hart, 'Positivism and the Separation of Law and Morals', 71 *Harvard Law Review* 593 (1958) and Lon L. Fuller, 'Positivism and Fidelity to Law — A Reply to Professor Hart', 71 *Harvard Law Review* 630 (1958).

[2] H.L.A. Hart, *The Concept of Law* (Oxford University Press 2nd edition 1997) (hereinafter cited as 'Hart, *The Concept of Law*') and Lon L. Fuller, *The Morality of Law* (Yale University Press 2nd edition 1969) (hereinafter cited as 'Fuller, *The Morality of Law*'). This characterization of the views of both men is somewhat superficial; for example, Hart criticized some of the positions taken by other positivist scholars.

[3] Swedish Ministry of Justice, 'Simplified protection for personal data applying misuse model' (unpublished memorandum), 30 November 2000. On 13 September 2002, the Austrian, Finnish, Swedish and UK governments published a paper suggesting wide-ranging amendments to the EU Data Protection Directive in line with the earlier Swedish proposal.

sufficiently clear in its objectives,…more bureaucratic and burdensome than it needs to be and…out of step with good regulatory practice'.[4]

In recent years, data protection law has moved from being a niche area to a topic of fundamental importance for both governments and the private sector.[5] Nevertheless, despite the social, economic, and legal significance of European data protection law, there is has been relatively little discussion of its overall coherence and effectiveness (which Fuller describes as the 'internal morality' of a system of rules) in a jurisprudential sense.

Data protection law has attained a level of importance which makes it worthy of being treated with the respect accorded to other areas of the law, which includes evaluating it in light of jurisprudential criteria. Such an evaluation is useful in a time of transition for data protection law to indicate both its strengths and weaknesses, and to suggest issues that require further thought by policymakers.

I. The Sources and Enforcement of European Data Protection Rules

Data protection law is largely a European creation, and derives largely from a ground-breaking judgment rendered in 1983[6] by the German Federal Constitutional Court which recognised a fundamental human right to 'informational self-determination'. Since then data protection has been incorporated into the law of all twenty-seven Member States of the European Union (the EU), as well as some non-EU European countries (such as Iceland,

[4] UK Information Commissioner, Invitation to Tender — Review of EU Data Protection Law, 14 April 2008, available at http://www.ico.gov.uk/upload/documents/invitation_to_bid_14_04_08/invitation_to_tender_final.pdf.

[5] For a detailed discussion of the practical significance of European data protection law in the business context, see Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press 2nd edition 2007).

[6] Bundesverfassungsgericht, Judgment of 15 December 1983, 65 BVerfGE 1.

Liechtenstein, and Norway), and has strongly influenced data protection laws in jurisdictions such as Argentina, Canada, the Dubai International Financial Centre (DIFC), Hong Kong, and Russia as well.

European data protection law is comprised of many different sources, which include, for example, the following: directives (most prominently the EU Data Protection Directive 95/46/EC (the 'EU Data Protection Directive'), and the E-Privacy Directive 2002/58/EC (the 'E-Privacy Directive')); national data protection law; papers and opinions published by the Member State data protection authorities (DPAs) and the Article 29 Working Party (a committee of the DPAs of all EU Member States); standards adopted by technical standards bodies and industry associations; articles and commentaries written by leading scholars; and other sources.

If one examines the sources of European data protection rules, one can discern several important distinguishing factors between them. One is the degree of legal compulsion that each one entails. For instance, European directives obviously have binding legal force, as do national data protection laws (even if their binding nature differs, with directives primarily binding on EU Member States, and national laws also binding on legal and natural persons). Standards promulgated by standardisation bodies may be binding in certain contexts (for example, if they are referenced in a directive or law, or in the context of membership in a particular group or association), while academic writings may be highly persuasive and be relied upon in certain cases by courts and regulators though they have no legally-binding force per se. Another difference relates to the manner in which these sources are drafted or enacted, with directives and laws being adopted based on the lawmaking process, DPA opinions drafted by the staff of the data protection authorities, standards adopted by the appropriate bodies, etc.

The diverse nature of the sources of European data protection rules raises questions as to which of them should be considered to be 'law'. In this context, Fuller's definition of 'law' as 'the enterprise of subjecting human conduct to the governance of rules'[7] seems as good as any. Lawrence Lessig famously proclaimed that 'code is law', i.e., that 'the software and hardware that make cyberspace what it is *regulate* cyberspace as it is'.[8] Other scholars have rejected this position, stating that it would result in citizens 'surrendering our political rights to market forces'.[9] It is not necessary to enter into this debate here, beyond noting that there seems to be little relation between the legal force of the particular types of data protection rules and their practical importance. Thus, certain academic commentaries, which have no binding force, may carry significant weight in a particular jurisdiction.[10] Likewise, the opinions of data protection authorities or the Article 29 Working Party may have no formal binding character, but may be cited by courts as precedent to which deference should be given.[11]

While industry standards usually carry no binding legal force, some may carry such important practical penalties for non-compliance that they become a kind of de facto standard. Many

---

[7] Fuller, *The Morality of Law* p. 74.

[8] Lawrence Lessig, *Code and other laws of cyberspace* (Basic Books 1999), p. 6.

[9] Marc Rotenberg, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)', 2001 *Stanford Technology Law Review* 1, http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf.

[10] An example is the commentary on the German Federal Data Protection Act edited by Prof. Spiros Simitis, which is highly influential in the German legal community and is often cited in German court decisions. Spiros Simits (ed.), *Bundesdatenschutzgesetz* (6. Auflage Nomos 2006).

[11] See *Campbell v Mirror Group Newspapers* [2002] EWHC 499, in which the English Court of Appeal interpreted the UK Data Protection Act 1998 in reference to an opinion of the Article 29 Working Party, stating 'to give a proper interpretation to the domestic Act I must look to the directive and the ancillary Recommendation of the working party'. This decision was later overruled by the House of Lords, [2004] UKHL 22, but without making any reference to the Article 29 Working Party.

such standards relate to data security, which is a prime element of data protection law.[12] An example is provided by the Payment Card Industry Data Security Standard (PCI DSS), which was adopted by a consortium of the payment card industry in 2006. Since failure to comply with the PCI DSS can ultimately result in a business being unable to process credit card payments, violation of the standard can be a 'death sentence' for a company and thus result in a higher level of effective compulsion than many statutory rules do.

On the other hand, provisions of EU directives and the national laws which implement them may be legally binding, but may not be complied with consistently in practice. An example is Article 4(2) of the EU Data Protection Directive, which provides that, in cases in which EU law applies under Article 4(1)(c), the data controller established outside the EU must designate 'a representative established in the territory of that Member State…'. It seems that such appointment is virtually never done, nor is compliance with this provision regularly enforced by the DPAs.

The diversity of sources of data protection rules, and the lack of a relationship between their formal legal force and their effectiveness, indicates that both data controllers seeking to comply with the law, and data subjects seeking to determine their legal rights, are faced with the difficult task of sifting through a vast repository of sources, and of determining which ones are really relevant to them. Studies by the European Commission have demonstrated a considerable degree of confusion among both data controllers and data subjects as to their data protection rights and responsibilities,[13] and the difficulty in determining their legal obligations may be one reason for this confusion.

---

[12] See EU Data Protection Directive, Art. 17, which requires that adequate security measures be used in processing personal data.

[13] See the Eurobarometer surveys referred to below in Part II of this article.

Another important issue concerns the status of compliance with European data protection law and how compliance is enforced. Hart believed that large-scale non-compliance, and a general lack of enforcement, could throw into question the status of a system of rules as 'law',[14] which view was also shared by Hans Kelsen.[15] In fact, the compliance status of European data protection rules, and the relative lack of enforcement of them, have been a major source of concern among policymakers. As the European Commission stated in 2003 in its 'First report on the implementation of the Data Protection Directive (95/46/EC)':[16]

> 'Anecdotal evidence, however, combined with various elements of 'hard' information available to the Commission suggests the presence of three inter-related phenomena:
>
> – An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority;
> – Very patchy compliance by data controllers, no doubt reluctant to undertake changes in their existing practices to comply with what may seem complex and burdensome rules, when the risks of getting caught seem low;
> – An apparently low level of knowledge of their rights among data subjects, which may be at the root of the previous phenomenon'.[17]

There is no doubt that the amount of enforcement of European data protection rules is quite small in proportion to the amount of personal data that are now being processed. For example, the Spanish Data Protection Authority has stated that up to 2007 it had received notification from data controllers of 8,463 international data transfers.[18] However, all the telephone calls,

---

[14] See Hart, *The Concept of Law,* p. 116, stating that one of the minimum conditions necessary for the existence of a legal system is that 'those rules of behaviour which are valid according to the system's ultimate criteria of validity must be generally obeyed…'

[15] See Hans Kelsen, *General Theory of Law and State* (Transaction Publishers 2005), p. 42, stating: 'A norm is considered to be valid only on the condition that it belongs to a system of norms, to an order which, on the whole, is efficacious'.

[16] Commission document COM(2003) 265 final.

[17] Ibid.

[18] Agencia Española de Protección de Datos, Informe sobre transferencias internacionales de datos, Julio 2007, p. 5, available at

e-mails, faxes, Internet browsing activities etc. carried out between Spain and countries outside the EU in a year, which can all be considered 'international data transfers' in the sense of data protection law and may therefore be subject to a duty of notification, must number in the millions or even billions. Even if one concedes that not all of these communications would need to be notified to the Spanish DPA under the law, one can still see that the number of notifications made to the Agency is an infinitesimally small percentage of the actual number of international data transfers from Spain. Thus, there is obviously massive non-compliance with rules on international data transfers from Spain; one can only assume that such non-compliance must extend to other areas of European data protection law as well.

The are many likely reasons for such widespread non-compliance, the most basic of which relate to two fundamental changes in the way data are processed. In particular, data processing is now both *networked* and *globalized*, phenomena which have taken hold since use of the Internet and electronic commerce became widespread in the late 1990s. Networked data processing means that to an increasing extent, data are processed on computer networks, so that the processing is frequently distributed among a large number of computers, many of which may be in different countries and regions. The distributed nature of data processing greatly complicates the ability of data controllers to determine what their compliance obligations are, since it multiplies the number of rules that may be applicable to processing operations, and also makes it more difficult for DPAs to enforce the law, since the number of entities processing personal data is much greater. The growth of the Internet has similarly resulted in data processing becoming increasingly international, with data often being accessed or processed across national borders. The growth of globalized data processing

---

https://www.agpd.es/portalweb/jornadas/transferencias_internacionales_datos/common/pdfs/INFORME_TIs.pdf.

similarly complicates both compliance and enforcement, since it makes it more difficult for data controllers to determine which law applies to their processing activities, and means that much data processing takes place outside the enforcement jurisdiction of the DPAs.

The response of data protection authorities to these phenomena has been to ratchet up the enforcement of data protection rules, which seems to have increased in recent years. Indeed, DPAs, courts, and other regulatory authorities have levied severe penalties for violations of data protection law.[19] In particular, the DPAs seem to have decided that, because of their lack of resources for enforcement, the most efficient way of policing data protection compliance is to conduct random enforcement actions in particular sectors. For example, in 2007 the Article 29 Working Party published a report on its first joint enforcement action, which included a joint investigation of data controllers in the private health insurance sector carried out by DPAs in a number of Member States,[20] and has since announced that the second joint investigation will cover telecommunications and Internet service providers.[21] Such random audits and enforcement action may be the only efficient response of overstretched enforcement authorities, and can be quite effective, since publicized action taken against a representative data controller often tends to motivate other ones to increase their compliance

[19] For example, in the following cases: (1) on 18 December 2007, the Dutch independent authority regulating postal and electronic communications services imposed a fine totaling €1,000,000 on three Dutch companies for surreptitiously installing spy- and adware on over 22 million computers belonging to Internet users in the Netherlands and elsewhere; (2) on 17 April 2007, the Spanish Supreme Court affirmed the €1,081,822 fine imposed in January 2001 by the Spanish Data Protection Authority on Zeppelin Television S.A., which produces the Spanish version of the 'Big Brother' television reality show for data protection violations; and (3) on 17 December 2007, the UK Financial Services Authority (FSA) fined Norwich Union Life £1.26 million for neglecting to put in place effective systems and controls to protect customers' confidential information.

[20] Article 29 Working Party, 'Report 1/2007 on the first joint enforcement action: evaluation and future steps' (WP 137, 20 June 2007).

[21] See Article 29 Working Party, 'Mandate to the Enforcement Subgroup to proceed to the 2nd join investigation action' (WP 152, 17 July 2008), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp152_en.pdf.

level. However, such random action must be carefully calibrated and considered so as to be applied consistently and fairly, and so as not to make some data controllers feel that they are being unfairly singled out for enforcement.

Despite the growing number of enforcement actions, the chance of an action being brought for a particular data protection violation is still relatively low in most cases. The lack of widespread and consistent enforcement of data protection violations has a negative affect on the willingness of data controllers to comply with European data protection rules. There is a gap between the complexity of the rules that govern data processing, and the relatively low risk of enforcement action being taken. The result is that data controllers often give more importance to areas of the law where the enforcement penalties are more draconian (such as tax, money laundering, securities law etc.) than they do to data protection law. In the globalized economy, all factors affecting cost (including legal compliance burdens) tend to be subject to a risk management exercise, with compliance being more likely when the risks and costs of non-compliance are higher than those of compliance. Thus, in many cases data controllers may regard data protection rules as a kind of bureaucratic nuisance rather than as 'law' in the same category as tax and other laws, mainly because of the relative lack of enforcement and the relative mildness of the possible penalties.

Besides 'legal' enforcement methods such as fines, injunctions, criminal penalties etc., 'soft' penalties such as adverse publicity are an important incentive to comply with data protection law, since damage to a company's reputation can ultimately cause it more harm in the marketplace than can a fine. In addition, customers increasingly expect a good level of data protection compliance from their suppliers, and such pressure can also be more effective at motivating a data controller to comply with the law than can traditional, legal enforcement methods.

II. Towards a Coherent and Effective Data Protection Regime

Fuller's concept of the 'internal morality' of law is based on eight key mistakes or 'failures' that a legal system can make, which he describes as follows:

> The first and most obvious lies in a failure to achieve rules at all, so that every issue must be decided on an ad hoc basis. The other routes are: (2) a failure to publicize, or at least to make available to the affected party, the rules he is expected to observe; (3) the abuse of retroactive legislation, which not only cannot itself guide action, but undercuts the integrity of rules prospective in effect, since it puts them under the threat of retrospective change; (4) a failure to make rules understandable; (5) the enactment of contradictory rules or (6) rules that require conduct beyond the powers of the affected party; (7) introducing such frequent changes in the rules that the subject cannot orient his action by them; and, finally, (8) a failure of congruence between the rules as announced and their actual administration.[22]

Fuller's 'internal morality' has nothing to do with religion, but rather with logic and internal coherence; he describes it as 'like the natural laws of carpentry, or at least those laws respected by a carpenter who wants the house he builds to remain standing and serve the purpose of those who live in it'.[23]

It would be wrong to ignore the achievements of European data protection law, such as the removal of barriers to data flows between the EU Member States,[24] and the adoption of a minimum level of data protection in all Member States.[25] However, there is no denying that it does exhibit a number of the faults contained in the above list, such as the following:

– *Lack of rules to cover common situations*: EU data protection law fails to provide rules for some data processing situations that occur often in practice. For example, Articles 25 and 26 of the EU Data Protection Directive fail to provide rules for several data transfer

[22] Fuller, *The Morality of Law*, p. 39.

[23] Fuller, *The Morality of Law*, p. 96.

[24] See EU Data Protection Directive, Art. 1(2).

[25] See EU Data Protection Directive, Art. 1(1).

scenarios that have become very common. Data may often be transferred from a data controller in the EU to a data processor outside the EU, but then also transferred by the data processor to a further data processor. This scenario can arise, for example, when the EU data controller transfers personal data to a data processor outside the EU, which then engages another data processor in another country to perform routine IT maintenance on its databases. Since the initial outsourcing to the data processing company is considered to be an international data transfer, and the access of the outsourcing company's servers by the IT maintenance company is considered to be an 'onward transfer' of the data, the situation constitutes an initial international data transfer to a data processor, followed by an onward transfer from one data processor to another. However, the law of most EU member states does not seem to contemplate a transfer of data from one data processor to another data processor, which results in data processing being in a legal limbo and the parties involved in the data transfer not knowing what they must do to comply with the law.[26]

These sorts of issues concerning international data transfers will likely increase as the outsourcing of data processing across a large number of external service providers without regard to geographical boundaries also increases.[27] Indeed, data processing has become so complex in recent years that it is becoming impossible for the law to provide

[26] This vacuum has caused business groups to propose to the European Commission a new set of EU standard contractual clauses for data transfers from controllers to processors in order to clarify the responsibilities of the parties involved. See Press Release, 'ICC submits 'model clauses' to EC for international data transfers', 20 October 2006, http://www.iccwbo.org/iccjbjb/index.html, stating 'The new draft highlights a number of issues that urgently need to be addressed but are lacking in the EC's original set of clauses, such as provisions dealing with a data transfer from one data processor to another data processor'.

[27] Regarding the explosive rise in the outsourcing of data processing across national borders, see 'Let it rise: A special report on corporate IT', The Economist, 25 October 2008.

rules for all the new processing situations that are developing, so that data controllers, data processors, and data subjects are frequently placed in the position of having to determine their rights and obligations for situations that are not contemplated under the law.

– *Failure to adequately publicize the relevant rules*: As studies published in 2004 by the European Commission have demonstrated, there is a low level of awareness of data protection law among both European data controllers[28] and citizens.[29] This lack of awareness seems to be due in large part to the failure of EU Member States to give proper importance to data protection and publicize it among citizens, manifestations of which include their failure in many cases to provide the proper independence for data protection authorities[30] and the proper financial resources for their operation.[31] As an example, there seems to be widespread confusion among data controllers about issues such as Member State legal requirements for use of the EU-approved standard contractual clauses for data

[28] Flash Eurobarometer, Executive Summary, http://ec.europa.eu/public_opinion/flash/fl147_exec_summ.pdf, stating 'Results of the EU average show that for the relative majority of persons responsible for data protection issues (39%), the lack of knowledge of the data protection law best explains why certain data controllers do not fully respect this legislation.'

[29] Eurobarometer Survey, December 2003, Executive Summary, p. 10, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_exec_summ.pdf, stating 'The level of knowledge about the existence of independent authorities monitoring the application of data protection laws, hearing complaints from individuals and imposing sanctions on law breakers was low across the European Union and two-thirds (68%) of EU citizens were not aware of their existence'.

[30] For example, in November 2007, the European Commission sued the government of Germany before the European Court of Justice because of a lack of independence of German federal state DPAs. Action brought on 22 November 2007 -- Commission of the European Communities v Federal Republic of Germany, Case C-518/07 [2008] OJ C37/8.

[31] One commentator has noted that 'funding for enforcement of the European Union's complex and stringent data protection law varies widely within the 27 EU Member States …' Laura Speer, 'Variable Funding of EU Privacy Law Means Uneven Enforcement Across European Union' (January 2007) *World Data Protection Report* 24.

transfers, and Member State formalities for approval of binding corporate rules. A few simple measures could go a long way toward increasing awareness, such as if the Article 29 Working Party would publish more charts and tables indicating Member State data protection requirements and formalities.[32]

– *Unclear rules*: There are certain characteristics of data protection law which seem to produce a particularly high level of confusion and complexity:

i. Lack of court decisions, and over-reliance on non-binding sources of law: There is a conspicuous lack of legally-binding decisions by courts and other regulatory authorities in the area of data protection,[33] and an over-reliance on non-binding sources such as informal opinions of data protection authorities and writings by academic commentators. While the latter types of sources can certainly be valuable, they lack the legal authority of binding sources, and may diverge from each other, which can lead to confusion.

ii. Reliance on general principles of law that are not explicitly included in applicable legislation: Data protection law relies heavily on general legal principles that are often not explicitly referred to in the applicable legislation, and may not be fully visible. An example is the principle of proportionality, which is referred to only a few times in the text of the EU Data Protection Directive,[34] and which may thereby give the misleading

[32] An example of such a useful compendium of Member State legal requirements is the 'Vademecum on notification requirements' published by the Article 29 Working Party on 3 July 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-vademecum.doc.

[33] See L Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law' (2000) 7 *Privacy Law & Policy Reporter* p. 11.

[34] For example, Article 11(2) states that information about data processing need not be given in the context of data processing for statistical purposes or for the purposes of historical or scientific research when the provision of such information 'proves impossible or would involve a disproportionate effect'; and Article 12(c) limits the duty to notify third parties to

impression that it is of little importance. In fact, the European Court of Human Rights routinely uses proportionality as a criterion for determining whether data processing is legal,[35] and the European Court of Justice has also applied the proportionality principle in relation to data protection.[36] However, since the proportionality principle is not explicitly mentioned in most data protection statutes, and many data controllers are used to thinking of data protection compliance in terms of satisfying a well-defined set of statutory requirements, they may find themselves at a loss in interpreting the principle.

– *Contradictory rules*: There is sometimes disagreement between courts and data protection agencies about some of the most fundamental concepts of European data protection law, even within the same country. As an example, in two decisions, the Paris Court of Appeal ruled in 2007 that the IP address used by an internet user does not constitute personal data, because it does not allow the user's direct or indirect identification.[37] However, the French Data Protection Authority (CNIL) has expressed disagreement with the two decisions, and they are currently being appealed. A similar situation has occurred in Germany, with one court deciding in 2007 that IP addresses constitute 'personal data',[38] and another finding in 2008 that they do not.[39] It is difficult for a party to determine its

---

whom data have been disclosed of any rectification, erasure, or blocking of the data when such notification "proves impossible or involves a disproportionate effort."

[35] See, e.g., *Leander v. Sweden*, Judgment of 26 March 1987, Series A, no 116, ECHR, finding that there was no breach of the proportionality principle and the European Convention on Human Rights when the Swedish government refused employment to the petitioner based on his being listed in a secret police register.

[36] See, e.g., *Productores de Música de España (Promusicae) v Telefónica de España* SAU (C-275/06) [2007] E.C.D.R. CN1; C-138/01 *Rechnungshof* [2003] ECR I-6041.

[37] Cour d'appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007, and Cour d'appel de Paris 13ème chambre, section A Arrêt du 15 mai 2007.

[38] Amtsgericht Berlin Mitte, Urteil vom 27.3.2007, Az. 5 C 314/06.

[39] Amtsgericht München, Urteil vom 30. 9. 2008, Az. 133 C 5677/08.

legal rights and obligations when it is faced with a disagreement between courts and regulatory authorities of its country about the definition of one of the most basic concepts of the law.

– *Failure of congruence between the rules and their administration*: This principle refers to a gap between the rules and how they are actually applied in practice. As pointed out above, there is a lack of compliance with and enforcement of data protection rules, which indicates that there is a gap between the legal rules and how they are applied. In addition, there are important exemptions from the scope of EU data protection law, in particular regarding data processing relating to national defence, security, and criminal law;[40] while there may be valid legal reasons for such a distinction, from the point of view of the ordinary citizen it is difficult to understand why data protection rules should not apply to the law enforcement processing of data, since such processing may present at least as great a risk to data protection as processing in the private sector may. These exemptions from the scope of the law may also undermine respect for EU data protection law among citizens and data controllers.

III. Conclusions

This article may seem to paint a gloomy picture of the state of European data protection law, but it is important to keep the law's strengths in mind as well. Besides have been enacted throughout the European Union, the EU Data Protection Directive has proven to be ahead of its time in laying out a broad policy architecture for the processing of personal data, and has

[40] See EU Data Protection Directive Art 3(2). As this article was being finalised, the EU institutions were engaged in a debate about the approval of a data protection instrument to govern 'third pillar' activities such as police and law enforcement.

also had significant influence on laws in other regions.[41] Thus, the law has had a number of successes.

However, problems with the law remain, and can be divided into three main categories:

Substantive problems. The substance of EU data protection rules should be reexamined in several areas. An example is the requirement in Article 25(1) of the EU Data Protection Directive that personal data may only be transferred to third countries that provide an 'adequate level of protection'.[42] While the goal of ensuring that personal data are not deprived of all protection when they are transferred outside the EU is appropriate and understandable, it is questionable whether restricting the transfer to third countries that have been declared to provide 'adequate' protection is the most efficient or workable mechanism for attaining this goal. Indeed, in the ten years since the Directive came into force only a handful of adequacy determinations have been rendered by the European Commission,[43] none of which cover any of the dynamic countries in the developing world to which data are increasingly being transferred (such as China and India). Thus, the rules on the issuance of adequacy determinations are clearly not working, and need to be reexamined.

Problems relating to EU politics. Many of the problems of EU data protection law are caused by political factors. An example of this is the unwillingness of DPAs and Member States to

[41] Jurisdictions whose data protection laws show the influence of EU law include Argentina, Canada, the Dubai International Financial Centre (DIFC), and Hong Kong.

[42] A formal finding of adequacy is carried out by the Member States and the European Commission following the procedure set out in Article 30(1) of the EU Data Protection Directive, with the advice of the Article 29 Working Party.

[43] At the time this article was finalized, such adequacy decisions covered Argentina; Canadian organizations subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act); the Bailiwick of Guernsey; the Bailiwick of Jersey; the Isle of Man; Switzerland; the US safe harbor system; and transfers of airline passenger data to the US Department of Homeland Security (DHS).

harmonize national requirements in areas such as notification requirements, formalities relating registration of the EU standard contractual clauses with the DPAs, and approval of binding corporate rules. While the EU Data Protection Directive is not intended to produce complete harmonization and leaves a certain amount of leeway in implementation to the Member States, it is intended to produce a high level of harmonization,[44] and in implementing it the Member States are supposed to pay due regard to the wording and purpose of the relevant provision of the Directive.[45] However, Member States still seem largely reluctant to harmonize national data protection requirements, based in many cases on an unwillingness to abandon long-held national views of data protection issues. DPAs may even take largely national views on implementation of decisions issued by the European Commission concerning international data transfers (such as the Safe Harbor adequacy decision and the decisions concerning the standard contractual clauses) and have imposed additional national requirements on their use.[46]

It is also striking that Member State governments seem to have largely absolved themselves of any responsibility for the creation of a more efficient and workable data protection

[44] See Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, para 96, stating regarding the Directive that 'the harmonisation of those national laws is therefore not limited to minimal harmonisation but amounts to harmonisation which is generally complete'.

[45] See Joined Cases C-465/00 and C-138/01 *Rechnungshof* [2003] ECR I-6041, stating regarding the Directive that 'that the national court must also interpret any provision of national law, as far as possible, in the light of the wording and the purpose of the applicable directive, in order to achieve the result pursued by the latter and thereby comply with the third paragraph of Article 249 EC'.

[46] For example, in a paper adopted by the *Arbeitsgruppe 'Internationaler Datenverkehr'* of the group of German data protection authorities (a subgroup on international data transfers of the conference of German federal and state data protection authorities or *Düsseldorfer Kreis*) on 12-13 February 2007, it is stated that the alternative standard contractual clauses of 2004 are not suitable for the transfer of employee data and may need to be expanded by additional clauses, since the liability and informational obligations are 'limited'. Abgestimmte Positionen der Aufsichtsbehörden in der AG 'Internationaler Datenverkehr' am 12./13. Februar 2007, p. 2.

framework. For example, Member State governments have generally not participated in workshops on international data transfers held in Brussels by the European Commission, submitted comments to the Article 29 Working Party on open consultations that group has held, or been willing to hold an open dialogue with citizens and data controllers on important data protection issues. This indicates that many governments may not understand the benefits that global data flows hold for their economies.

Progress in areas such as greater harmonization of data protection law within Europe will only be possible if Member States make a political commitment to resolve current difficulties. The European Commission should also make greater use of its powers to move the Member States in the direction of greater harmonization of data protection law; even if there are legal limits to the extent to which the Commission can require harmonization, its powers of moral suasion to 'name and shame' Member States can be quite affective in this regard.

Lack of awareness. Despite efforts in recent years by the DPAs and the European Commission to increase awareness of data protection law, there is still widespread lack of awareness of the law and its requirements by both citizens and data controllers. Many data controllers do not understand what their compliance obligations are, data protection authorities are confused about how data are currently being processed by business, and citizens do not fully understand their rights and obligations.

The level of awareness would be enhanced if there was greater transparency in data protection policymaking. This means that, for example, initiatives of the Article 29 Working Party and the European Commission should be subject to public comment before being adopted; regular hearings should be held in Brussels and national capitals on major data protection legislative initiatives; and Member State governments should become more involved in data protection policymaking. In this respect, one can agree with Fuller's

criticism that law should not be regarded as a 'one-way projection of authority' by governments, but as a collaborative enterprise in which the acceptance and participation of the legal order by the governed is necessary to have an effective and efficient system of regulation.[47]

Ideally, the EU would adopt a more congruent and simplified approach to data protection than now exists. This could mean, for example, combining the EU Data Protection Directive and the E-Privacy Directive into a single instrument, to simplify understanding of the relationship between the two. Case studies or guidelines could be published by the Article 29 Working Party and the European Commission, based on consultation between citizens, data protection authorities, and data controllers, in order to provide guidance on application of the legal framework to real-world data processing situations. Data protection rules would become unified to provide a single set of rules as much as possible for both governmental and private-sector processing of personal data. The European Commission would police Member State divergences from the Directive more closely, and Member States and DPAs would discuss important changes to national data protection law and practice among themselves before they were implemented. Of course, the chance of any of these changes being made in the near future is remote.

Data protection law is a European success story that was ahead of its time and has since spread around the world. But the EU Data Protection Directive was enacted just before the Internet revolution and the globalization of data processing got underway, and thus requires rethinking and adjustment to retain its internal cohesion, and thus its effectiveness, for authorities, data controllers, and individuals alike.

[47] See Fuller, *The Morality of Law*, p. 227.