Chapter 1
Introduction to Enforcing Privacy

David Wright and Paul De Hert

1.1 Introduction

This book received its final edit at a crucial moment in the EU process of data protection reform with the finalisation of the trilogue negotiations between the European Parliament, Council and Commission, and the final stage of the arduous process of bringing the General Data Protection Regulation (GDPR) into law. The Regulation contains a new governance model that combines powerful data protection authorities (DPAs), along with increased co-operation, a lead DPA and a European Data Protection Board with real functional and financial independence and the power to issue binding decisions. Attention with regard to DPA co-operation and enforcement should be given particularly to GDPR Chapters VI (supervisory authorities) and VII (co-operation and consistency), the latter defining amongst others the powers of the Board in its consistency monitoring capacity.

The EU reform process was finalised in a rocky period when courts and DPAs started hitting the news with far-reaching actions and judgments.¹

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued the Schrems judgment, invalidating the European Commission’s Decision of 2000 that recognised the adequacy of the EU-US Safe Harbor framework. In addition to this invalidation of the adequacy decision, the CJEU upheld the power of national DPAs to independently investigate international data transfers based on adequacy

¹ Linkomies, Laura, and Stewart Dresner, “Multinational face increasing pressure from DPAs. A Belgian court supported the Belgian DPA’s record breaking 250,000 Euros per day fine on Facebook”, Privacy Laws & Business, Issue 138, 2015, pp. 1–4.

D. Wright (✉)
Trilateral Research, London, UK
e-mail: david.wright@trilateralresearch.com

P. De Hert
Faculty of Law and Criminology, Vrije Universiteit Brussel, Brussels, Belgium
e-mail: paul.de.hert@vub.ac.be; paul.de.hert@uv.it
decisions. The judgment is a must-read concerning enforcement. The Court sees it as a duty flowing from Article 12 of the EU Data Protection Directive and Article 8 of the EU Charter on Fundamental Rights that a DPA, even when there is an adequacy, must, with complete independence, investigate complaints. If the DPA finds a problem, it cannot disable the adequacy decision but must be able to challenge this decision in court.²

As DPA enforcement friendly as the Schrems judgment was, the Weltimo judgment delivered five days earlier was also important. On 1 October 2015, the Court decided in a case concerning a company based in Slovakia but offering services to Hungarians that when a DPA receives a complaint, it may exercise its investigative powers irrespective of the applicable law and before even knowing which national law is applicable.³

This book has been conceived in a wider landscape of reform both inside and outside Europe.⁴ Bringing data protection and privacy to life, turning it from a paper existence into a reality is a common element in all these reforms.

This book tries to capture that development through the lens of enforcement, a term that denotes this process of turning paper into reality or, more eloquently, to translate a set of legal standards designed to influence human and institutional behaviour into social reality.⁵ More is needed for effective and legitimate privacy arrangements than just and clear rules: enforcement can contribute to the legitimacy of these rules: regulators that are endowed with legitimate authority to define and impose norms can easily lose that authority if they have no effective way of enforcing these rules and, conversely, a regulator that achieves a high level of compliance will enhance its legitimacy.⁶

The book does not cover all possible aspects that could be dealt with under the banner of “enforcement” or that could be linked with broader themes. It is definitely

---

⁴For an overview of recent proposals for modernising information privacy law in the USA, the European Union, Australia and New Zealand, see Gunasekara, Gehan, “Paddling in unison or just paddling? International trends in reforming information privacy law”, International Journal of Law and Information Technology, 2013, pp. 1–37. Also, on the matter of accountability in Australia, the United States (e.g., Title V, Gramm-Leach-Bliley Act of 1999) and Canada (e.g., Sch. 1, Principle 1, Personal Information Protection and Electronic Documents Act (PIPEDA), 2000), see Crompton, Malcolm, Christine Cowper and Christopher Jefferis, “The Australian Dodo Case: An Insight for Data Protection Regulation”, BNA World Data Protection Report, Vol. 9, No. 1, 2009, pp. 5–8.
not a book on “regulating” privacy, which is one of these possible broader themes. Within the stricter limits of the theme of enforcement, the book does not address all pending issues. The book does not look in detail at the role of the European Data Protection Supervisor (EDPS) or, for that manner, the future role of the European Data Protection Board. Equally, the organisational aspects of enforcement, such as the right for data protection authorities to prioritise their workflows is not covered and with upcoming court decisions on this aspect, we expect it to be an important legal topic in the future.

We view our book as predominantly pragmatic.

First, we need to say something about the terminology of “privacy” and “data protection”. There is some discussion about the respective content of the terms, their similarities and differences. Some authors use term “data privacy”, embracing in particular the European understanding of “personal data protection” and the Anglo-Saxon one of “informational privacy”, in order to “avoid terminology that might seem focused too much on a particular legal system”. In a similar vein of what matters is the result, we have not insisted on using a specific terminology and although the outcome is a book mainly on data protection, we have opted to use the term privacy on the cover, partly because we view “data protection” as one type of privacy. We prefer the wider term “privacy”, because there are several types of privacy. We think that regulators and privacy advocates should not circumscribe privacy to equate with only data protection. Other types of privacy deserve protection and enforcement too. While this book is primarily concerned with data protection, many of the measures discussed in these pages are applicable to the enforcement of all types of privacy.

---


We also need to explicate the phrase “enforcing privacy”. Enforcement typically means the activity of a regulator to ensure that third parties comply with a law or regulation or code. If regulators do not enforce laws or regulations or codes or do not have the resources, political support or wherewithal to enforce them, they effectively eviscerate and make meaningless such laws or regulations or codes, no matter how laudable or well-intentioned. This is the challenge that many regulators face: they do not have the resources or political support for enforcement to do their jobs effectively. In some cases, however, the mere existence of such laws or regulations combined with a credible threat to invoke them is sufficient for regulatory purposes. It may not be necessary to enforce privacy regulation against every company that fails to comply. Selective enforcement may be sufficient to send a message to all delinquent companies (as well as public sector or even third sector organisations) that they should get their houses in order. But the threat has to be credible. As some of the authors in this book make clear – it is a theme that runs throughout this book – “carrots” and “soft law” need to be backed up by “sticks” and “hard law”.

In this book, we and our co-authors view privacy enforcement as an activity that goes beyond regulatory enforcement. In his chapter, Graham Greenleaf distinguishes between enforcement and compliance. He points out that there is often evidence of enforcement of national laws, but there is little information on the extent of compliance. In some sense, enforcing privacy is a task that befalls to all of us. This is a point that James Rule makes in his envoi to our book. Privacy advocates and members of the public play or can play an important role in enforcing privacy. For those of us old enough, we might recall the proclamation of Howard Beale, the veteran news presenter played by Peter Finch in the 1976 classic film *Network*: “Things have got to change. But first, you’ve gotta get mad! You’ve got to say, ‘I’m as mad as hell, and I’m not going to take this anymore!’” This is where we are with the continuing intrusions upon privacy by governments, intelligence agencies and corporate warlords. It might serve their interests to say that privacy is dead, but it does not serve our interests, the interests of we the people, of a healthy, democratic society. In effect, we have to echo Howard Beale and say that we are as mad as hell and we are not going to take it anymore. Edward Snowden obviously felt this way. There are different ways to enforce privacy, in addition to those of the regulator. The essays in this book demonstrate some of the different ways by means of which we, collectively, can enforce privacy.

This brings us to a second point: the geographical scope of the book is global. Authors from all over the globe are participating and their valuable voices are heard in all four sections of the book: countries, international, instruments, the future. This explains why we have perspectives on international enforcement written by authors coming from several continents and why the country reports on Spain and Hungary are followed by reports on Japan, the US and Latin America. These reports are not structured in an identical way. A rigid format does not always guarantee vivid or interesting outcomes. To compensate for the relative freedom of direction accorded to authors, almost all authors participated in a closed workshop convened by the editors as a side event at the conference on *Computers, Privacy and Data Protection* held in Brussels in January 2014.
Third, respectful of the ambition of that important Brussels conference was the editors’ decision not to limit the book to one group of authors, for instance, academics, but to consult a wider group of people willing to author a contribution – hence, the presence of activists, of officials working for data protection or privacy-related authorities and prominent policy-makers. Some of the more political voices are clustered in the Future section, with minimal editorial restriction so as to respect the energy, vision and willingness to impact on the policy agenda. To us, the chapters in that section will become useful testimony for subsequent researchers and with more than just tolerance, we accepted some of them being written in the first person singular.

1.2 Pragmatism and theory: two themes strike the attention

The choices discussed above are identical to the ones we made four years ago when we compiled Privacy Impact Assessment, a 523-page book allowing a multitude of authors with different geographical and professional backgrounds to speak out on a novel phenomenon that is developing globally but not at the same speed. The reception of that book in terms of appreciation and sales was excellent and strengthened our belief that this kind of mixed book was indeed answering a need to go beyond strictly practical or academic books. We then and now opted to refrain from giving strict thematic direction or to ask contributors to test a certain hypothesis or theory.

We are well aware that out there is a burgeoning field of theory and evidence with regard to policy-making and especially regulatory policy. The choice to engage with that literature was left to the authors. Several authors, in particular those with an academic background such as Greenleaf and De Hert and Boulet have taken up the challenge. That does not mean that the book as a whole does not deliver cross-cutting themes that are theoretically relevant. Two themes strike the attention.

First, there is the theme of state regulation v. self-regulation. The latter is the central topic in the third chapter (“Failures of Privacy Self-Regulation in the United States”), but the theme echoes throughout other chapters as well. Law students are most familiar with state-controlled norm-setting and enforcement. The reality is far more complex and shows the existence in many domains of society of governance structures other than government structures, systems of rule-creation and enforcement that do not depend solely on state command-and-control, but instead involve participants from a wider community. An extreme form of governance is self-regulation, a model where those who are the primary subjects of the system’s rules come together to agree a governance structure and undertake to abide by the rules it produces. The model is not absent, also in the context of the Internet. Think only of the rule-setting by major IT firms when developing the technological architecture. But the purely self-regulatory model is not a dominant one since governments and

---

states need to step in for a plurality of reasons (power, concern for privacy and other fundamental rights, etc.). Governance of this type is referred to as co-regulation, to be distinguished from governance purely by law, on the one hand, or self-regulation or contract on the other. Reed rightly observes that co-regulation has become the predominant governance structure for those Internet activities extending beyond national boundaries, but even for purely national arrangements, various factors can account for a turn to co-regulation.

The impact of these regulatory models on the theme of enforcement is evident; enforcement is a particular problem with self-regulatory governance systems because they tend to lack coercive mechanisms to sanction rule-breaking. Self- and co-regulatory strategies need to be continuously monitored to see whether they keep their promises. The same, however, goes for state-controlled regulation. Too few are the studies critically examining the output of, for instance, the public authorities that are said to help safeguard our privacy and personal data. Enforcement, therefore, has become a key duty for all. The efforts of governments and big companies towards social sorting, categorisation, profiling and data matching erode individuality and propel us ever closer to Huxley’s *Brave New World*. Invasions of privacy lead to a breakdown in trust. If we know that governments, big companies and other evil-doers are spying on us, without our consent, we are less likely to trust them. The loss of trust in social institutions leads to a loss of social capital; it creates a dysfunctional, distrusting society. Government and big companies know more and more about us, but we know less and less about them and about what they are doing with our personal data. Privacy is essential for trust in political and social institutions.

Second, but linked to the foregoing, there is the debate on the choice of enforcement instruments. Successful enforcement seems to demand coercive means of enforcing regulations, even if that coercion is used only as a last resort. The importance of the recent actions by competent US authorities (the Federal Trade Commission in particular) to check on the firms that have accepted the Safe Harbor agreement is therefore more than significant. The whole EU policy agenda today seems to be turned towards creating more coercion and giving administrative enforcement powers to the national data protection authorities, but strangely enough, this book, at least several contributions to it, brings the message that “hard” powers need to be complemented by “soft” powers and that “sticks” are in need of “carrots”. Billy Hawkes, former Irish data protection commissioner, says in his country the use of both “soft” and “hard” enforcement measures “is to bring about compliance rather than to punish. Even where punitive action is taken through the courts,
the objective is always to achieve compliance by the offending organisation and by other organisations in its sector.” To achieve such outcomes, a DPA needs a range of “hard” and “soft” powers, as Hiroshi Miyazaki comments. Also important, as Billy Hawkes further notes, is the ability of the DPA to deploy the tools in its regulatory tool-box with flexibility and an ability and willingness to work closely with other regulators. These are, he says, key enablers for smaller DPAs. Other DPAs favour a tougher sanctions regime. Dutch DPA Jacob Kohnstamm says in his chapter that significant fines will help data protection authorities to carry out their task and that being able to impose sufficiently high fines can act as a deterrent to data controllers, leading to a higher degree of compliance. Billy Hawkes says that it is open to question whether the more punitive approach adopted in the Regulation will actually lead to a higher standard of compliance. In this regard, it is interesting to note that the Spanish regulator which had the highest fines and highest number of fines decided to “modulate” its fines, sticks in favour of a softer approach. The evidence shows that DPAs have some different approaches and regulatory philosophies. What does the empirical evidence suggest? Grant and Crowther in their capter suggest that fines need to be complemented by other instruments such as naming and shaming.

The “sticks and carrots” logic in regulation is more than anecdotic: for the tortoise to move, both a stick and a carrot are needed; for a governing mechanism to work, both threats and incentives are needed. Under this perspective, the provisioning of sanctions – and not necessarily their imposition – and the increased load of obligations seem to hold the role of the stick in the earlier mentioned metaphor, which needs to be coupled, though, with a “carrot”. The “carrot” implies providing for a “suitable” incentive, for an appropriate stimulation that would sufficiently tempt data controllers to move towards the inspired vision of “not mere compliance”. The golden question in this regard is whether the respective legislative frameworks envisage carrots and whether choices between hard law and soft law, between carrots and sticks, are legitimate or, on the contrary, purely opportunistic. Taking this scheme seriously demands creativity. Taking that question into account, one could, for instance, defend the proposition that no notification of breaches – always bad for reputation – is needed when preventive security measures are taken. The awareness that Europe today is perhaps too focused on creating sticks, partly justifies chapters with experiences from abroad (negative, but also positive), chapters on the use of technology to regulate and enforce norms and chapters reflecting on the purposes of administrative fines as opposed to criminal fines. The wealth of detailed description in Chap. 2 teaches us that the work of data protection authorities cannot be presumed to impose sanctions alone.

1.3 The structure of the book

For this volume, we have brought together experts in the field of enforcing privacy. Contributors to this book include privacy advocates, regulators, academics, lawyers, a technologist and a parliamentarian. In this volume, they consider different ways of enforcing privacy and different issues that arise in attempts to enforce privacy.

Following this Introduction, David Wright reviews the enforcement powers of data protection authorities, but makes the point that not all DPAs have all enforcement powers they need. Hence, DPAs often co-operate with each other and sometimes co-ordinate their enforcement actions as a way to leverage their shortage of resources. Nevertheless, they face various barriers to co-operation and co-ordination, which they are attempting to overcome. Wright’s chapter sets the scene for the rest of the book, which considers various ways of enforcing privacy.

As mentioned above, the contributions to this book are clustered in four main sections. The first concerns countries, the second focuses on international mechanisms, the third on instruments and the fourth on challenges for the future.

The first section focuses on the US, Hungary, Japan, Spain and Latin America. Self-regulation puts the onus for enforcing privacy on individual organisations, but the title of Bob Gellman and Pam Dixon’s chapter – “Failures of privacy self-regulation in the United States” – says it all: self-regulation is not an effective way of enforcing privacy. They back up their contention with various examples, including self-regulatory activities with the involvement of government, industry, academia and civil society.

Across the Atlantic, Ivan Szekely performs a case study of enforcing privacy and data protection in Hungary, where political factors undercut the regulator’s powers, which has drawn criticism from the European Commission and others. The title of his chapter is “From a model pupil to a problematic grown-up”, by which he means that Hungary initially led the way in eastern Europe’s transition to democracy in the early 1990s, but then faltered. He concludes that Hungary’s positive and negative experiments in enforcing privacy can serve as a model for both European and non-European countries.

In Japan, Hiroshi Miyashita explores the relative effectiveness of hard power and soft power as mechanisms for enforcing privacy. He also explores the differing enforcement approaches in Japan and Europe, as illustrated by the hacking of the Sony PlayStation Network.

Artemi Rallo, formerly Director of the Spanish Data Protection Authority (Agencia Española de Protección de Datos, AEPD), considers hard power and soft power too, but uses the terminology of sticks and carrots. Heretofore, Spain has had the toughest sanctions for breaches of its data protection law, but in recent years, the AEPD has modulated its “sticks” (relatively heavy fines) in favour of “carrots” (lower fines). The chapter explores whether this has made a difference in terms of enforcing privacy.

The first section of the book ends with a chapter on enforcing privacy in Latin America, with special attention paid to Uruguay, by Ana Brian Nougrères. Data protection legislation is a relatively new phenomenon in Latin America, but eight
countries have adopted legislation since Argentina took the initiative in 2000. Argentina together with Uruguay has the distinction of meeting the adequacy standards set out in the EU’s Data Protection Directive.

The second section of the book focuses on international mechanisms for enforcing privacy. There are various regional and thematic networks that help in this process, and one of these is the International Working Group on Data Protection in Telecommunications (IWGDPT), which is the subject of the chapter by Alexander Dix, the chairman of the IWGDPT. The first point that he makes is that privacy today can no longer be enforced on a national level only, an observation with which we fully agree. Dan Svantesson takes up the theme in his chapter on enforcing privacy across different jurisdictions. He considers jurisdictional issues that arise where there are differences in privacy laws, and then examines the implications of the International Covenant on Civil and Political Rights (ICCPR) on the enforcement of privacy across different jurisdictions.

Blair Stewart, New Zealand’s Assistant Privacy Commissioner and a pioneer of privacy impact assessment, makes the case for mandatory breach notification as a means of enforcing privacy and, in particular, he discusses cross-border notification, an issue that has not had much air time until now. He argues that policy-makers and regulators must pay more attention to the parameters of cross-border notification if its potential is to be realised to the benefit of our globalised economy.

His Antipodean colleague, Graham Greenleaf, proposes “responsive regulation of data privacy” as a measure for assessing data privacy laws, which he does with regard to the 12 Asian countries that have such laws. Along the way, he makes some comparisons between Asia and Europe, especially in regard to their enforcement mechanisms. He points out that no Asian privacy regulator has yet levied fines measured in hundreds of thousands of US dollars, as is now a frequent occurrence in both Europe and the US.

Chris Connolly and Peter van Dijk bring us back to the Atlantic side of the planet with their chapter on enforcement and reform of the EU-US Safe Harbor agreement. That agreement has generated controversy ever since its introduction in 2000 as a way of sidestepping the adequacy requirements of Article 25 of the EU Data Protection Directive. As a means of enforcing privacy, the agreement has been less than effective, at least, not until very recently. They blame poor enforcement of the agreement. At the time this book goes to press, the European Commission and the US Department of Commerce are attempting to reach an agreement on a replacement for the original Safe Harbor agreement.

The third section of the book discusses instruments for enforcing privacy. Hazel Grant and Hannah Crowther consider how effective monetary penalties (or fines) have been at enforcing privacy, with a particular focus on the fines levied by the UK Information Commissioner’s Office (ICO). They stress the importance of combining fines with other enforcement measures, such as “naming and shaming”. Although the ICO has some of the highest fines in Europe at its disposition, they raise the question whether the UK’s fines are too low to be effective. As they note, that question should go away when the European Data Protection Regulation comes into force. The Regulation contains a provision for fines of up to four per cent of a company’s turnover.
Another important instrument for enforcing privacy is class action litigation. The US has had far more experience with class action suits than any other country. Marc Rotenberg, Director of the Electronic Privacy Information Center (EPIC), and his colleague David Jacobs delve into the intricacies of class action suits and, in particular, the efficacy of cy pres awards, the theory of which is to make the award to some entities on behalf of consumers where the awards to individual consumers would be nominal at best. Cy pres derives from the French phrase si près, which literally means “so near” or, in this context, “as near as possible”.

Kirsten Bock’s chapter poses the question of whether data protection certification and privacy seals are effective instruments for enforcing privacy or merely decorative. The answer is that it depends. She sets out various conditions that must be met in order for privacy seals or trustmarks to be effective.

Paul De Hert and Gertjan Boulet consider administrative and criminal law sanctions as remedies to infringements of data protection law. They reflect on the relative “silence” regarding enforcement under the European data protection legal framework. The Data Protection Regulation distinguishes between criminal and administrative sanctions. It makes administrative enforcement mandatory but leaves criminal enforcement optional. They contend that the lack of harmonisation of criminal law sanctions is unsatisfactory. They recommend that Member States define as clearly as possible what offences shall be considered criminal or administrative, and enforced by means of criminal and administrative law.

Regulators and individuals can enforce privacy through the use of technologies. Daniel Le Métayer takes us on a tour of privacy-enhancing technologies. However, as he points out, the adoption of these technologies is still rather limited, even if it is growing, especially in the aftermath of recent privacy breach scandals. He adds that we cannot evade the issue of trust in the technologies themselves, that recent history has shown that cryptographic tools that were considered as the cornerstone of many secure systems might very well have been either bugged or hacked by secret agencies and might thus have been a major source of leaked personal data for years. He concludes that technology can play a key role in enforcing privacy but should not be used in isolation or seen as a convenient way to forget about privacy.

The fourth and final section of the book addresses challenges for the future. Billy Hawkes, formerly data protection commissioner of Ireland, explores the challenges facing data protection authorities with limited (human) resources in enforcing privacy. He examines the enforcement approach of the Office of the Data Protection Commissioner (ODPC), focussing on its use of a combination of “soft” and “hard” enforcement tools. He examines in particular how the ODPC has used its audit tool in relation to Ireland-based multinational companies that process personal data in connection with the provision of services across the European Union. He also comments on how the ODPC has involved other DPAs in such investigations and how this situation might change under the Data Protection Regulation.

Billy Hawkes’ counterpart in the Netherlands, Jacob Kohnstamm, follows with a chapter entitled “Getting our act together: European Data Protection Authorities
face up to Silicon Valley”. Kohnstamm speaks of the challenge facing DPAs in working more closely together across borders. His chapter reviews some joint investigations by European and other DPAs in the past decade or so, and then looks to the future to identify what is needed to facilitate better co-operation across borders. He comments that the biggest challenge for data protection authorities is getting organisations to acknowledge that privacy by design, transparency and respecting the personal nature of their customers’ data is good for business. But another challenge is arriving at the point where data subjects can trust organisations to follow the rules.

The last chapter in this last section, written by Member of the European Parliament Jan Philipp Albrecht, is entitled “Regaining control and sovereignty in the digital age”. He was the rapporteur for the European Parliament’s position on the Data Protection Regulation. He contends that the Googles and Facebooks of this world “disempower us not only as customers who consume what they have to offer but also as citizens of democratic societies governed by the rule of law. They dictate their rules to us. This is particularly true of what drives and perpetuates the new economy: our “personal data””. His challenge for the future is stark: “If things remain as they are, we shall be completely disenfranchised and easily fleeced in the digitised world. We shall find ourselves living in a totalitarian controlled society, which has come into existence and holds sway because these businesses gather vast amounts of information about us, and are becoming more entrenched in our daily lives.” Albrecht’s chapter may be a sombre assessment of the realpolitik in progressing data protection reform, but appropriate nevertheless. His chapter underscores the importance of enforcing privacy.

We asked privacy guru James Rule to write a kind of envoi for the book, his view on the future of privacy enforcement. He acknowledges as “impressive” the global community of professionals who enforce privacy codes, but says they face a complex and daunting array of forces against their efforts. He says that public indignation against privacy intrusions has resulted in the establishment or strengthening of privacy institutions. He concludes that the “defenders of privacy need to consider measures that will more greatly mobilise the attentions of individual data subjects”. To that end, he recommends the development of “hard-hitting, galvanising appeals that will resonate with ordinary people’s privacy concerns – and embed themselves in public attention, even in the absence of dramatic events like the Snowden revelations”. He suggests three such galvanising appeals or “capsule” demands for “Strong Privacy” to help solidify an alliance between the public and professional privacy advocates.

Despite the cynicism of corporate warlords who declare that privacy is dead, the contributors to this book clearly do not agree. We, the editors, hope this book offers readers and policy-makers some insights into what works and doesn’t work as measures to enforce privacy. If those insights translate into stronger measures and if this book creates greater resistance to those who proclaim the death of privacy, then we will have achieved our objective.
References


*Privacy Laws & Business*, “EDPS aims to be proactive and focus on external relations”, Issue 133, 2015, pp. 1–4.

