2015

Risk Management in Data Protection

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Brussels Privacy Hub

Christopher Millard
Cloud Legal Project

Dan Jerker B. Svantesson
Bond University

Orla Lynskey
London School of Economics

Editorial

Risk management in data protection

Christopher Kuner*, Fred H. Cate**, Christopher Millard**, Dan Jerker B. Svantesson****, and Orla Lynskey****

Data protection has long relied on risk management as a critical tool for ensuring that data are processed appropriately and that the fundamental rights of individuals are protected effectively.

Risk management is an explicit requirement of many data protection laws. For example, the 1988 US Computer Matching and Privacy Protection Act requires government agencies to perform a cost–benefit analysis of proposed data matching.[1] Security breach notification laws often link notice to an assessment of the risk to individuals posed by the breached information. As the Article 29 Data Protection Working Party has noted, for notification to be effective 'it is important to have an appropriate risk management framework in place . . .'.[2] And risk management is the goal of Privacy Impact Assessments.

The EU Data Protection Directive 95/46/EC requires that security measures must 'ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected' (Article 17); that 'processing operations likely to present specific risks to the rights and freedoms of data subjects' be subject to 'prior checking' by Member States (Article 12); that personal data may be processed when 'necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subjects . . .' (Article 7(f)); and that access rights to data processed for scientific research may be limited 'where there is clearly no risk of breaching the privacy of the data subject' (Article 13(2)).

Even beyond these familiar legal requirements, many organizations have employed risk management as an effective tool for protecting privacy.

However, in recent years, risk management has started to take on a more prominent role in data protection. For example, the Article 29 Working Party stressed in its 2014 *Statement on the role of a risk-based approach in data protection legal frameworks* that the role of risk management in data protection is 'not a new concept, since it is already well known under the current Directive 95/46/EC', and that 'the risk-based approach has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation'.[3]

The draft text of the European Union General Data Protection Regulation indeed focuses significantly on risk management. The text that emerged from the European Parliament stresses the need for 'the controller or processor' to 'evaluate the risks inherent to the processing and implement measures to mitigate those risks'.[4] The draft Regulation would require data controllers to demonstrate compliance with it having regard to, among other things, the 'risks for the rights and freedoms of the data subjects'.[5] Under a wide variety of circumstances the controller would be required to 'carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks'.[6] The draft of a 'partial general approach' to Chapter IV of the Regulation that has been circulated by the Council Presidency further builds on the risk-based approach, conditioning the obligations of the data controller to implement appropriate measures and be able to demonstrate compliance with the Regulation on 'the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights

* Editor-in-Chief.

** Editor. Professor Cate is a senior policy advisor at the Centre for Information Policy Leadership at Hunton & Williams LLP and has participated in their project on risk management.

** Editor.

*** Managing editor.

**** Book review editor.

1 5 USC § 552a(o).

2 Article 29 Data Protection Working Party, *Opinion 03/2014 on Personal Data Breach Notification*, 693/14/EN WP 213 (2014), 4.

3 Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN, WP218 (2014), 2.

4 European Parliament Resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, P7 TA(2014)0212, 12 March 2014, ¶ 66.

5 Id, at art 22.

6 Id, at art 32a.

and freedoms of individuals'.[7] The risk-based approach is further reflected throughout the Council's text.[8]

There are other recent examples of the new prominence given to risk management. In 2013 the Council of Ministers of the Organisation for Economic Co-operation and Development (OECD) revised the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, first adopted in 1980, to 'implement a risk-based approach'.[9] In the accompanying Explanatory Memorandum, the drafters noted the 'importance of risk assessment in the development of policies and safeguards to protect privacy'.[10]

And there have been a host of government reports on risk management in data protection. The French Commission Nationale de l'informatique et des Libertés (CNIL) led the way with its *Methodology for Privacy Risk Management*, revised most recently in 2012, which 'describes *a method for managing the risks* that the processing of personal data can generate to individuals'.[11] There the CNIL writes: 'Using a risk management method is the safest way to ensure objectivity and relevance of the choices to make when setting up a processing of personal data'.[12]

The US Federal Trade Commission in 2012 published a report recommending that companies should 'implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization'.[13]

In 2013, the UK Information Commissioner's Office published an exhaustive report on *Privacy Impact Assessment and Risk Management*. Prepared by Trilateral Research & Consulting, the report reflects an effort to promote a better 'fit' between PIAs and 'risk management standards and methodologies'.[14] The ICO subsequently published a comprehensive PIA Code of Conduct in February 2014, which provides organizations with step-by-step guidance on how to conduct PIAs and advises them to consider privacy and related risks to individuals.[15]

The US National Institute of Standards and Technology (NIST) in 2014 issued a Privacy Risk Model discussion draft to help organizations to 'assess the privacy impact on individuals whose information is collected, used, stored, and transmitted by information systems, and how organizations can prevent adverse impact on those individuals'.[16] The year 2014 also saw the publication of the Article 29 Working Party's *Statement on the role of a risk-based approach in data protection legal frameworks* in which it noted support for 'the inclusion of a risk-based approach in the EU data protection legal framework'.[17]

To be clear, we do not believe that privacy can be viewed solely as a risk management exercise based on quantified definitions of 'harm'. However, we do applaud the attention being given to risk management and its role in data protection. In its proper place, risk management can help prioritize the investment of scarce resources in protecting privacy and enforcing privacy obligations. It can identify serious risks to privacy and measures for mitigating them. It can expand our collective thinking about the range of risks that the processing of personal data can present to individuals, organizations, and society, especially in a world of nearly ubiquitous surveillance, big data, cloud computing, and an onslaught of Internet-connected devices. And it can help bring rigor and discipline to our thinking about data processing and how to maximize its benefits while reducing its costs.

But however valuable, risk management is no panacea, and there is substantial work to be done if it is to achieve its full potential for protecting privacy. We wish to highlight four areas that we believe are essential to obtaining a maximum value from risk management.

First, despite the long-standing role of, and intensified recent attention to, risk management in data protection, it is still a developing field that lacks many of the widely accepted principles and tools of risk management in other areas.

It is vital that risk management around data protection, while remaining flexible, not continues in the largely ad hoc, colloquial terms in which it has evolved today. In other areas—for example, financial and environmental risk—we have seen the development of a professional practice of risk management, including specialized research,

7 Note 13772/14, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [First reading]—Chapter IV (2014), at 13 [art. 22.1].

8 See id, at arts 23, 25, 30–34, 44.

9 Organization for Economic Co-operation and Development, *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), 30.

10 Organization for Economic Co-operation and Development, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended by C92013)79 (2013), 12.

11 Commission Nationale de l'informatique et des Libertés, *Methodology for Privacy Risk Management* (2012), 4.

12 Id, at 9.

13 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012), 30.

14 Trilateral Research & Consulting, *Privacy Impact Assessment and Risk Management* (2013), 15–16.

15 UK Information Commissioner's Office, *Conducting Privacy Impact Assessment Code of Conduct* (2014).

16 National Institute of Standards and Technology, *NIST Privacy Engineering Objectives and Risk Model Discussion Draft* (2014), 3.

17 Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN, WP218 (2014), 2.

international and sectoral standards, a common vocabulary, and agreed upon principles and processes. The same is needed in data protection risk management. In some cases, these can be borrowed from areas in which formal risk assessment is more fully developed, but in others it requires the collaboration of regulators, industry, and academics to fill important gaps.

Second, one of the most obvious omissions to date is a clear understanding of the harms or negative impacts that risk management is intended to identify and mitigate in the area of data protection. This is the starting point for effective risk management in other fields, yet in data protection regulators and businesses alike have failed to articulate a comprehensive framework of harms or other impacts, much less to reach consensus regarding those that should be part of effective risk management. Much work remains to be done on the critical issue of identifying the relevant impacts that should be considered in risk management.

Private sector entities have also been active in attempting to further define the relationship between data protection and risk management. In 2014, the Centre for Information Policy Leadership at Hunton & Williams LLP issued a white paper, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, that focused on this critical issue: 'Data protection and privacy laws are meant to protect people, not data. But from what exactly are people being protected? What threats? What harms? What risks?'[18] The Centre proposed a matrix of these harms in an effort to move the process of creating, vetting, and ultimately building consensus around a framework of harms and other negative impacts. Much work remains to be done on the critical issue of identifying the relevant impacts that should be considered in risk management.

As NIST has noted: 'Harms from security breaches are generally well understood. In privacy, consensus is still being developed around what constitutes harms. However, if the privacy engineering objectives are intended to mitigate the risk of privacy harms, then the underlying harms need to be explicated in order to assess the utility of the objectives'.[19]

There appears to be growing agreement that harms must be understood to include not only tangible impacts, such as financial or physical harms, but also intangible impacts and possibly even broader harms to society more broadly. But beyond these broad concepts, there is little agreement.

This is a serious shortcoming because making risk management work effectively and consistently requires that there be a widely shared classification of impacts—positive and negative—on individuals, organizations, and society. Specific categories might differ from country to country or culture to culture, but the absence of a common understanding as to what impacts should be minimized (or maximized) threatens not only quality risk management and meaningful accountability, but also effective data protection. Opinions differ as to the standard for measuring risk: some argue that, as the Centre for Information Policy Leadership has noted, the approach to the categorization of impacts needs to be based on '*objective* descriptors of harm',[20] while others find that the status of data protection as a fundamental right makes this determination inherently subjective.

The absence of a widely accepted framework of impacts to be avoided or sought out presents both an opportunity and a challenge. The opportunity is to develop modern, effective risk management tools and a framework of impacts—both harms and benefits—building on decades of experience with risk management broadly. The challenge is to do so quickly to keep pace with dramatic changes in technology and human and institutional behaviour. Regulators and industry need to act speedily to identify possible approaches to creating workable frameworks and building consensus around them.

Third, it is critical that everyone involved in data protection have realistic and appropriate expectations for risk management. Risk management does not—and should not—alter rights or obligations. If a law conveys a right to data protection, risk management cannot alter that right, just as if the law imposes obligations on controllers or processors, risk management does not change those obligations.

While risk management does not alter rights or obligations, it may be essential to determining when rights or obligations are implicated. It is true that the Court of Justice of the European Union has held that as a general principle, an interference with data protection rights does not depend on whether there has been any harm or inconvenience to an individual. However, some specific obligations may be activated only if a harm is present. For example, under the Parliamentary text of the draft General Data Protection Regulation, 'indiscriminate general notification' of security breaches would be abolished, and 'replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects'.[21] Under this regime, risk

18 Centre for Information Policy Leadership at Hunton & Williams LLP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* 2 (2014), see also Centre for Information Policy Leadership at Hunton & Williams LLP, The Role of Risk Management in Data Protection (2014).

19 *NIST Privacy Engineering Objectives and Risk Model Discussion Draft*, at 3, n 9.

20 CIPL, *A Risk-based Approach to Privacy*, at 7.

21 Id, at ¶ 70.

assessment therefore would be necessary to know when notification or other obligations might apply. Similarly, the revised *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* are limited in their scope to personal data that 'because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties'.[22] Absent an assessment of that risk, it is impossible to know whether the guidelines even apply.

Similarly, the goal of risk management is not to eliminate risk, but to reduce the risk as fully as practical and to be explicit about the remaining risks and how they will be managed so that the controller, and ultimately the data subjects and the regulators, understand the risks and undertakings that remain.

Risk management can also identify 'appropriate' responses that are effective in mitigating risks but also support the often critical benefits that risk management necessarily involves balancing.

The Explanatory Memorandum that accompanied the 2013 revisions to the OECD Guidelines makes it clear that management of 'risk' is intrinsically connected with 'proportionality', indicating, in the context of transborder data flows for example, that 'any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (i.e. not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data, the purpose and context the processing'.[23]

The Article 29 Working Party has recently echoed this theme in the context of applying legitimate interests under article 7(f) of the EU Data Protection Directive: 'The purpose of the Article 7(f) balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference'.[24]

Finally, to be effective, risk management must work in practice. This requires that risk management tools be efficient, scalable, and flexible, so that they work for large organizations and for small SMEs.

This has been a particular focus of the ongoing negotiation over the Regulation. In its 3 October 2014 note to the Council detailing efforts to reach agreement on a 'partial general approach' to article IV, the Presidency noted 'the need to further reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-based approach'.[25] As one step towards that end, the draft text suggests that 'best practices to mitigate the risk' could be provided by 'approved codes of conduct, approved certifications, guidelines of the European Data Protection Board or through the indications provided by a data protection officer'.[26]

In addition, the regulation of risk management should avoid unnecessary or duplicative risk assessments. For example, the EU Parliament's text of the draft EU General Data Protection Regulation provides that a 'single assessment shall be sufficient to address a set of similar processing operations that present similar risks'.[27]

It is also important that data protection risk management tools fit within existing risk management methodologies and programmes. This is necessary for many reasons, including allowing data protection risk management to benefit from the expertise developed in other areas, ensuring that data protection risk management takes advantage of the considerable resources already being devoted by organizations to risk management in other areas, and enhancing the efficiency (and reducing the cost) of data protection risk management.

Risk management offers substantial benefits for the practice of data protection, focusing scarce resources where they are needed most, protecting individuals' fundamental rights effectively and appropriately, and facilitating efforts to make data protection more seamless across national borders. To achieve these goals, however, there remains substantial work to be done, and we encourage regulators and business leaders to work together and with experts in risk management in other areas, civil society, and academics to ensure that risk management achieves its full potential in data protection.

doi:10.1093/idpl/ipv005
Advance Access Publication 12 May 2015

22 *OECD* Guidelines, at ¶ 2.

23 OECD, *Supplemental Explanatory Memorandum,* at 30.

24 Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN, WP218 (2014), 41.

25 Note 13772/14, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [First reading]—Chapter IV (2014), at 1.

26 Id, at 4.

27 Draft EU General Data Protection Regulation (unofficial consolidated version after LIBE Committee vote), at art 33, ¶ 1.