Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

20-Jan-2016

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

DSTI/ICCP/REG(2015)1/REV2
For Official Use

Working Party on Security and Privacy in the Digital Economy

OPPORTUNITIES AND CHALLENGES IN DEVELOPING A RISK MANAGEMENT APPROACH TO PRIVACY

This draft revised report reflects suggestions made by SPDE delegates. Its content will be used as a basis for the background report prepared by SPDE for the Cancun Ministerial Meeting (21-23 June 2016).
CDEP delegates are invited to approve this report for declassification by the written procedure by January 30. Unless objections are received by this date, the report will be considered declassified.

E. Ronchi: elettra.ronchi@oecd.org; L. Bernat: laurent.bernat@oecd.org

JT03389146

Complete document available on OLIS in its original format

English - Or. English

NOTE BY THE SECRETARIAT

This draft revised report reflects suggestions made by SPDE delegates. Its content will be used as a basis for the background report prepared by SPDE for the Cancun Ministerial Meeting (21-23 June 2016).

CDEP delegates are invited to approve this report for declassification by the written procedure by January 30. Unless objections are received by this date, the report will be considered declassified.

The report was developed by Carman Baggaley, consultant to the OECD and former Senior Strategic International Policy Analyst at the Office of the Privacy Commissioner of Canada.

TABLE OF CONTENTS

INTRODUCTION

1. Thinking about privacy from a risk perspective is not new. The Security Safeguards Principle in the original 1980 OECD Guidelines refers to the need to protect personal data from the "risk" created by unauthorised access, destruction, use modification or disclosure of data. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, introduced in the following year, refers to risk and the European Union's Data Protection Directive 95/46/EC contains several references to risk.

2. However, the concept of risk has evolved significantly since 1980. Many organizations now use sophisticated risk management tools and processes to take risk into account in their day-to-day activities. Taking note of these developments, policy makers, academics and privacy professionals have recently started to think about applying risk management systematically to make the protection of privacy more rigorous and more effective. In particular, the revised OECD Privacy Guidelines highlights the importance and potential value of taking a risk management approach to privacy protection:

> "Personal data are increasingly used in ways not anticipated at the time of collection. Almost every human activity leaves behind some form of digital data trail, rendering it increasingly easy to monitor individuals' behaviour. Personal data security breaches are common. These increased risks signal the need for more effective safeguards in order to protect privacy."[1]

3. One of the most significant changes to the Guidelines was the inclusion of a new Part Three recommending that organisations introduce "privacy management programmes" – a new concept in the Guidelines – as a means of implementing the Accountability Principle. These programmes should include "appropriate safeguards based on privacy risk assessment".

4. The revised Guidelines also recognize that notification to enforcement authorities and individuals of security breaches involving personal data should be based on an assessment of the risk:

> "Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. … Accordingly, the new provision that has been added to the Guidelines … reflects a risk-based approach to notification."[2]

5. In addition, paragraph 18 recommends that any restrictions on transborder flows of personal data should be "proportionate to the risk presented taking into account the sensitivity of the data, and the purpose and context of the processing."

6. As the Supplementary Explanatory Memorandum that accompanies the revised Guidelines notes, the need to develop safeguards based on privacy risk assessment is a recurring element in the discussions about privacy management programmes.

7. While the revised Guidelines emphasize the importance of applying the concept of risk to privacy, the Supplementary Explanatory Memorandum does not elaborate on or explain how such an approach would work in practice, nor does it define this concept. In March 2014, the OECD Working Party on Security and Privacy in the Digital Economy (SPDE) held a roundtable that began to explore the practical aspects of a risk management approach to privacy protection.

8. Building on these discussions and on a subsequent meeting of the Working Party, this paper elaborates on the general concepts of risk and risk management; provides an overview of the current

interpretation of the concepts of privacy risk and privacy risk management; discusses the differences between these concepts and the general risk management approach, and explores avenues to reconcile them. The paper also discusses some of the potential benefits of applying a risk management approach to privacy and identifies possible areas for future work.

9. This paper draws heavily on the OECD Recommendation on *Digital Security Risk Management for Economic and Social Prosperity* ("OECD Security Risk Recommendation") on its Companion Document[3], and on the OECD's work on the *Data-Driven Innovation*[4].

10. The OECD has a long history of advocating the use of risk management in a number of different areas as part of its mandate of "Better Policies for Better Lives." See for example, *Disaster Risk Assessment and Risk Financing: A G20 / OECD Methodological Framework* and *Recommendation of the Council on the Governance of Critical Risk.*[5]

RISK AND RISK MANAGEMENT: AN OVERVIEW

11. This section provides an overview of the general concept of risk and risk management as they are currently understood. It builds more particularly on recent OECD work on digital security risk management.

Defining Risk

12. In common language, risk refers generally to the possibility that an event, usually undesirable, will occur. As the Companion Document to the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity notes, "Everyday language uses the term risk in a loose way. For example, it can be used to mean threat, vulnerability, incident, likelihood, chance and danger. Risk management, however, requires a clear distinction between causes and their consequences and addresses the former (threats, vulnerabilities and incidents) in order to manage the latter (risk)."[6]

13. Individuals engage in activities to achieve some objective, seizing opportunities in view of some benefits. When doing so, they consider both the potential benefit and the risk. The risk includes the potential for adverse effects resulting from their actions: loss of money, undermined reputation, physical or psychological damage, etc. Individuals deal with risk numerous times a day, such as when they cross the street to catch the bus. Most of the time, they manage the risk intuitively. They approximately assess the potential benefits of an action as well as the uncertainty related to it. Then they adjust their decision to minimise the possibility that an undesirable incident or outcome will occur. We drive more slowly when driving conditions are poor; some people choose not to fly when they travel; and some people purchase extended warranties when they purchase electronic goods. In the first scenario, driving more slowly reduces the risk; in the second scenario not flying is an attempt to avoid the risk associated to flying, foregoing the benefit of faster travel; and in the third scenario, insurance is a means of transferring risk.

14. In these examples, individuals are attempting to reduce risk to an acceptable level, for example by attempting to minimise the likelihood of an undesirable or harmful outcome – an accident, an injury or a financial loss. Risk management can also result in individuals avoiding the risk entirely by not carrying out the activity, which implies they are also foregoing the benefit of the activity. In all cases, risk management

aims to optimise a decision making process related to an activity in order to increase the likelihood of achieving its expected benefits while reducing the possibility of undesirable outcomes.

15. While risk is a common and widely used term, it is a much more complex and nuanced concept than it appears at first glance.[7] There are many definitions of risk and the risk theory continues to evolve.[8] Following the OECD 2015 Recommendation on digital security risk management for economic and social prosperity, this paper will rely primarily on *ISO Standard 31000, Risk Management—Principles and Guidelines* that defines risk as the **"**effect of uncertainty on objectives" (see box 1), assuming that it represents the best consensus among experts. The Companion Document to the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity elaborates on the ISO definition to define risk as "the effect, or the consequences, of uncertainty on the objectives pursued by stakeholders, that is the deviation that reality can impose over what they anticipate."[9]

16. These definitions contain three important concepts: "uncertainty", "objectives" and "effect or consequences". Uncertainty is the lack of certainty regarding a potential event, e.g., a situation that may or may not occur or the consequences may be uncertain if it does occur. Uncertainty result from many factors, including: the actions of individuals, the weather, the spread of a disease or the life span of a machine. In many situations, the uncertainty is unmeasurable and uncontrollable; in other cases, uncertainty can be measured, for example, the probability that it will rain on any given day. Often, the degree of precision of such measurement varies, from very limited (e.g. low/medium/high) to very precise quantitative metrics.

17. Risk is a function of uncertainty. Without uncertainty there is no risk, but one can have uncertainty without risk. Many events are uncertain, but unless one has a stake or an interest in the outcome affected by the uncertainty, there is no risk. Risk is the consequence of uncertainty on outcomes or objectives that are valued.

18. An organisation's objectives can relate to a variety of goals – financial, environmental, social, product quality, etc. – and they can be organization-wide or they can be focussed on a specific activity such as a project, process or product. Consistent with the OECD's mandate, this paper focusses on the impact of risk on economic and social objectives.

19. Risk is about the consequences of uncertainty on the objectives, and it should not be confused with risk factors. Risk is caused by sources or "risk factors" that are often categorized as "threats", "vulnerabilities" and "incidents". Threats are typically external to the organisation; vulnerabilities are typically internal; and incidents result from their combination. Both threats and vulnerabilities are necessary to create consequences for an activity. Threats without vulnerabilities, or vulnerabilities without threats do not increase the risk. Although as discussed below, this threat/vulnerability/incident terminology, while common in the digital security risk space, is not always appropriate when discussing privacy risk.

Risk Management

20. Risk is common to all human enterprises, and in particular economic and social ones. Taking risk – investing in new products or services or expanding into new markets – is an inherent part of business ability to seize opportunities. Managing risk has become a widely accepted practice that is conducted by many types of organisations. The overarching purpose of risk management is to help organisations achieve their objectives Depending on the context and the nature of the organisation, these objectives may be expressed in legal, financial, social or other terms.

21. Risk management has become a well-established area of professional practice and academic interest. As a result, sophisticated tools, methodologies, standards and terminology have been developed to identify, measure and manage risk.

22. The 2009 publication of *ISO 31000 Risk Management—Principles and Guidelines* and an associated *ISO Guide 73 Risk Management Vocabulary* reflects the growing importance of risk management. ISO 31000 draws on previous work in the area to present a common vocabulary and a generic, widely accepted approach that can be used by a variety of organisations to address different types of risk. This standard defines a "risk management framework" as "a set of components that provide the foundations and organisational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation."[10]

23. Thus risk management involves using a coordinated set of activities and methods to identify, assess and treat the risk that an organisation faces. The overall objective is to facilitate decision making by taking into account the effect of uncertainty on the organisation's objectives and thereby increase the likelihood of success.

24. Risk management is a methodology or set of processes that involves a number of discrete steps or elements:

1. Assessing or establishing the context – this involves identifying the objectives of the activity, including its potential benefits, and looking at the values, laws, regulations, the culture, identifying stakeholders and their concerns and other factors that define what a successful achievement of the objective means and that could affect the risk management methodology. Some of these factors may be internal to the organisations such as the socio-economic objectives of the activity; other may be external.

2. Risk Assessment – this analytical step consists of three distinct tasks:

a) Identifying potential risk factors. This includes looking at risk sources such as the employees of a company, potential hazards in a workplace, or security vulnerabilities that can create or contribute to risk.

b) Analysing the risk factors. This typically involves taking into account the likelihood or probability that an event will occur. The likelihood of an event occurring can be described qualitatively – e.g. low, medium or high or it can be assigned a numeric value.

c) Evaluating the risk. This phase involves assessing the severity or magnitude of the estimated consequences of uncertainty (i.e. the possibility of events occurring) on the organisation's objectives.

3. Risk Treatment – determining the most appropriate way to respond to the risk. This decision making step could involve one or more of the following:

a) Accepting the risk.

b) Reducing the risk to an acceptable level by modifying the likelihood of the occurrence or the impact of the consequences of the event occurring while preserving the potential benefit of the activity. Risk can be reduced through a mixture of technical or organisational controls, innovation, i.e. designing the activity differently including its business model, and

preparedness measures (see below). This then requires determining whether the residual risk is acceptable given the potential benefits.

c) Sharing the risk or transferring it to another party.

d) Avoiding the risk by not carrying out the activity and thus forgoing the potential benefits.

25. The choice of risk treatment depends on several factors including the organisation's tolerance of risk, also called "risk appetite".

4. *Regular Monitoring and Review* of the context and the assessment and treatment of the risk. This is essential since most elements of the context are dynamic and to create a cycle of continuous improvement. It requires to examine issues such as:

a) are the organisation's objectives and expected benefits still the same,

b) has the context changed;

c) Has the risk level changed;

d) Have the risk treatment measures been effectively implemented;

e) Was the risk assessment accurate; and

f) Is the risk management framework operating as intended?

26. The environment is constantly changing: new threats are always emerging; markets, laws or regulations evolve; the benefits the organisation hopes to achieve and its risk appetite may change. Therefore, rather than a one-time activity, risk management is dynamic. It has to be an iterative process with the goal of fostering continuous improvement. Regular monitoring is required to assess the effectiveness of the methodology. Modifications may be required based on changes in the external environment, the emergence of new threats, the availability of new information, the emergence of more effective controls or other changes in the context or objectives of the organisation.

27. Documenting the risk management methodology is essential to establish a cycle of improvement and ensure accountability. Risk management should be interactive, incorporating effective and regular interaction and consultation with internal and external stakeholders.

28. A number of important interrelated principles or concepts flow from the discussion above:

- Risk management assumes that there is always some level of risk associated with carrying out an activity and, therefore, one has to accept a certain level of risk to carry out an activity. The only way to eliminate risk entirely is to not carry out the activity, i.e., forgoing the potential benefits. Failure to properly consider the benefit at the outset may lead to mitigation strategies that needlessly impair or limit the benefit.

- Risk is not a binary concept. Activities cannot be simply characterised as "risky" or "risk-free". Rather, the goal of risk management is to reduce the risk to a level that is acceptable in light of the potential benefits and taking context (i.e., values, mission, etc.) into account. This is the main difference between risk management and security, which would be best characterised as a state of risk avoidance, i.e., where risk has been entirely eliminated.

- One cannot determine the acceptable risk level in the abstract. It is always contextual.
- Risk management involves making decisions based on risk assessment. Risk assessment aims at understanding a situation in order to enable appropriate decision making. In other words, risk assessment is an analytical process that feeds risk treatment, which is a decision making process.
- Once reduced, the risk that remains is typically referred to as "residual risk" and this has to be evaluated to determine if it acceptable, highlighting the cyclical nature of the process. Since risk cannot be completely eliminated, the persistence of some residual risk means that undesirable events can occur despite the presence of risk reduction measures. This, in turn, suggests that organisations need to be prepared to deal with undesirable events (i.e., the "Preparedness and continuity" principle in the OECD Security Risk Recommendation) even after implementing risk treatment measures. Preparedness measures are essential to reduce the risk, i.e. the consequences of incidents, when they happen.

PRIVACY RISK AND PRIVACY RISK MANAGEMENT IN THE LITERATURE

29. This section provides an overview of some recent and current initiative to apply risk management concepts to the protection of privacy.

Recent Initiatives to Apply Risk Management Concepts to Privacy Protection

30. Organisations, particularly businesses, have to deal with many different types of risk, including operational risk, compliance risk, supply chain risk, reputation risk, credit risk, etc. As discussed above, all of these types of risk involve the possible effect of uncertainty on organisational objectives. Increasingly, organisations try to deal with risk holistically on a strategic enterprise-wide basis (sometimes called "Enterprise Risk Management") as opposed to a more traditional silo approach. Sophisticated risk management methodologies for these types of risk are well-developed.[11]

31. In contrast, the concept of privacy risk management is not well developed. It is even difficult to find a commonly accepted definition of privacy risk.[12] Privacy risk is rarely mentioned in traditional risk management literature and it is typically not seen as a critical aspect of enterprise risk management.

32. Thinking about privacy from a risk perspective is not new. For example, the Security Safeguards Principle in the OECD Guidelines, dating from 1980, refers to the need to protect personal data from the "risk" resulting from unauthorised access, destruction, use modification or disclosure of data. Breach notification laws, some of which have been in force for more than a decade are premised on the assumption that only data security breaches that pose a risk need to be reported. The European Union's Data Protection Directive 95/46/EC contain numerous references to risk. One of the purposes of privacy impact assessments (PIAs) is to encourage or require organisations to identify and assess the potential privacy risk of new or redesigned programs or services and assist in reducing the risk to an acceptable level. And "Privacy by Design" is essentially a proactive approach to reducing vulnerabilities at the technical design stage to minimise the possibility that privacy risk will arise in the first place.

33. With the possible exception of implementing the security safeguards principle – tailoring security safeguard based on risk assessment – privacy risk has been approached on a somewhat *ad hoc* basis and it has rarely been integrated into organisation's overall risk management strategies. However, an increasing

number of regulators, standards bodies and other organisations are now looking at ways to apply a more systematic risk management approach can be applied to data protection. Some of these initiatives are summarized below.

34. Dr Ann Cavoukian, when she was the Information and Privacy Commissioner of Ontario, was an early advocate of privacy risk management. A paper issued by her office in 2010 advocates "integrating Privacy by Design within an organisation's existing risk management process."[13]

35. The Centre for Information Policy Leadership is engaged in a multiyear project on the role of risk management in data protection. Building on the Centre's work on organisational accountability, the risk project is designed to help "bridge the gap between high-level privacy principles on the one hand, and compliance on the ground on the other".[14]

36. The U.S. National Institute of Standards and Technology (NIST) is engaged in an ongoing project to develop a privacy risk management framework for US federal information systems. NIST held two workshops in 2014 to explore the feasibility of developing a privacy risk management framework to further NIST's privacy engineering work and provide guidance to developers and designers of information systems that handle personal information. In May 2015, NIST published a draft privacy risk management framework.[15]

37. In 2012, the French Commission Nationale de l'Informatique et des Libertés (CNIL) issued two documents: a *Methodology for Privacy Risk Management*; and *Measures for Privacy Risk Treatment*.[16] These documents, primarily intended for use by controllers, data protection officers (DPO) and chief information security officers were developed to "assist them in creating a rational understanding of the risk arising from the processing of personal data and to choose necessary and sufficient organisational and technical measures to protect privacy." These were supplemented by three interrelated manuals for conducting PIAs published in 2015. The PIA Methodology manual sets out four steps when conducting a risk-based PIA: *i)* define and describe the context of the processing of personal data under consideration and its stakes; *ii)* identify existing or planned controls (to comply with legal requirements and to treat privacy risks in a proportionate manner); *iii)* assess privacy risks to ensure they are properly treated; and *iv)* make the decision to validate the manner in which it is planned to comply with privacy principles and treat the risks, or review the preceding steps.[17]

38. Nymity has published a White Paper on Privacy Risk Reporting Methodology that "introduces an approach for measuring privacy risk" intended to help organisations take a more quantitative, empirical approach to measuring external risk factors; integrate the operational elements of privacy risk; and align privacy risk with operational and compliance risk management.[18]

39. The Obama Administration's draft Consumer Privacy Bill Of Rights Act would require "covered entities" to conduct privacy risk analysis in certain situations and take reasonable steps to mitigate any identified privacy risk, which include, providing heightened transparency and individual control.

40. The Future of Privacy Forum has developed a data benefit analysis (DBA) tool to be used in conjunction with more traditional PIAs "to form a balanced, comprehensive view of big data risks and rewards."[19] The proposed DBA involves assessing variables such as the nature of the benefit, the identity of the beneficiary, the size or scope of the benefit and the likelihood of success. Taking into account the likelihood of success produces a "discounted benefit value" that can be weighed against privacy risks identified through a PIA.

A Focus on Minimising Privacy Harms

41. Although these initiatives demonstrate a growing interest in applying risk management ideas to the protection of privacy there are significant differences in their scope, and the rigour with which they draw on well-developed risk management methodologies. However, with the exception of the NIST initiative, they have one thing in common: they tend to see privacy risk management as a means of avoiding or minimising the impact of privacy harms, rather than as a means of managing uncertainty to help achieve specific objectives.

42. Focussing on harm is challenging because, unlike in other areas such as health and safety regulation where risk management is widely used, there is no general agreement on what constitutes a privacy harm or how to categorize privacy harms, i.e., on the outcomes one is trying to avoid.

43. There are any numbers of ways to categorize privacy harms and this, in large part, is a function of the many different ways that one can define privacy. Daniel Solove has perhaps gone further than other academics in creating a detailed taxonomy of harms. His taxonomy is an attempt "to shift focus away from the vague term 'privacy' and toward the specific activities that pose privacy problems."[20] It includes four basic categories of harmful activities – information collection, information processing, information dissemination and invasion – further subdivided into 16 subcategories.

44. Solove refers to these as "harmful activities." Understanding "threat" on the basis of its definition by ISO – "a potential cause of an unwanted incident, which may result in harm to a system or organisation" – some of these activities could perhaps be more accurately characterised as threats. For example, some of his subcategories of harmful activities such as surveillance, identification and disclosure may cause harm but they can also be benign.

45. NIST has identified four "problems" that can result from problematic data actions:

1. Loss of self-determination, including loss of autonomy, exclusion, loss of liberty;

2. Discrimination, including the harms of stigmatisation and power imbalance;

3. Loss of trust – the breach of implicit or explicit expectations or agreements about the handling of personal information; and

4. Economic loss – direct financial losses as well as the failure to receive fair value in a transaction involving personal information.[21]

46. The Centre for Information Policy Leadership's (CIPL) 2014 paper, "A Risk-Based Approach to Privacy: Improving Effectiveness in Practice", categorises possible "harms" under three headings: "tangible damage to individuals, intangible distress to individuals, and societal harm".[22] Tangible damage includes bodily harm, loss of liberty or freedom of movement and financial damage. Intangible distress includes a chilling effect on freedom of speech, reputational harm, unacceptable intrusion into personal life and discrimination or stigmatisation. CIPL cites damage to democratic institutions and loss of social trust as example of social harm.

47. The CNIL's Methodology paper uses the term damage rather than harm. It suggests that damage to data subjects may be physical, material or moral.

48. The Obama Administration's draft Consumer Privacy Bill Of Rights Act defines "Privacy risk" as "the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional or other harm to an individual."[23]

49. Nymity's White Paper makes the important point that while the impact of harms such as damage to an organisation's brand or an increase in costs "can be translated into dollar values, and is generally congruent across industries and geographies"

> "Harm to an individual, however, is much more difficult to articulate, let alone measure. Harm to individuals must be considered in the context of cultural values and attitudes; what is considered harmful in one culture may be considered desirable in another[24]."

50. The Article 29 Working Party in its "Statement on the role of a risk-based approach in data protection legal frameworks" suggests that such an approach must go beyond a narrow "harm-based-approach". The Working Party believes that a risk-based approach "should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)."[25]

51. Thus there is no consensus or a clear understanding of the harms, or a definition of risk, being addressed. However, the OECD has suggested in the supplementary explanatory memorandum to the revised Privacy Guidelines that "Risk is intended to be a broad concept, taking into account a wide range of possible harms to individuals".[26]

APPLYING RISK MANAGEMENT TO PRIVACY

Objectives

52. Risk management is a process by which activites in which organisations wish to engage are evaluated to ensure that possible risks have been addressed to an extent that makes them acceptable within the risk tolerance of the organisation in light of the potential benefit. The purpose of risk management is to help an organisation respond to, and make decisions about, the effect of uncertainty on the organisation's objectives in order to increase the likelihood of success. How does this translate to the protection of privacy?

53. First of all, there is the question of the organisation's objectives. An organisation can have several different objectives. Some of these objectives may be complementary; others may require some degree of balancing or optimisation, for example some economic objectives may, at times be at odds with social objectives. Simply stating that the objective of privacy risk management is or should be the protection of privacy is not very helpful since privacy is a notoriously difficult concept to define and privacy can mean different things to different people in different situations.

54. Organisations process – i.e., collect and use – personal information to achieve a variety of objectives. Some of these objectives may primarily benefit the organisation; others may also benefit society at large or the individuals who buy or use products or services. Processing personal data may create legal, financial, reputational or other risk for data controllers; it can also create risk for individuals and for society at large. Applying risk management to privacy protection involves taking all of these benefits and forms of risk into account.

55. One possible way to move forward is to focus on the objectives of privacy risk management, i.e., shift the focus away from avoiding harms to social and economic objectives as the OECD has done with

the Digital Security Risk Recommendation and consider the ability to use data productively while providing appropriate privacy protection as a measure of success.

56. The ongoing NIST project has identified three privacy engineering objectives:

- Predictability – enabling reliable assumptions about the rationale for the collection of personal information and other data actions to be taken with that personal information;
- Manageability – providing the capability for authorized modification of personal information, including alteration, deletion, or selective disclosure of personal information; and
- Disassociability – enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.[27]

57. These objectives, which mirror the well-established data security objectives of confidentiality, integrity and availability, are a promising start although they have a clear engineering perspective as opposed to a broader, organisation-wide perspective. They also address uncertainty, the other key term in the definition of risk management. For example, as NIST points out,

> "… predictability is about designing systems such that stakeholders are not surprised by the handling of personal information. … Thus, predictability facilitates the maintenance of stable, trusted relationships between information systems and individuals and the capability for individuals' self-determination, while enabling operators to continue to innovate and provide better services.[28]"

Risk Management and the OECD Privacy Guidelines

58. Although the concept of risk management was not well developed when the Privacy Guidelines were published in 1980, one can see the basis of a risk management approach to privacy protection in them. The preamble to the Recommendation of the Council concerning the 2013 revised Guidelines recognises that "more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks". By creating obligations for data controllers and giving individuals rights, the Guidelines create a framework that allows individuals to manage the uncertainty about how their personal data would be used.

59. For example, the purpose specification principle, together with the openness principle, is intended to provide individuals with sufficient information to allow them to make informed risk management decisions about whether to enter in a relationship and provide personal data based on a specified purpose. The use limitation principle is intended to limit uncertainty by restricting how the data can be used. Changing the purpose may introduce uncertainty; if so, the individual should then be able to make another risk assessment and treatment decision. The right of access provides an additional mechanism to assess and manage risk.

60. Daniel Solove has referred to this approach to privacy regulation as "privacy self-management".[29] He argues that it is being tasked with doing work beyond its capabilities. It expects too much of individuals and it does not provide people with meaningful control over their data.

61. Solove identifies three problems with informational self-management: first, there are severe cognitive problems that impair individuals' ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data; second, even well-informed and rational individuals cannot appropriately self-manage their privacy because there are too many entities collecting and using personal data making it difficult for people to weigh the costs and

benefits of revealing information or permitting its use; and finally, privacy self-management addresses privacy in a series of isolated transactions rather than assessing the costs and benefits cumulatively and holistically and these individual decisions might not collectively yield the most desirable social outcome.

62. Solove goes on to note that privacy does more than just protect individuals.

> "It fosters a certain kind of society, since people's decisions about their own privacy affect society, not just themselves. Because individual decisions to consent to data collection, use, or disclosure might not collectively yield the most desirable social outcome, privacy self-management often fails to address these larger social values.[30]"

63. Expecting individuals to manage their own risk assumes that they have sufficient and accurate information to assess risk and the expertise and ability to evaluate and treat the risk. However, organisations may not have sufficient incentive to provide individual with adequate or complete information about the possible risk of processing personal data. On the contrary, they may have an incentive to underestimate the risk or they may have an incentive to provide incomplete information about the risk. Thus, the values and interests of the organisation may not be fully aligned with those whose personal data are processed.

> "A key issue for privacy protection is this possible misalignment of the data controller's interests with those of the data subject. More generally, the fact that the party carrying out the risk assessment (the data controller) is not the one facing the risk (the data subject) is a major difference between security and privacy risk assessment.[31]"

Rationales for Regulation

64. This possible misalignment between the interests of the organisation and interests of the public and their respective views of the risk of an activity is not unique to privacy protection. Traditional free market economics assumes that buyers or users have sufficient information to act in their own interest and make rational decisions about the products or services they purchase. However, this is often not the case; the "market" does not always provide individuals with adequate or complete information.

65. One of the rationales for government regulation is to correct market failures, including the failure caused by imperfect information or information asymmetry, i.e., the seller has more information than the buyer. Governments also regulate to achieve specific social objectives, for example, to ensure that all individuals are treated fairly by prohibiting certain types of discrimination. Governments can intervene in many ways, for example, by prohibiting specific activities, by attempting to ensure a product is sufficiently safe (minimising the risk) or by forcing the organisation to provide sufficient information to help the individual assess the risk for themselves.

66. Arguably, market failure also exists with respect to data protection. Individuals may not have adequate information about how their personal data are being used or if it is being adequately protected to allow them to make rational decisions about privacy protection. Organisations have typically not competed on the basis of data protection. As well, there may be a failure on the demand side. As a result, individuals are often faced with the binary choice of consenting to practices that may not meet their expectations or abandoning their use of a service.

67. Although it is not typically discussed in these terms, privacy regulation can be viewed as a means to correct these market failures and by doing so achieve a variety of social and economic objectives. Data protection legislation can address privacy risk, for example, by prohibiting some uses of personal information that are deemed unacceptable and, more generally, by creating a safer space for individuals to engage in activities free from undue scrutiny by the State or organisations. As well, data protection

legislation can help achieve broad economic objectives by facilitating the free flow of personal data that feeds the modern economy while ensuring that individuals can have confidence that their personal data will not be misused.

68. From a privacy risk management perspective, data protection laws can empower individuals by requiring organisations to provide them with information about how their data will be used and by doing so this reduces the uncertainty for individuals. However, legislation will only achieve these objectives if it establishes clear regulatory obligations and creates meaningful legal, financial and reputational risk if organisations fail to meet their obligations. Effective legislation forces the organisation to take privacy seriously and acknowledge the risk flowing from the processing of personal data.

69. While privacy laws create some certainty for organisations and for individuals, they have been criticised for creating a one-size-fits-all approach to privacy protection that focusses on compliance rather than the protection of privacy. Focussing on compliance reduces the risk of enforcement actions, fines and adverse publicity, but it does not necessarily lead to greater protection of privacy, nor does it always contribute to realizing the economic and social benefits that can result from the use of personal data. This suggests that there is a need to do more systematic analyses of privacy regulation to see if it accomplishes its goals of enhancing protection for individuals while allowing uses that meet the needs of a data-driven economy.

Privacy Risk

70. As discussed above, risk is typically caused by some combination of threats, vulnerabilities and incidents – rogue employees, inappropriate security controls, inadequate training, skilled attackers, a natural disaster or some other uncertainty. For example, a hacker or a competitor may be able to gain access to a company's confidential information. Or a company's costs may be affected by abnormal weather conditions that affect supply costs.

71. Like other forms of risk, privacy risk can be caused by rogue employees, poor training or some other threat, vulnerability or incident. A careless employee can disclose personal information by using "reply all" to send an e-mail; a manager can create a risk by not conducting appropriate due diligence when hiring a contractor to shred documents; or a decision to save money by delaying the installation of a network patch can contribute to a data breach.

72. However, privacy risk is not necessarily caused by a system failure, an external threat or an unexpected incident. Privacy risk can be caused by an organisation consciously deciding to use personal data to meet organisational objectives, for example, to profile its customers or to offer new services. As a result, as the NIST Privacy Engineering Objectives and Risk Model Discussion Draft notes, the terminology of security "threats" and "vulnerabilities" may not be appropriate for assessing privacy risk.[32] NIST has proposed the term "problematic data actions" to describe activities that potentially cause privacy harms.

73. In many situations, the determination of the acceptable level of risk is typically carried out by the organisation that faces the risk. The amount of risk that the organisation or individual is willing to accept, (when engaging in a certain activity) is referred to as the organisation's risk appetite. When a business conducts risk management analysis, it may consider the impact on other stakeholders, including its customers, but it is primarily interested in the risk to the company. Effective regulation forces an organisation to consider the interests of other stakeholders.

74. This misalignment of the data controller's interests with the interests of the data subject can also be a function of differences in the way risk and benefits are perceived and valued. Risk perception is the

subjective judgment people make about the severity and/or probability of a risk. Perception of risk often varies from person to person and individuals' perception of risk may differ significantly from expert opinion.

75. The concept of risk perception is particularly relevant with respect to the risk of natural hazards and when discussing food safety or environmental hazards. Individuals may have widely differing views about the risk posed by vaccines, genetically modified organisms and wind turbines, to use some topical examples. And these views may differ from the views of experts.

76. Risk perception is also relevant in the context of privacy risk management. Individuals may have varying views on the privacy risk associated with using social networks and these may differ from the risk identified by regulators and other experts.[33] Or, as the Companion Document to the OECD Security Risk Recommendation observes, "many people are aware that they can be infected by a virus, but do not necessarily understand the potential consequences such as identity theft, financial fraud or theft of trade secret."[34] As well, individuals may have limited ability to act if they do not have sufficient information to assess the risk because of a lack of transparency in the marketplace or if the absence of effective competition limits their ability to choose a more privacy protective product or service.

Risk communication

77. One of the challenges in risk management is managing the inherent tension that exists between differing views of risk. One of the goals of risk communication is to bridge this gap between these differing views, including the gap that may exist between expert opinion and public perception. Risk communication is not about persuading individuals that there is no risk or that their perception of risk is wrong. Good risk communication is a two-way process that involves engaging with the public, recognising individuals' right to be heard and providing them with the information to make informed decisions or in some cases to participate more fully in public policy making. Poor risk communication can erode trust, undermine goodwill and contribute to poor decision-making.

78. Laws and regulations can mandate risk communication. For example, drug manufacturers are required in many countries to provide detailed descriptions of the risk of adverse reactions when marketing their drugs in an attempt to correct the information asymmetry discussed above.

79. Nutrition labelling can be viewed as a means of risk communication – one of its purposes is to help individual assess the risk and benefits in eating foods by providing them with information about possible risk sources – fat, sugar, sodium, etc. – as well as information about the nutrients in the food.

80. Privacy risk communication is a concept that has received relatively little attention. In some respects, it is closely related to the Openness principle in the Guidelines – the expectation that organisations will be open about their practices and policies with respect to personal data. Short notices, based on the nutritional labelling model and "multi-layered privacy notices", simplified notices providing basic information supplemented by more complete privacy statements, are basic forms of risk communications. Privacy icons are also being used to convey information about privacy practices and some regulators have introduced or are considering privacy seal programs – a "stamp of approval" for an organisation's privacy practices.

81. Privacy impact assessments (PIAs), which were modelled on environmental impact assessments, have the potential to be an effective privacy risk communication tool. PIAs are designed to encourage or require organisations to identify and assess in a systematic way the potential privacy risk of new or redesigned programs or services and assist in eliminating or reducing the risk to an acceptable level. They can also be an effective way to communicate privacy risk both internally and externally.

82. To the extent that privacy risk communication does occur, for example, through PIAs, it tends to focus on the potential harms flowing from the processing of personal data and ways to mitigate these harms without taking the potential benefits into account.[35]

Treating Privacy Risk

83. As discussed above, on the basis of risk assessment, organisations can respond to risk in four different ways:

- Avoiding the risk, for example by not taking on a project and thus forgoing the potential benefits;
- Reducing the risk to an acceptable level by modifying the likelihood of the occurrence or the impact of the consequences of the event occurring while preserving the benefit, for example by designing the activity differently or by changing the business model.
- Sharing the risk or transferring the risk to another party, for example through a joint venture or by taking out insurance; or
- Accepting the risk.

84. In many situations, the choice of a treatment strategy and the determination of an "acceptable level of risk" are made by the entity that carries out the activity and faces the risk. The amount of risk that an entity is willing to accept to undertake an activity is known as its "risk appetite". An organisation's risk appetite depends on many factors and in some cases, it can be limited by the legal and regulatory context. However, in the case of privacy risk management, the data controller may have a greater "risk appetite" than the data subject or there may be significant differences in terms of risk perception.

85. Privacy risk can be avoided by not collecting personal information when it is not necessary or by not launching a service that involves sharing personal data with third parties. However, it is not possible to eliminate risk entirely without eliminating the benefits. (If personal data are being collected that is not needed to achieve a given objective then there is no economic cost in eliminating the risk.) The likelihood of a privacy risk occurring can be reduced by addressing the risk factors. Limiting retention periods for personal data, improving physical, technical and organisational security measures, enhanced training of staff, audit mechanisms to detect unauthorized access and privacy impact assessments are some of the controls that can be used to reduce risk.

86. The impact of a privacy incident can be reduced by measures such as the use of encryption, anonymisation, pseudonymisation and the aggregation of data to reduce the risk of identity theft or other harms if personal data are lost or inappropriately accessed. Risk management is continuous. It is not enough to implement these measures and assume the risk has been mitigated; further risk assessment should consider the possible consequences to the data subject, for example in the event that re-identification occurs.

87. Sharing or transferring risk is a useful strategy in some circumstances. Data breach insurance is becoming an increasingly common method for organisations to minimise their financial risk. Data breach insurance transfers the liability to the insurer but it does not necessarily reduce the non-financial risk to the organisation or the privacy risk to the data subjects. However, the level of premiums charged will depend on risk and market forces may provide an incentive for organisations seeking insurance to reduce their risk. Similarly, outsourcing may reduce risk for the organisation but not for the data subject. As paragraph 16 of the OECD Guidelines states that "A data controller remains accountable for personal data under its control without regard to the location of the data." This includes situations where a third party is processing data

on the behalf of the data controller. Accountability cannot be outsourced. In fact, organisations considering outsourcing should conduct due diligence and should review the privacy practices of the third party as part of its risk management program.

88. Although the primary responsibility for treating privacy risk should reside with the data controller, individuals can and do take steps to respond to perceived privacy risk. Some individuals carefully limit their digital footprint, for example by not participating in social networking service, by restricting the amount of personal data information they post online; or they may make use of pseudonyms where possible. Some individuals make use of privacy enhancing technologies.

89. As well, organisations can provide tools, either voluntarily or as required by legislation, to help individuals exercise their privacy rights. Access and correction, data portability, withdrawing consent, the right of erasure and "the Right to be Forgotten" are some of the tools that individual can use to try to limit the possible harms that can result from the misuse of their personal data.

UNDERSTANDING PRIVACY RISK MANAGEMENT

Defining Privacy Risk

90. The concept of "privacy risk" as it is typically used in most discussions of privacy risk management is inconsistent with the concept of risk used in other areas and introduced in the first section of this paper. It is generally not based on the management of uncertainty. Privacy is often viewed as a binary state – an activity is risky or it is risk-free – rather than as a continuum. There is a spectrum of risk and a range of measures to mitigate the risk.

91. If we define risk as "the effect of uncertainties on objectives" how can we define "privacy risk"? Drawing on the OECD's definition of digital security risk[36], one could potentially define "privacy risk" as a type of risk related to the processing of personal data. Like digital security risk, privacy risk can result from the combination of threats and vulnerabilities in the digital environment, but it can also result from a deliberate action taken by an organisation, what NIST refers to as "problematic data actions". For example, an organisation may decide to make a change its privacy policies in order to achieve certain objectives, but this change could create uncertainty with respect to privacy, and thus risk, for the users of the service. Or a government could pass a law or take some other action to make it easier to obtain personal data held by businesses, creating privacy uncertainty for individuals and for the businesses holding the personal data.

92. Like digital security risk, privacy risk is dynamic in nature. The sources of risk are constantly evolving and they can be intentional or unintentional and they can result from human actions, technology or even from natural events.

93. The possible effects or consequences of privacy digital uncertainty can be expressed in economic and social terms: financial loss, loss of competitiveness, loss of opportunity, stigmatization, damage to reputation, image or trust, a chilling effect on speech or freedom of association, etc.

94. Privacy risk is often viewed as different from other forms of risk because it relates to harm to individuals. However, other forms of risk such as occupational safety risk and food safety risk also relate to individuals. As discussed above, in those situations where the risk is not borne solely or perhaps even primarily by the organisation assessing the risk there is a possible misalignment of interests. Organisations may tend to underestimate privacy risk, just as they may tend to underestimate health and safety risk.

95. Effective privacy regulation is one way to correct this misalignment. If they are significant and predictable, fines and other forms of sanctions can create financial, legal and reputational risk for organisations processing personal data, and help ensure that privacy risk management is given the same weight and importance as other categories of risk. Following this idea, the aim of the risk based approach would be to increase the business importance of privacy risk management in organisation economic and social decision making, as it is typically the case for digital security risk management. In other words, privacy risk management should be addressed as part of the broader economic risk management framework of organisations and be integrated in economic decision making rather than solely as a technical issue of a legal nature.

Managing Risk and Benefits

96. The assessment and treatment of risk are distinct risk management steps. Risk assessment is an analytical process; risk treatment is decision making process.

97. In deciding how to treat risk, organisations take into account the social and economic objectives they are pursuing. The goal should be to reduce the risk to an acceptable level, relative to the anticipated economic and social benefits, while taking into account the potential impact on the interests of others. While an organisation may face financial risk, reputation risk or legal and regulatory risk as a result of the processing of personal data, the risk to the organisation needs to be clearly distinguished from the risk to the individual and the risk to society.

98. Balancing risk and benefits and determining the acceptable level of risk becomes far more complex when the benefits flow to the organisation or to society at large rather than primarily to the individuals whose personal data are being used. In a data driven society, personal data can be used for any number of worthwhile social objectives: to improve health care; to facilitate the efficient movement of people; to respond to disasters; or to identify individuals at risk. In those situations where the interests and values of those who establish, use and benefit from the personal data may not be fully aligned with those whose personal data are processed, some mechanisms or processes are needed to reconcile conflicting interests.

99. In some areas, governments and regulators are responsible for reconciling conflicting interests. For example, government agencies and regulators use risk management techniques when regulating pharmaceutical products, the use of pesticides and other contaminants and the production of food in an attempt to achieve widely shared social objectives – safer and more effective drugs, a healthier environment and food safety. Governments regulate the introduction of new drugs by analysing and weighing both the safety of the drug – the possible harm that can result – and the efficacy or benefits that the drug provides, as well as the economic interests at stake. However, it is not clear that data protection regulators have the specialized expertise to perform a similar role with respect to balancing privacy risk and the social and economic benefits that can result from using personal data.

POTENTIAL BENEFITS OF A PRIVACY RISK MANAGEMENT APPROACH

100. A risk management approach to privacy has several potential benefits. It can:

- Improve privacy protection for individuals while fostering social and economic benefits;
- Help data controllers develop and implement effective privacy management programmes as a means of fulfilling their accountability obligations;
- Contribute to greater compliance by helping organisations understand the risk and determine where and how to use their resources; and
- Contribute to global interoperability.

Improving Protection for Individuals while Fostering Social and Economic Benefits

101. Risk management is intended to help organisations achieve their objective by reducing uncertainty. Organisations process personal information to achieve a variety of objectives. Some of these objectives may primarily benefit the organisation by increasing market share or revenues. Individuals benefit from lower prices, improved quality and the introduction of innovative products and services. Society as a whole benefits from improved health care, more efficient transportation systems and more effective social programs.

102. Processing personal data may create legal, financial, reputational or other risk for data controllers. As well, as the OECD has noted, it can also create risk for individuals and for society at large:

> "The dramatic opportunities enabled by changes in technologies and global flows have also raised new challenges and concerns for individuals, organisations, and society with respect to the protection of privacy. … These changes, along with the evolving role of individuals and the increasing economic value of personal data, give rise to concerns related to the security of personal data, unanticipated uses, monitoring and trust. The result is a privacy environment that is challenging for organisations and individuals to navigate.[37]"

103. Privacy risk is a function of uncertainty. Organisations may be uncertain about how privacy laws will be applied, they may be uncertain about regulators or their customers will respond to new initiatives involving the processing or personal data or they may be uncertain about how to respond to security threats. For individuals, this uncertainty may be the result of concerns about how their personal data are being used or whether it is being adequately protected.

104. A risk management approach has the potential to help organisation achieve their objectives and to improve protection for individual if it helps organisations assess the privacy risk of new products, services and other activities and allows them to calibrate their policies and practices accordingly. Risk management can also help organisations weigh the risk and benefits of specific projects.[38]

105. Risk management can also break the market failure problem by providing organisations with the incentives and the means to improve privacy protection and make privacy a market differentiator, i.e., a factor on which business competes.

106. Effective communication of risk can help individuals better understand the risk they face when using services or when an incident occurs. For example, one of the rationales for introducing data breach notification schemes is to inform individuals of possible risk so they are empowered to take actions to help protect themselves.

Scaling Accountability

107. The revised OECD Privacy Guidelines recommend that data controllers should introduce tailored privacy management programmes based on the structure, scale, volume and sensitivity of their operations as a means of implementing the Accountability Principle. They include a new Part Three that elaborates on the concept of accountability and articulates its key elements. The revised Guidelines reflect the growing interest in accountability.

108. The concept of accountability is not new. It was in the original OECD Guidelines issued in 1980 and it can be found in national laws such as Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA). But like the concept of privacy risk management, accountability is now receiving increased attention from regulators, academics and policy makers.

109. In the context of data protection, accountability has at least two elements: putting into place effective mechanisms and procedures to give effect to the organisation's policies and obligations; and accepting responsibility, i.e., being answerable to regulators and other stakeholders for complying.[39] In the words of the Article 29 Working Party, accountability is a way to move data protection from "theory to practice".

110. In moving from theory to practice, organisations have to tailor their privacy management programmes to their specific circumstances, "A one-size-fits-all approach would only force data controllers into structures that are unfitting and ultimately fail."[40] Organisations need to take into account factors such as the type of data, the size of the data processing operation, the intended purposes of the processing and the number of envisaged data transfers.

111. Privacy risk management can help organisations tailor their policies and practices to ensure that they reflect the risk to both the organisation and the individuals whose information is being processed:

> "Implementation of controllers' obligations through accountability tools and measures (e.g. impact assessment, data protection by design, data breach notification, security measures, certifications) can and should be varied according to the type of processing and the privacy risks for data subjects. There should be recognition that not every accountability obligation is necessary in every case – for example where processing is small-scale, simple and low-risk.[41]"

112. Regular risk assessment can also help organisations adjust their privacy management programmes to reflect evolving risk and other changes in context and help ensure that their programmes are effective. Risk assessment features prominently in the accountability guidance developed by Canadian privacy commissioners:

> "Organisations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments. Organisations should develop procedures for conducting such assessments, and develop a review and approval process that involves the Privacy Officer/Office when designing new initiatives, services or programs.[42]"

Privacy Risk and Compliance

113. One of the challenges for organisations when trying to comply with privacy laws and regulations is translating legal and policy requirements into language that engineers and product developers can understand when designing and developing products and services. One of the goals of the NIST privacy engineering project is to develop outcome-based objectives that can guide design requirements.

> "There is a communication gap around privacy between the legal and policy, design and engineering, and product and project management teams that increases the difficulty for organisations to manage privacy concerns effectively, understand risk and implement mitigating controls before harm occurs. A contributing factor is the lack of a common vocabulary and set of tools that can be used to build consistent requirements and technical standards across organisations.[43]"

114. Assessing risk can help organisations comply more effectively with the obligations set out in basic principles such as collection limitation, data quality and security safeguards by forcing them to consider the sensitivity and the quality of the personal data they are using, whether collecting it is necessary and the safeguards needed to protect it. Assessing risk is also an essential element of PIAs and Privacy by Design, important accountability and compliance mechanisms.

115. Assessing and responding to risk can help organisations move beyond mere compliance with legal requirements and assist in integrating the protection of personal data into their enterprise-wide risk management methodology.

116. Risk management helps organisations understand the effect of uncertainty on their objectives, weigh the risk against the associated benefits and make choices about what actions, if any, to take in order to achieve business objectives. Risk management allows organisations to assign priorities. Risk management cannot eliminate all risk; rather it is a means to help organisations decide which risk is the most pressing and what actions to take to minimise it.

117. A risk management approach to privacy helps organisations assess the privacy risk associated with introducing new products or service, contracting out services, using personal data for a new purpose or installing new information systems. The CNIL's Methodology paper suggests that "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."[44]

118. Regulators can also make use of risk assessment to prioritise action. In a speech to the 35th International Conference of Data Protection and Privacy Commissioners, Chantal Bernier, the then Assistant Privacy Commissioner of Canada, explained that the Office of the Privacy Commissioner of Canada assesses the severity of data breaches on a scale from negligible to severe risk and uses this assessment to calibrate the Office's response.[45] She then went on to highlight three benefits of such an approach:

- A clear risk assessment framework grounds the Office's analysis in a way that ensures an approach that is both consistent and adaptable in the face of fast paced change;
- It allows the Office to transparently calibrate its compliance action to respond to an unprecedented diversity of privacy risk; and
- This calibration of compliance action has allowed the Office to be more efficient and strategic.

119. However, it is important to recognise that privacy regulators will use risk methodologies in a more limited way. In terms of risk to data subjects, regulators will typically focus on the risk assessment phase, leaving data controllers to establish the context, treat the risk and engage in ongoing monitoring and review. Like any organisation, regulators may make use of risk management strategies for internal governance purposes.

Contributing to Global Interoperability

120. Two interrelated themes are reflected in the revised OECD Privacy Guidelines: a focus on a risk management to enhance the practical implementation of effective privacy protection; and promoting greater interoperability of privacy frameworks to enhance privacy protection on a global level. Paragraph 21 of the revised Guidelines urges member countries to "encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines."

121. The Supplementary Explanatory Memorandum goes on to note some of the benefits of improved interoperability:

> "Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by

organisations and ensure that privacy requirements are maintained. It can also enhance individuals' awareness and understanding of their rights in a global environment.[46]"

122. As the OECD suggests, improving global interoperability is challenging. There are significant differences among national privacy and data protection laws. Some laws are based on the premise that privacy is a fundamental human right; other laws are more consumer-protection oriented; some jurisdictions have broad comprehensive laws while others rely on sector specific laws. There are even fundamental differences around basic concepts such as what constitutes personal data.

129. One potential way to overcome these differences is to develop a "high-level, overarching legal framework that provides overall rules for data governance", an approach that Christopher Kuner refers to as "constitutionalism".[47] However, as Kuner and others have noted, there are a number of difficulties involved in developing, reaching agreement on, and implementing an international treaty, convention or other high-level legal instrument to govern personal data.

123. Interoperability, a term which refers to "the ability of diverse systems and organizations to work together"[48] recognizes these differences. A risk management approach to privacy has the potential to bridge these differences. While the context – the laws, the regulations, the cultural values, etc. -- in which organisations operate may vary across the globe, many of the uncertainties and organisational objectives are the same. Global organisations are able to use risk management processes and methodologies to comply with diverse regulatory requirements and different social and cultural values in other areas such as food production, medical devices and pharmaceuticals.

124. A risk management approach to privacy protection can likewise contribute to global interoperability and enhanced privacy protection if stakeholders take a more rigorous approach to privacy risk management, including integrating privacy risk management into their organisation-wide risk management methodologies. Realising this potential will require developing and using a common vocabulary, some consensus around concepts such as privacy risk, the values that a risk management approach is trying to achieve and some common metrics or measuring mechanisms to assess privacy risk.

CONCLUSIONS

125. This paper has identified several areas where privacy risk management can benefit organisations and other stakeholders:

- Enhancing privacy protection while contributing to the achievement of social and economic objectives;
- Helping organisations develop and implement effective privacy management programmes as a means of fulfilling their accountability obligations;
- Allowing organisations to make objective decisions about risk and how to respond to minimise the risk; and
- Contributing to global interoperability by helping bridge the differences between national and regional data protection and privacy laws.

126. A privacy risk management approach holds promise for enhancing privacy protection while contributing to economic prosperity but it should not be seen as a magic bullet that can solve all of our privacy challenges. Focussing on risk should not detract from thinking about other challenges that are exacerbated by a data-driven society. There is a need to focus on ways to improve transparency so individuals have a better understanding of how their personal data are being used; to think about innovative ways to empower individuals and to think of creative ways to monitor the use of personal data by organisations to ensure this is being done responsibly in line with individuals' values and expectations.

127. Effective privacy risk management can create value for an organisation by building consumer trust and protecting its corporate image. It can assist the organisation in making choices about its use of personal information and its information practices. Poorly executed risk management can erode trust and expose organisations to legal risk.

128. Like any form of risk management, privacy risk management should be based on good information and reflect stakeholder concerns and interests; it should be scalable and it should take human and cultural factors into account and it should be responsive to change.

129. From an organisational perspective, it should become part of economic decision making wherever the economic activity relies on the processing of personal data. Privacy risk management should become part of the broader risk management framework of organisations, which implies that it is not only seen as a legal risk calling for legal measures, but also as a business risk directly affecting the organisation's reputation, revenues, and trust in the marketplace, i.e., among customers, shareholders, employees, and other stakeholders. This would require significant internal support including buy-in at the highest level of the organisation and clear lines of responsibility.

130. The integration of privacy risk management into economic decision making and broader business risk management frameworks could also make it easier for organisations to approach privacy protection as an opportunity, for example by using it as a differentiator on the marketplace.

131. Thus it could be useful to approach public policies for privacy protection also from the perspective of how they can increase the strategic importance of privacy risk to organisations, and address the current market failure whereby privacy protection is not a sufficiently effective differentiator in the market place.

132. Privacy risk management is contextual. As a first step, organisations should assess the context in which they are operating, taking into account relevant laws, regulations, technology trends and cultural considerations, identifying stakeholders and their concerns and other factors such as the political environment that could affect the risk management methodology. In considering privacy risk, organisations should also take into account factors such as the types and sensitivity of the personal data being processed; the purpose of the processing; the relationship between the organisation and the individuals whose personal data are being used; and the level of understanding that reasonable individuals would have of the processing

133. Privacy risk management involves analysing the risk in light of the context and the anticipated benefits and making decisions about controls needed to protect the individuals' interest while at the same time recognising that this may impact the economic and social benefits that can be achieved.

134. Privacy risk management should not be viewed as "an alternative to well-established data protection rights and principles."[49] A risk management approach should not be used to dilute privacy rights. Used effectively it can strengthen rights by making individuals more aware of privacy risk. It can also make privacy protection more effective by helping organisations understand the privacy risk they may

be creating and by helping them make decisions about minimising the risk. Finally, it can help organisations comply more effectively with their obligations set out in basic principles such as collection limitation, data quality and security safeguards.

135. Applying a more rigorous, risk management methodology to privacy protection has great promise. Realizing this potential will involve addressing several challenges, some of which are discussed below.

136. First, we need a more precise vocabulary and greater clarity around concepts – risk, threats, vulnerabilities, "problematic data actions", damage, harm, etc. – and to distinguish clearly between risk factors, privacy risk and privacy harms. Identifying the risk factors – the causes – is necessary in order to manage the consequences – privacy risk. Existing glossaries such as those developed by ISO, the CNIL and NIST provide a promising starting point.

137. Second, we need to reach general agreement about what we mean when we refer to privacy harms – what we are trying to avoid. As discussed above, we do not yet have agreement on, or a clear understanding of, the harms, or the risk, we are trying to avoid. Although a case can be made that we should define privacy harms broadly, it may be helpful to limit the scope of the concept and clearly distinguish between the risk of harm and the harm itself. As Ryan Calo has argued, "A risk of privacy harm is no more a privacy harm than a chance of a burn is a burn. They are conceptually distinct: one is the thing itself, the other the likelihood of that thing."[50] Calo also makes the useful suggestion that we should uncouple privacy harms from privacy violations and recognise that not all privacy violations cause harm and that privacy harms can occur in the absence of a privacy violation.

138. Third, we need tools to assess *both* the risk and benefits. Eliminating risk entirely is rarely possible and in many cases it may be socially undesirable if it unduly interferes with important social or economic benefits. While the privacy risk flowing from the processing of personal data may be borne primarily by the individuals whose data are being used, the benefits may flow to the organisation, society or the individuals in question. Developing mechanisms to identify and reconcile these potentially conflicting interests is critical. Is this a role for regulators, for legislators, multi-stakeholder committees or do we need to develop new mechanisms such as some variant on existing bodies that assess institutional research involving humans?

139. Finally, there is the issue of the extent to which organisations should be expected to communicate privacy risk to individuals and how this relates to openness and transparency obligations. Risk communication is an integral part of risk management in many areas where the risk may be borne by the public. As noted above, pharmaceutical companies are explicitly required to identify the risk associated with drugs both when advertising their products and in product monographs and package inserts. Nutrition labels are a simple form of risk communication. In addition, other regulated products such as pesticides contain warnings about health and or environmental risk. PIAs have the potential to serve as a risk communication vehicle but to date this promise has not been fulfilled.

140. The OECD is well-suited to take up these challenges as part of its work on the data-driven economy. It can draw lessons from the Recommendation on *Digital Security Risk Management for Economic and Social Prosperity* and its work on *Data-Driven Innovation: Big Data for Growth and Well-Being* and, more generally, on previous work that OECD has done in other areas involving risk management. As well, the OECD can draw on the expertise of the delegations from member countries and from observers who attend meetings of the Working Party on Security and Privacy in the Digital Economy.

ENDNOTES

1 OECD (2013), *The OECD Privacy Framework* OECD Publishing, Paris. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. p.20.

2 *Ibid*., p.27.

3 OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en.

4 OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264229358-en. Chapter 5.

5 http://www.oecd.org/gov/risk/g20oecdframeworkfordisasterriskmanagement.htm.

6 OECD (2015), *op cit*., , p.32.

7 About risk terminology, see OECD, 2015, *op cit*., p.30.

8 See, for example, Terje Aven, Ortwin Renn, and Eugene A. Rosa, "On the ontological status of the concept of risk" Safety Science 49 (2011) pp.1074–1079.

9 *Ibid*., p. 10.

10 International Organization for Standardization, *ISO 31000:2009 Risk management—Principles and guidelines*, p.2.

11 See Chapter Three of *Privacy impact assessment and risk management*, a report prepared for the United Kingdom's Information Commissioner's Office by Trilateral Research & Consulting, 4 May 2013, for a useful overview of several risk management standards and methodologies in use in the UK and elsewhere.https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf

12 The only definition I could find defined privacy risk as the "Potential loss of control over personal information, such as when information about you is used without your knowledge or permission." Mauricio S. Featherman a and Paul A. Pavlou b, "Predicting e-services adoption: a perceived risk facets perspective", Int. J. Human-Computer Studies 59 (2003), p. 455.

13 Information and Privacy Commissioner, Ontario, "Canada, Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default", 2010, p.1) https://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf

14 The Centre for Information Policy Leadership, "A Risk-based Approach to Privacy: Improving Effectiveness in Practice" (2014) p. 1.

www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF

15 National Institute of Standards and Technology, Privacy Risk Management for Federal Information Systems, NISTIR 8062 (Draft), May 2015, http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

16 Commission Nationale de l'informatique et des Libertés, "Methodology for Privacy Risk Management" (2012) and "Measures for the Privacy Risk Treatment" (2012). http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf and http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf

17 Commission Nationale de l'informatique et des Libertés,"Privacy Impact Assessment Methodology" p. 7.http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf

18 Nymity, "Privacy Risk Reporting Methodology", p.3. https://www.nymity.com/~/media/Nymity/Whitepapers/Privacy%20Risk%20Reporting%20Methodology.pdf

19 Jules Polonetsky, Omer Tene and Joseph Jerome, "Benefit Risk Analysis for Big Data Project", Future of Privacy Forum, September 2014, http://www.futureofprivacy.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf

20 Daniel Solove, "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol 154, no. 3, January 2006, (pp 481-482. https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf

21 National Institute of Standards and Technology, Privacy Risk Management for Federal Information Systems, NISTIR 8062 (Draft), May 2015, *op cit.*, p. 55.

22 The Centre for Information Policy Leadership, *op cit.*, p. 1. **Error! Hyperlink reference not valid.**

23 Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

24 Nymity, *op. cit.*, p. 3.

25 Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", 30 May 2014, p. 4. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

26 OECD (2013), *op cit.*, p. 24.

27 National Institute of Standards and Technology, Privacy Risk Management for Federal Information Systems, NISTIR 8062 (Draft), May 2015, *op cit.*, p. 18.

28 *Ibid.*, pp. 18-19.

29 Daniel Solove, "Introduction: Privacy Self-Management and the Consent Dilemma", 26 Harv. L. Rev. 1880 (2013).

30 *Ibid.*, p. 1881.

31 OECD (2015), *op cit*., p. 38.

32 National Institute of Standards and Technology, "NIST Privacy Engineering Objectives and Risk Model Discussion Draft" www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf (2014), p.3.

33 See Claus-Peter H. Ernst Johannes, "Risk Hurts Fun: The Influence of Perceived Privacy Risk on Social Network Site Usage", http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1139&context=amcis2014

34 OECD, (2015), *op cit*., p.43.

35 However, see Polonetsky, Tene and Jerome, *op cit*.

36 "Digital security risk" is the expression used to describe a category of risk related to the use, development and management of the digital environment in the course of any activity.

37 OECD (2011), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", OECD Digital Economy Papers, No. 176, OECD Publishing. http://dx.doi.org/10.1787/5kgf09z90c31-en, p.22.

38 See Polonetsky, Tene and Jerome, *op cit*. They have developed a benefit risk methodology to assess big data projects.

39 See Joseph Alhadeff, Brendan Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions". http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1933731

40 Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability" 13 July, 2010, p.13 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

41 Article 29 Data Protection Working Party "Statement on the role of a risk-based approach in data protection legal frameworks", 30 May 2014, p. 3. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

42 Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner of British Columbia, "Getting Accountability Right with a Privacy Management Program." https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

43 National Institute of Standards and Technology, "Privacy Engineering Objectives and Risk Model - Discussion Deck: Objective-Based Design for Improving Privacy in Information Systems", *op cit*. p.1.

44 CNIL, "Methodology for Privacy Risk Management", *op. cit*., p. 9.

45 A Risk Based Approach for Accountability and Compliance: Remarks at the 35th International Conference of Data Protection and Privacy Commissioners. https://www.priv.gc.ca/media/sp-d/2013/sp-d_20130926_cb_e.asp

46 OECD (2013), *op cit*., p. 34.

47 Christopher Kuner, "The Governance of Globalized Data Flows—Current Trend and Future Challenges", paper prepared for June 23-24 Meeting of the Working Party on Security and Privacy in the Digital Economy, DSTI/ICCP/REG92015)3. p. 13.

48 See, Paula J. Bruening, "Interoperability: analysing the current trends & developments", *Data Protection Law & Policy*, May 2012, p.13.

49 Article 29 Data Protection Working Party "Statement on the role of a risk-based approach in data protection legal frameworks", p. 2.

50 M. Ryan Calo, "The Boundaries of Privacy Harm", *Indiana Law Journal*, Vol. 86:1131, p. 1157. http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf.