“A Risk-based Approach to Privacy?”
An Initial Issues Paper for Privacy Risk Framework and Risk-based Approach to Privacy Project
Workshop I
Paris, France
20 March 2014

This paper has been produced solely to set the context — and to provoke discussion — at the first Workshop of the Privacy Risk Framework Project of the Centre for Information Policy Leadership. None of its contents should be taken as the final views of the Centre, or of any of its Members or Principals.

The Locomotive Act of 1865 stipulated that self-propelled vehicles on the public highway should be accompanied by a man with a red flag walking 60 yards ahead of each vehicle.

I. Scope and Objectives

1. 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?

2. Is it enough — or sufficiently meaningful — to say that privacy is a human right and that the laws exist to safeguard “fundamental rights and freedoms”? Has the time come for clarity of those rights? How might privacy regulation and its implementation in practice be made more effective? What new or additional thinking is required? What, exactly, does a risk-based approach to privacy involve?

3. These questions raise issues which go beyond mere compliance with regulatory requirements. They go to the heart of what responsible and accountable organisations seek to achieve. They also demand scrutiny of the rationales for regulation.
4. As the pace of technological change outstrips the conventional thinking of lawmakers, regulators and businesses, a calibrated, risk-based approach may improve the ability of businesses to take a better-informed and better-structured approach to the handling of colossal volumes of personal information that they store and use on a daily basis. These issues become more pressing as companies seek to design, implement and demonstrate corporate privacy management programs and an ethical approach, often through programmes of Corporate Social Responsibility.

5. If the data privacy implications of products, services and other activities can be assessed from the perspective of their impact on individuals, can the likelihood of serious harm be reduced? Can the results of such assessments be reflected in better-targeted privacy programmes and other safeguards? How can it be made easier for non-experts to understand what they should — or should not — do?

6. Could a new consensus on a risk-based approach also help regulators fix and communicate their priorities for interpreting and enforcing the rules? Could it also provide businesses a better idea of what to expect and how best to avoid regulatory trouble?

7. In the longer term, how might this approach help policy-makers and legislators shape rules for the future that are more effective and less burdensome and which take into account the possible risk and harm to the privacy of individuals?

8. The Centre’s Risk Project seeks to answer some of these questions by exploring what is meant by taking a more risk-based approach to privacy. This initial discussion paper sets out some of the issues, with an attempt to develop a framework that improves the ability of businesses to understand, identify, assess and manage privacy risks.

II. Follow-on from Accountability

9. Many of these issues flow naturally and inevitably from the Centre’s pioneering work on Accountability, which so far remains largely unexplored. The Accountability Principle calls upon organisations to assess and mitigate the privacy risks to individuals raised by data use. The approach contemplates customised systems for internal, on-going oversight, with assurance reviews and external verification. There is a broad consensus that accountable organisations need to monitor and assess whether their internal arrangements manage, protect and secure data effectively in practice. An accountable business should be able to demonstrate that it has developed and implemented appropriate risk management measures.

10. What remains outstanding from the Accountability debate, however, is sufficient examination of what is actually meant by “privacy risks to individuals” and how organisations can best assess and manage them. A consensus here should go a long way to building practical tools for organisations to identify, classify and assess the risks in terms of likelihood and seriousness and on how best to balance risks against benefits. Understanding the risks to individuals from specific data uses also helps to identify not only the legal and policy requirements to ensure compliance, but also the social, ethical and cultural dimensions for which mitigating controls are warranted. In
turn, this allows higher or more complex risks to be prioritized and resourced through a corporate privacy programme as a matter of organizational accountability.

III. Regulatory Limitations

11. Calls for a risk-based approach extend beyond the focus on Accountability. In 2013, in the context of the proposed overhaul of the European privacy regulatory framework, Vivian Reding confirmed that “…we want to build an approach that adequately and correctly takes into account risk” and the EU Council of Ministers argued that “…the risk inherent in data processing operations should be the main criterion for calibrating the applicability of data processing obligations….”

12. Risk already features, to some extent, in existing legislative texts, including in the proposed EU Data Protection Regulation, and in enforcement strategies of some national data privacy regulators.

13. The case for a prescriptive risk-based approach is put forth by those who are keen to see genuine and effective safeguards in place — coupled with responsible and accountable conduct by businesses — but who also see existing regulatory frameworks as outdated or which may give rise to too many limitations and unintended consequences. Sharper focus on risk is seen as promising a more effective way to regulate data use. Specifically, it would enable us to tackle two of the perceived main shortcomings of traditional approaches: the lack of concrete objectives for privacy regulation and the absence of triggers or processes for setting priorities.

14. Concerns of this nature have been voiced across a spectrum of viewpoints, including public and private sector organisations, policy and law-makers, regulators and civil society. The debate is increasingly global and relevant given that several mature markets are considering revising or adding to their regulatory frameworks, and that emerging markets are enacting regulation for the first time. There is, indeed, a growing accord for fresh approaches to “getting it right” when it comes to ensuring privacy and good data protection: integrating the right policies and the right procedures, with the right technological safeguards and the right leadership on cultural and people issues. The need is to find approaches that work “on the ground” and in the real worlds of businesses and consumers, not just on the pages of laws and regulations.

15. Traditional ways of regulating privacy and data protection appear to be criticised for their lack of clarity on the underlying regulatory objectives and their intended results. Although it is universally agreed that privacy is an important and elusive value, with an ever-increasing public and political profile, there is less agreement about what are the virtues to be promoted and what are the evils or harms to be prevented. If expressed at all, objectives are generally pitched in high-level aspirational or abstract terms. Too often, they are simply implicit or taken for granted. Privacy legislation is accused of lacking clarity in concrete terms, for not being outcome-based or the sort of “smart regulation” that has been widely adopted in other spheres.
16. The absence of sufficiently clear objectives feeds other points. Critics say, for example, that there is too much focus on process and procedures, with the emphasis on how things should be done, and not enough on what results should be sought. Requirements are said to be too prescriptive and bureaucratic, without sufficient reflection on what happens in the real world. There is too much of a “one size fits all” approach, without consideration of context or market-place diversity and competition, where innumerable different business models supply a vast range of services. At the same time, the system is described as too paternalistic or insufficiently consumer-driven, without taking enough account of the benefits for consumers (who must be the best judges of their own best interests) or of the economic and social benefits of innovation and efficiency. As with red-flag automobile laws, the so-called Precautionary Principle may be too dominant, with too much focus on worst case scenarios. Finally, the regulation of data protection is said to be too abstract and theological, relying too much on aspirational paperwork, without enough action and “bite”.

17. A parallel concern about traditional approaches is the lack of triggers or processes to enable organisations to set priorities. Privacy requirements are often cast in absolute terms, with little recognition of the need to reflect context, scale or significance. It is assumed, therefore, that there is either full compliance or noncompliance. This is not sustainable in a world where both regulators and businesses must stretch limited resources; where both need to be “Selective to be Effective”; and where both need a clear and agreed understanding of the priorities. Finally, a lack of priority and focus on areas of greatest and real harm to individuals may lead to organisations either missing opportunities, i.e. running into “reticence risk”, or “missing the wood for the trees”, as their traditional approaches to and structures for dealing with legal compliance cease to be fit for the new information age.

IV. The Benefits of using Personal Information

18. Not only are some threats to privacy more serious than others, but privacy itself is not — and never can be — an absolute value. It must be balanced against other human rights, such as personal security and freedom of expression. There is also a need to strike the right balance with the benefits that arise from the commercial and public use of personal information. The benefits may flow directly to the individuals concerned or they may (as with medical research, law enforcement or improved living standards) accrue at a more societal level. The nature and the extent of the benefits can vary significantly. In the same way as there is too much vagueness over the dangers of using personal information, there is insufficient scope to identify and assess the benefits. Also, there is a “reticence risk” that some benefits may be lost altogether due to regulatory uncertainty, excessive caution or even inaccurate application of the data privacy laws. Finally, the mechanisms for weighing and balancing the respective dangers and benefits are still largely undeveloped without a clear consensus about the best ways forward.

V. Emerging Thinking and Momentum

19. A number of headline messages have emerged from various workshops and discussions held in the last couple of years on, or around, the scope for a more risk-
based approach. These included the Centre for Information Policy Leadership accountability project workshops in Warsaw and Toronto, a session at the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw, and an informal workshop sponsored by The Privacy Projects in London. In written form, the reports of the “Data Use and Impact Global Workshop” and the “Data Protection Principles for the 21st Century” have both drawn attention the need for greater focus on the use of personal information and the risks attendant on the various uses. A similar approach is anticipated in a forthcoming World Economic Forum “Rethinking Personal Data” report. Finally, in early 2014, Centre members participating in the Steering Committee for this Centre project also contributed to this Discussion Paper.

20. In summary, the key messages from these sources include:

• A risk-based approach appears to be worth exploring for various reasons – to provide clearer steers for responsible businesses seeking both to be more accountable in practice and to comply with an emerging legal requirement and regulators’ expectations that they will conduct privacy risk assessments; to address regulatory limitations or uncertainties; to help both regulators and businesses to prioritise and be effective; to help address some of the challenges posed by new technologies which call for new tools and processes that would augment and adapt data protection principles for the new information age; to develop mechanisms that go beyond regulatory compliance as a goal in itself; and finally to improve the prospects for global inter-operability.

• A risk-based approach should be seen as complementary and in addition to mandatory legal requirements, improving their overall effectiveness, and not as dilution of individuals’ rights, avoidance or as voluntary “self-regulation” instead of privacy regulation.

• To date, there has been remarkably little contact between the disciplines of Risk Management and Privacy/Data Protection. Any risk-based approach should leverage existing practices and learnings from the risk management world.

• Businesses are well used to assessing and managing risk from their own perspective as part of their Enterprise Risk Management process, such as looking at privacy as an enterprise risk, security risk, liability risk, compliance risk or reputational risk.

• But any attempt to assess and manage risks in terms of the impact on individuals would be novel and raises different considerations.

• There is so far little agreement as to what is meant by the privacy risks faced by individuals. The classification of privacy risks must be settled before focusing on how best to address them.

• There is merit in building on regulatory and legislative encouragement for Privacy Impact Assessments.
• There would be a particular advantage in developing a common approach, acceptable to as many businesses and regulators as possible.

• Any approach must be kept as simple as possible.

• Attempts to manage privacy risks should be integrated closely alongside other risk management arrangements, with businesses encouraged to experiment and collect relevant data.

• As a starting point, initial consensus on the nature of privacy risks, in terms of the threats and harms, would be useful, together with agreed methodologies for assessing likelihood and seriousness and balancing the results against the benefits.

VI. A Matrix of Threats and Harms

21. A framework is needed to link and prioritise the types of threat and harm before weighing the results against the benefits. The suggested Matrix of Threats and Harms demonstrates how this can be done in practice and how it could be developed as a Template, at least for initial testing. A Template could be very attractive for both businesses and regulators and which, in due course, may receive some form of regulatory endorsement.

22. The Horizontal Axis of the suggested Matrix sets out the Threats that could lead to the Harms listed in the Vertical Axis.

23. Threats are grouped together under two main headings:

   i. inappropriate use of personal information
   ii. personal information in the wrong hands

24. There are then two main types of Harm which could be suffered by individuals:

   iii. tangible damage
   iv. intangible distress

25. A third type of Harm, Societal Harm, may be controversial and harder to express but is added for completeness.
### Threats Arising from Use of Personal Information

<table>
<thead>
<tr>
<th>Tangible Damage to Individuals (physical or economic)</th>
<th>Inappropriate Use, e.g.</th>
<th>In Wrong Hands, e.g.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• inaccurate or outdated;</td>
<td>• lost or stolen; and</td>
</tr>
<tr>
<td></td>
<td>• unanticipated use;</td>
<td>• unjustifiably</td>
</tr>
<tr>
<td></td>
<td>• unusual use beyond</td>
<td>accessed, transferred,</td>
</tr>
<tr>
<td></td>
<td>societal norms; and</td>
<td>shared or published.</td>
</tr>
<tr>
<td></td>
<td>• unjustifiable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>inference or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>decision-making.</td>
<td></td>
</tr>
</tbody>
</table>

#### Tangible Damage to Individuals (physical or economic)

- Bodily harm
- Loss of liberty or freedom of movement
- Damage to earning power
- Other significant damage to economic interests

#### Intangible Distress to Individuals (which can be objectively established)

- Detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions
- Chilling effect on freedom of speech, association etc.
- Reputational harm
- Personal, family, workplace or social fear, embarrassment or anxiety
- Unacceptable intrusion into private life
- Discrimination or stigmatisation

#### Societal Harm

- Damage to democratic institutions (e.g. excessive state or police power)
- Loss of social trust (“Who knows What about Whom?”)
VII. Elaboration of Threats

26. Some types of threat arising from the handling of personal information are obvious; others need to be amplified, with possible omissions explained.

27. The two threat headings deliberately do not include a specific reference to the collection of personal information because the collection is viewed as part of the data lifecycle, i.e. collection, processing and use of data, which in its entirety is subject to continuous risk assessment.

28. For similar reasons, the threats do not explicitly include any reference to purpose limitation. Again, any wider purpose than originally contemplated would constitute and can be controlled at the relevant time, as a matter of inappropriate use. Therefore, a “new” use which presents a threat with a real likelihood of causing significant harm would not be acceptable.

29. In a risk-based environment, it is the use of the information that arguably poses the greatest threats and where particular attention must be focused. Central importance is therefore attached in the Matrix to Inappropriate Use. This also has the advantage of avoiding the familiar practical problems associated with over-emphasis on collection alone, not least the dangers of information overload for consumers, or how to deal with situations where there is no interface with individuals and data are not collected directly from individuals. The assessment of threat arising from use must also be contextual. In other words a flexibility is required which recognises that the context will be an important factor in determining a level of threat and the potential to cause harm.

30. Appropriate use, therefore, needs to be decided by reference to agreed upon criteria that are both objective and contextual. Four suggested examples follow:

- using inaccurate or outdated personal information — essentially data quality, though with the caveat that information can be accurate and yet still pose a threat and that inaccurate data will matter more in some contexts than others;
- unexpected or unanticipated use — a use that a reasonable individual in this context would not have expected or could not have anticipated;
- unusual use beyond societal norms — a use of which any reasonable individual in this context would object; and
- unjustifiable inference or decision-making — an inference or decision which the organisation cannot objectively defend.

31. It is worth repeating that these uses are not outlawed in themselves. “Inappropriate” use, as with the other threats, only becomes unacceptable where it would or could impose significant harm and cannot be justified by countervailing benefits to individuals, groups or society as a whole. A beneficial use may thus be entirely acceptable even though no-one anticipated it at the outset.

32. Also, the information provided to the individual, or a consent are not by themselves a panacea. A use of personal information can be inappropriate even though it may have been specified or foreseen in information communicated to an individual. The prominence and the extent of the individual’s freedom of choice will be amongst the
factors to consider, and may play a part in conditioning expectations, but “small print” disclosure cannot, by itself, justify an “unusual” use.

33. The second heading deals with personal information which could or does pass into the “wrong hands.” Most obviously this covers data breaches where the information is lost by the organisation or is stolen. But it also embraces situations where a threat could be generated by sharing the information with, or passing it to, a third party or otherwise placing it in the public domain. Again the “threat” is not outlawed as such, but has consequences where it may generate potential or actual harms and may not be justified.

- Is this a satisfactory summary of the Threats arising in connection with personal information?
- Is it accepted that a risk assessment should particularly focus on use, rather than solely on collection and purpose?
- How well do the two main headings work?
- Is it right to emphasize the importance of context and objectivity?

VIII. Elaboration of Harms

34. The sub-categories of the two types of harm faced by individuals are largely self-explanatory. **Tangible damage**, normally physical or economic, includes:

- bodily harm;
- loss of liberty or freedom of movement;
- damage to earning power; and
- other significant damage to economic interests, for example arising from identity theft.

35. Although as noted below, **intangible distress** has to be assessed objectively, it can still be harmful and includes, for example:

- detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions;
- chilling effect on freedom of speech, association etc.;
- reputational harm;
- personal, family, workplace or social fear, embarrassment, apprehension or anxiety;
- unacceptable intrusion into private life; and
- discrimination or stigmatisation.

36. For both tangible damage and intangible distress, the harm may be potential (it could or would have this effect) or actual (it will, is having or has had this effect).

37. While risk assessment involves tests of foreseeability, these must be objective descriptors of harm —harm imposed on the reasonable man or woman in this context. In the same way as tort law ignores the “egg-shell skull”, the test is not—and cannot
be — concerned with the impact on each particular individual, let alone an individual with particular sensibilities. The test must again be context-driven, although information communicated to the relevant individuals, and any consent they have given, will again be factors.

38. **Societal harm** can arise directly from business activity. It is more likely to occur, though, where the personal information — quite possibly obtained legally or otherwise from businesses — is used by governmental bodies. It includes:

- damage to democratic institutions, for example excessive state or police power;
- loss of social trust (Who Knows What About Whom?).

- Is this a satisfactory summary and classification of the harms which could arise from the use of personal information?
- Are there some harms which should be defined differently or excluded?
- Are there other harms which should be added?
- What concrete examples best illustrate different types of harm?
- What can be learned from cases (US, UK and elsewhere) where courts have demanded high thresholds of harm before awarding redress to claimants or upholding regulators’ actions?

IX. **The Matrix as a Risk Management Tool**

39. Risk Management calls for judgement, based upon honest, well-informed and justifiable answers to structured questions.

40. It is envisaged that as a new service, product, technology or activity is developed, a business could use the Matrix to raise questions and structure a series of judgements arising from each of its inter-sections. Each inter-section requires two specific judgements to be made. A numerical scale would add calibration and rigour:

   i. **How likely** is it that this Harm could arise from this Threat? Can this be sensibly quantified on a numeric scale?

   ii. **How serious** would this Harm be if it arose from this Threat? Can this be sensibly quantified on a numeric scale?

41. Both judgements should be informed by as much hard data as possible (e.g. the nature and volume of the data, consumer complaints, survey results, industry norms etc.). Also, regulatory guidance could provide an important source of relevant data and regulatory expectations relating to Likelihood and Seriousness of particular harms. The point has already been made that both assessments must be applied objectively, using the reasonable person test. Tangible damage will be objective and usually easier to assess but, even for intangible distress, assessments cannot be based on subjective perceptions. Both the Likelihood and the Seriousness judgements, however, can and should reflect — and feed into the equation — a prospect of serious harm to a few individuals or less significant harm to many individuals.
42. Each inter-section is a function of the level of the threat and the likelihood that the threat will cause harm. The key judgement is whether there is a **significant risk**. In other words, is there a **significant likelihood that the particular threat could lead to the particular harm with a significant degree of seriousness**? Different businesses will have different appetites for risk. Subject to any guidance from its regulator (see below), each business will wish to decide where to fix the level at which a risk is judged to be significant.

43. Where the judgement is made that there is a significant risk, appropriate action is then needed to mitigate the risk. This might, for example, involve a change of scope, further safeguards or the adoption of a new or improved Comprehensive Privacy Programme. A further post-mitigation assessment would then be required.

- Is the “significant risk” test the right one?
- Is this too simple for practical use?...
- ...or too complicated?

X. **Balancing the Benefits**

44. At any stage where it is judged that significant risk exists or remains, a secondary process is needed to determine whether the **benefits, nonetheless, sufficiently outweigh the risks**.

45. The benefits may accrue to an individual, to the relevant group of individuals, or to a wider public value and society. Benefits to the business alone are unlikely to outweigh a significant risk to individuals. The important point is that the specific benefits must be:

- identified;
- articulated;
- justified by reference to the appropriate external criteria; and
- judged to outweigh the risk.

46. The accountable business must then stand ready to demonstrate how that judgement was reached. There may be a case, not attempted in this paper, for developing a similar Matrix to identify and measure the relevant benefits.

- Does the test of “outweighing benefits” work?
- Are there situations where the risks may be too great whatever the benefits?

XI. **The Matrix as a Tool to Prioritise and Guide Regulatory Intervention**

47. Regulators cannot do everything. Their responsibilities and challenges are growing. Their resources are limited and sometimes in decline. They must be selective to be
effective; they need to concentrate on the serious, not the trivial. But how should they set their priorities? How, in particular, do they decide which businesses or activities to target for preventative or investigatory intervention?

This is where the Risk Management Matrix may be useful also as a tool for regulators. A consensus based on the language and methodology of the Matrix could help regulators fix and communicate their own priorities for interpreting and enforcing the rules. This would give businesses a better idea of what to expect and, at a minimum, they could adopt a “mirror-image” approach in their efforts to avoid regulatory trouble and exceed compliance requirements.

One could speculate various possibilities for a Regulator which adopts or endorses the Matrix as its starting-point:

- The Regulator could signal that it will use the Matrix to target sectors, businesses or activities for attention, anticipating action where it concludes that there is a significant likelihood that a particular threat could lead to a particular harm with a significant degree of seriousness;

- The Regulator could indicate that it expects, as a matter of due diligence, all or some businesses to conduct a risk management exercise on these lines, concentrating its attention on situations where a satisfactory exercise has not been conducted; and

- The Regulator could use the Matrix to determine whether the business has adopted appropriate risk mitigations (e.g. limitations, restrictions, safeguards).

There would be a further advantage if regulators could communicate tolerance levels to help businesses decide whether a risk is significant. It would be a powerful message, for example, if a regulator were to state that a risk would be significant for a particular type of activity when the assessment score exceeds a prescribed level.

The approach implies that regulators will need to assess the efficacy of risk processes. In keeping with the principle that risks are usually mitigated but seldom eliminated, there may, however, be situations where a regulator concludes the risk assessment process was reasonable and complete but simply disagrees with the end-decision. In that situation, the company may be exposed if the harm does, in fact, materialise. In other situations — as the FTC has shown with imaginative use of consent decrees that have affected privacy programmes — a regulator which finds fault with risk assessments is well-placed to ensure constructively that its rulings have positive effects in the future.

Is this a sufficiently full account of the potential for regulators?

XII. The Matrix as a Tool Where a Harm Has Been Suffered.

There is also scope for both regulators and courts to use the Risk Management Matrix as a remedial tool where a harm has actually been suffered by one or more
individuals. It may help determine how the harm came about, not least in efforts to repeat similar incidents. More directly, the Matrix could influence the nature and scale of regulatory sanctions or compensatory redress. It may, in particular, help to decide the foreseeability of the harm that arose from the threat.

53. In a world where regulators rightly pay most attention to those who knowingly ignore their obligations (or are cavalier or repeat offenders), they are entitled to ask for evidence that a risk assessment had, in fact, been conducted before the activity in question was launched.

54. It is to be expected that a risk-based approach would be accompanied by significantly heavier penalties and sanctions, where risk-assessment has been non-existent or manifestly inadequate.

XIII. Implications for Law-makers

55. This discussion paper is preliminary and exploratory. It focuses on approaches which may be attractive to businesses and regulators within the frameworks of current legislation. If this proves to be an effective way of maintaining and improving protections in practice, it might be contemplated in the longer term that suitable legislative text could be developed to embrace more comprehensively a risk-based approach in preference to measures which have been judged as ineffective.
**Annex 1: Glossary**

The terms and definitions provided below are not new concepts. Most of them already exist within risk management schemes, but have been adapted for this paper.

**Threat** — anything or any activity with the potential to cause *harm*.

**Harm** — adverse impact on individuals, including physical, mental, social and economic impacts.

**Risk** — a function of the level of a *threat* and the likelihood that the *threat* will cause *harm*.

**Risk Assessment** — the process by which the *risk* associated with a particular *threat* is identified and categorized.

**Risk Management** — the process, including risk assessment, by which significant *risk* is weighed against benefits and, as necessary, mitigated.

**Benefit** — a positive advantage — whether physical, mental, social or economic — for an individual, a group of individuals or for a recognised wider public value.
Annex 2: Main Source Materials (roughly dated in order)

- Privacy Impact Assessment Handbook — ICO
- Various papers on Risk and Regulation — Better Regulation Commission
- Risk-based Regulation — Professor Julia Black, LSE
- Managing Information Risk — HM Government
- Data Protection Regulation Action Policy — ICO
- Smart and Dumb Questions to Ask about Risk Management — Professor Michael Power, LSE
- Accountability: Data Governance for the Evolving Digital Marketplace — Centre for Information Policy Leadership
- Methodology for Privacy Risk Management — CNIL
- Getting Accountability Right with a Privacy Management Programme — Canadian Commissioners
- Privacy Impact Assessment and Risk Management — Trilateral Research
- Draft Code on Conducting PIAs — ICO
- Data Sharing between Public Bodies — Law Commission
- Data Use and Impact Global Workshop — Fred H. Cate / Mayer-Schonberger
- Data Protection Principles for the 21st Century — Fred H. Cate / Peter Cullen / Mayer-Schonberger
- Rethinking Personal Data — World Economic Forum
- “Big Data Protection” — Professor Lokke Moerel
Annex 3: Examples of Businesses which have Attempted to Manage Privacy Risks

**Company A**

Company A has a Privacy Program which uses a quantitative risk-based approach to Privacy Impact Assessments of processes, programs and technology. That approach evaluates factors that affect the risk of harm to individuals such as data sensitivity, activity sensitivity and volume, and factors that contribute the likelihood of the risk being realized such as third party involvement, geographic scope, incident and audit history.

Quantitative analysis of these inherent risk factors yields the scope of privacy controls that must be evaluated and a required level of aggregate control effectiveness in order to ensure that the inherent risks have been sufficiently mitigated (i.e. residual risks are sufficiently low).

Each privacy control is then evaluated according to a standardized effectiveness scale to determine whether the aggregate control effectiveness requirement for the process, program or technology has been met.

-------------------------------------------------------------------------------------------------------------------------------------

**Company B** – to follow

**Company C** – to follow
### Annex 4: Examples (non-exhaustive) of Risk Assessment Schemes used by UK Regulators

- Health and Safety Executive / Local Authorities Enforcement Liaison Committee Priority Planning system;
- Office of Fair Trading — Trading Standards Risk Assessment Scheme;
- Food Standards Agency — Food Hygiene and Food Standards Intervention Rating Schemes; and
- Local Authority Integrated Pollution Prevention and Control and Local Authority Pollution Prevention and Control) Risk Methodology.