28

Mr Ivo Opstelten
Minister of Justice
Ministerie van Veiligheid en Justitie
Turfmarkt 147
20301 - 2500 DP Den Haag

Brussels, 28 May 2014

Dear Minister Opstelten,

We are writing to you as the Industry Coalition for Data Protection (ICDP)* in light of the upcoming meeting of the EU Justice and Home Affairs Council on 5-6 June. We would like to share with you some thoughts on the key topics relating to the General Data Protection Regulation that are on the agenda for this meeting. We hope you find them useful.

ICDP supports the opportunity to harmonise and modernise the European data protection framework. By creating conditions for both privacy and innovation to flourish, a revised EU data protection framework that is robust, balanced and future-proof could boost economic and social growth. However, if enacted in the present draft form, the Regulation would delay the launch of innovative services in Europe, cause substantial loss in revenues for businesses of all sizes and in a wide range of industries, limit opportunities for new market entrants, strongly increase administrative costs and create legal uncertainty.

ICDP strongly agrees with the European Data Protection Supervisor, Peter Hustinx[1] that data protection legislation is most effective when it follows a risk-based approach. A risk-based approach has the potential to substantially improve outcomes for data subjects while reducing administrative burdens for data controllers and processors. By adopting a largely precautionary approach, we felt that the European Commission missed an opportunity to increase legal certainty, reduce administrative burdens and provide citizens with more effective protection. While we shared the overall directions and the meaningful changes the Council has discussed over the last months, we are concerned by some recent suggestions that would move away from a risk-based approach. Following are some thoughts on these recent changes and ideas on how to strike the right balance between protection and flexibility, control and accountability, to eventually equip the European Union with a framework that will remain valid for many years.

Key points:

- We welcome the ongoing efforts to find the right balance between facilitating the free flow of information and safeguarding the personal data of European citizens. We believe that most of the refinements suggested by the Council to the provision on **international data** transfers strike the right balance.

- A real **one-stop-shop mechanism** allows companies to deal with only a single privacy regulator no matter how many Member States they operate within. We

1 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-02-14_letter_Council_reform_package_EN.pdf

would like to stress that it is essential that a One stop shop for organizations and individuals means one decision, one outcome. This is one of the key improvements that the proposed Regulation was intended to offer all stakeholders by providing legal certainty and greater efficiency for industry, citizens, and regulators alike.

- **Pseudonymous data and the pseudonymisation of data are two separate, yet important and complementary concepts**. Discussions around replacing one with the other do not address the fundamental issue both concepts aim to resolve, namely **the ability to process data that cannot be directly identified back to the data subject**.
- A **differentiation between automated processing and automated processing that creates a profile** is overly complex, not necessary for effective protection of data subjects, and could undermine the achievement of a genuine risk-based approach.
- **Profiling based on pseudonymous data** should not fall under the more restrictive provisions of Article 20, intended to regulate profiling with higher risks for the data subject (e.g. when it creates new legal effects).
- To remain future-proof, the data protection framework needs to stay **technology neutral**, including with regards to data portability.
- **A clearly-defined relationship between data controller and data processor** is vital for the success of the future data protection framework.
- **Cutting red tape** such as the **authorization for a data exchange within a controller group of undertakings** within EU be expanded to **processors** as well as to transfers to **third countries** if an adequate level of data protection is ensured.

We hope that you find this input useful for the discussions you will be having in the first week of June. We are of course at your disposal should you or your services wish to discuss these issues in greater detail.

Yours sincerely,

***About the Industry Coalition for Data Protection**

The Industry Coalition for Data Protection (ICDP) is comprised of 16 associations representing thousands of European and international companies who are building, delivering, and advancing the digital experience. Members of ICDP include: Association for Competitive Technologies (ACT), American Chamber of Commerce to the EU (AmCham EU), BSA | The Software Alliance (BSA), DIGITALEUROPE, European Association of Communications Agencies (EACA), European Digital Media Association (EDiMA), European Multi-channel and Online Trade Association (EMOTA), European Publishers Council (EPC), European Internet Services Providers Association (EuroISPA), Federation of European Direct and Interactive Marketing (FEDMA), GS1, IAB Europe, Interactive Software Federation of Europe (ISFE), Japan Business Council in Europe (JBCE), TechAmerica Europe and the World Federation of Advertisers (WFA).

ANNEX

DETAILED COMMENTS ON SELECTED ISSUES OF THE DRAFT GENERAL DATA PROTECTION REGULATION
May 2014

International Data Flows

ICDP welcomes the ongoing efforts of the Council to find the right balance between facilitating the free flow of information and safeguarding the personal data of European citizens in a global context. Users as well as business are participating in a physical and online world which crosses jurisdictions' borders and hence requires a framework that **allows for the international transfers of data which are in accordance with appropriate safeguards or derogations for specific situations.**

Territorial scope

We welcome refinements regarding the territorial scope of the legal requirements, in particular the clarification that the mere accessibility of a website in the Union or of an email address and of other contact details or the use of a language generally used in the country where the controller is established is insufficient to ascertain the applicability of law and jurisdiction. In our view, the Regulation should apply when a product or service is "specifically targeted" at customers or users in the EU. It is equally important that such clarifications are applied to both controllers and processors.

Adequacy

One of the main difficulties in the adequacy process today is an apparent focus on the existence of formal rules rather than an **assessment of the actual, real-world protections extended to personal data.**

We, therefore, **welcome the overall approach** taken of broadening the scope of the various factors to be considered, such as participation in multilateral or regional systems and others. [Article 41 (2c)]; as well as the recognition that one or more specific sectors, such as a private sector within a third country, may offer an adequate level of protection. [Recital 80, Article 41]. Leaving the existing decisions in force until amended, replaced or repealed also improves the much needed legal certainty, which a sunset clause would no doubt undermine [Articles 41 (3a) and 42 (5b)].

These are key to achieve an international transfers regime that is future proof and recognizes multilateral efforts also in the area of privacy and data protection.

There remains sporadic references to "**specific authorization**", instead of "further" as proposed by the Commission, when there is an adequacy decision or safeguards are in place. The essence of these measures is that once they are approved, no other (or "further") notification is required. If we open the door for additional ("specific") requirements, it defeats the purpose of these instruments, it will create uncertainty and could undermine the system that has been in place and working. Therefore, the Commission's original proposal ("such transfer shall not require any "further" authorization) seems to be more in line with the purpose of the law. [Recital 80, Article 41 (1), 42 (2a)]

Appropriate safeguards

We **welcome the Council's efforts to further define "appropriate safeguards" and give these a proper legal status**. In addition to codes of conduct and certification schemes, which we believe should have European wide effects, we welcome the Council's support of the Commission's proposal to allow the use **of binding corporate rules (BCRs)** for both controllers and processors [Article 4 (17)], including joint undertakings or group of enterprises engaged in a joint economic activity. This instrument has become an important addition to the existing tools allowing for the international transfer of data and we welcome the integration of this instrument in the legislation. However, we do share concerns on the lengthiness and cost of such approval processes and that further improvements are needed to make this instrument more broadly available than it is today

We welcome clarification of previous proposals that the requirement of **prior authorization** should be limited to certain cases [Article 42 (2a)], and the recognition that approved codes of conducts and certification schemes do not require such authorization.

We also welcome the possibility to use **standard contractual clauses** in downstream processing contracts between processors, which mirrors positive steps and work that European regulators are undertaking in this area.

Derogations for specific situations

The reason for the reference to "explicit" **consent** in some places [Article 44 (1a) and Recital 86], but not in others is somewhat unclear. ICDP would welcome clarification that the "explicit" standard is not applicable in all situations, and points out that this requires Articles 4 and 7 to be amended accordingly. We are also concerned about the suggestion to limit the existing permission of transfer when it is necessary in relation to a contract or legal claim [Recital 86].

While we remain concerned about the possibility of **suspending data transfers** based on the rather vague concept of "public interest', we do welcome clarifications suggested that these should not allow for actual suspension of all data flows to that third country, but for reasonable limitation concerning specific categories of data. However, as previously suggested, we believe that appropriate safeguards should also be taken into consideration. [Article 44 (5a), Recital 87]

Finally, we welcome the fact that the Council acknowledges the **value of the "legitimate interests" ground** as a basis for data transfers. ICDP notes that this legal basis will be of primary importance because of its superior potential to protect privacy compared to contract and consent, because it can provide a meaningful and most of the time more appropriate alternative to consent, and because it proves particularly useful for SMEs. In this regard, consistency should be ensured between the relevant Recital and Article, clarifying that this legal ground is available for both processors and controllers [Recital 88 and Article (1h)]

Circumstance regarding a "legitimate interest" for temporary or non-bulk or non-frequent data transfers should be acknowledged and established for circumstances where transfer of personal data is incidental but necessary for completion of support

function, troubleshooting or routine control etc. Additional circumstances should be considered, such as established contracts between controllers, processors and sub-processors, use of pass-words to access systems/data, encryption and VPN tunnels securing the transmission of data flows. Furthermore this legitimate interest should be also acknowledged under a reciprocity condition prior conclusion of an adequacy assessment of a third country.

Data exchange within groups of companies

ICDP welcomes the approach of cutting red tape such as the authorization for a data exchange within a controller group of undertakings within EU (Article 22 (3a) Amendment 117 EP). Thereby it is recognized that the transfer of personal data within a group of undertakings does not impose a higher risk than transferring it within one legal entity. This authorization for data exchange within a group of companies should be expanded to processors as well as to transfers to third countries if an adequate level of data protection is ensured.

One Stop Shop

To allow for a One stop shop for organizations and individuals to truly mean: one decision, one action and allowing for local redress, the following must be taken into account:

- For an effective allocation of competences, the trust and full endorsement of the system by all DPAs is required. The procedural aspects of the One Stop Shop need to be defined by law.
- This contains a catalogue of competences among DPAs based on: main establishment of the organization, nature of the case and proximity angles.
- It puts the effective exercise of the individual's rights first.
- It allows the individual the right to obtain effective administrative redress as they can always go to their local DPA.
- It foresees the ability of the local DPA to take local decisions on a complaint when the case is clearly arising in a local context and there is no need for a European wide decision.
- For wider problems that affect individuals in different Member states (more than 2 Member states) and/is based on a pan-European practice or require coherent/consistent application of the law, the 'lead authority' is competent while DPAs concerned remain involved in order to ensure that the data controllers' behavior is modified.

The level of involvement of a local DPA other than the lead DPA (consultation, coordination, draft measure) will vary from case to case depending on the proximity level and the demand for consistent application of the law. Because not all cases are clear-cut, it is essential to reconcile the need for effective individual redress with that of consistent and effective application of the EU data protection framework. Hence we would like to highlight a few key aspects that should be taken into account:

- **Providing for clear rules on the distribution of competences:**

  1. Each DPA remains competent in most cases competent to hear complaints from individuals being resident in its Member State.

  2. Each DPA is competent to decide on a complaint that is directly linked to a processing activity that is taking place on its territory. For example, if a customer is concerned that their data stored on a computer device which they had left in for repair was misused by a staff member in that store then it is correct that this would be examined by the local DPA in the country in question. Even in cases where the OSS applies, the local DPA should be able to assist the lead DPA on investigations on the territory of the former in order to expedite the process. This does not apply to the setting of fines to the controller or processor, or to decisions that relate to pan EU compliance, data protection audits or consistency of interpretation which are considered to have a "general nature". These cases will be dealt through OSS.

     Data Protection Audits such as those undertaken by certain regulators in the EU are important in ascertaining data protection compliance for the whole range of data processing activities of a controller in the EU. A lot of resources are invested both from the side of the controller and the DPA in order to ensure that these audits are thorough and robust. It is therefore important that such practices fall within the scope of the OSS – the lead DPA, in close coordination with other DPAs that need to be consulted, should be the sole responsible entity for undertaking such audits.

  3. In the cases where the OSS is triggered, a single authority, the lead DPA, will have the exclusive power to impose fines, ***determine remedies*** and exercise authorization powers. Each DPA remains competent to take investigatory powers, ***propose draft measures in cases of matters arising on their own territory*** and assist, as required, in the ***implementation of the corrective measures in their territory*** designed to stop a violation of individuals' data protection rights. This demonstrates a clear emphasis on guaranteeing the fundamental right to data protection as provided by Article 16 TFEU. While the competences of the local DPA are clarified and strengthened, it should be clear that in any case the final decision on corrective measures including whether to impose a fine would rest with the lead DPA.

- **Clarifying the concept of main establishment.** To provide legal certainty to both individuals and companies, the concept of main establishment should be clarified as follows:

  - Need for consistency in defining the main establishment of the controller and processor, preferably using the same criteria.

  - When defining the main establishment, different criteria may be considered, but focusing on where the main decision are taken as to (1) the purposes, conditions and means of the processing of personal data or (2) the applicable technical and organizational measures, procedures and policies for the protection of the rights of the data subjects are taken.

- These should be based on objective criteria such as the: location of the controller or processor's designated European headquarters; the location of the entity within a group of undertakings which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; or the location where effective and real management activities are exercised determining the data processing through stable arrangements for the undertaking or group of undertakings.

- **Allowing individuals or companies to challenge the designation of the lead DPA:**

  1. A company (including a non-EU controller with no representative) or individuals may ask confirmation from the DPA regarding its designation of the lead DPA, and other DPAs must take the utmost account of such confirmation ("confirmation procedure").

  2. In cases where the DPAs disagree about the designation of the lead DPA, those DPAs should refer the matter to the EDPB ("challenge procedure"). The EDPB should provide a non-legally-binding opinion by a simple majority on which DPA is the lead DPA taking into account the criteria of the OSS; other DPAs should take the utmost account of the EDPB opinion. The controller or processor in question shall have the right to intervene in this process and he Board shall take its views into account when forming its opinion. A satisfactory appeal mechanism shall also be put in place for the controller.

- **Setting-up clear rules for judicial review and judicial redress**:

  1. Right to go before national DPAs: Maintaining proximity for individuals by allowing them to always go to their national DPA to put forward a complaint, which should be duly considered and act upon as appropriate within a reasonable delay. Judicial redress: Maintaining proximity for individuals by allowing them to always go before courts in their own jurisdiction to exercise their rights against a controller or processor.

  2. Judicial review:

     i. Judicial review of a decision imposing fines should be conducted before the national courts of the lead DPA. This rule should not deprive individuals of the right to an effective remedy since the situation in which individuals will seek judicial review will be limited to those where: (1) the OSS is triggered; (2) individuals disagree with the DPA regarding the imposition of a fine and its amount.

     ii. With this system, lead DPA decisions do not need be implemented into national law. As is generally the case under EU law, national courts can refer cases to the CJEU for a preliminary ruling in case of issues related to the interpretation of the Regulation.

- **Improving the consistency mechanism**:

  1. Other cases referred to the EDPB for opinion:

     i. Lead DPA issue ("challenge procedure"): Consulted DPA declines to be the lead or other competent DPA objects to confirmation; those DPAs must

escalate; EDPB must opine within one month by a simple majority (to obtain legal certainty).

ii. OSS cooperation procedure: When several local DPAs are involved in the same matter or in cases where a complaint is brought by an individual before a local DPA and where the OSS rules apply, a cooperation procedure should be triggered. In case of fundamental disagreement between the Lead DPA and others involved, the Lead DPA may escalate to EDPB; EDPB opines within one month by a two-thirds majority. Authorities shall take utmost account of this opinion.

iii. Urgency procedure: the instances where an urgency procedure shall be required will be limited and very clearly defined. It will not involve the power to issue fines as it does not directly impact individuals' privacy and should limit the possibility of corrective measures to what is strictly necessary.

Pseudonymous Data

The introduction of pseudonymous data as a subset of personal data would allow for an injection of a risk-based approach where it is most needed, and in a way which is entirely consistent with ECJ jurisprudence and the EU principles of necessity and proportionality.

Pseudonymous data and the pseudonymisation of data are two separate, yet important and complementary concepts. Discussions around replacing one with the other do not address the fundamental issue both concepts aim to resolve, namely **the ability to process data that cannot be directly identified back to the data subject.** The legitimate business models of many stakeholders are not well served by a framework that fails to capture both pseudonymous data in its raw state and pseudonymisation as a processing technique. By replacing the concept of "pseudonymous" data with that of "pseudonymisation" many models will no longer fall under the scope of the "pseudonymous data" collection or processing. Allowing for the differential treatment to unauthenticated users is critical to the dynamics of advertising and e-commerce.

ICDP strongly supports **maintaining both concepts in the Regulation with a workable definition of pseudonymous data** that covers both (i) data that has once directly identified an individual and has undergone a process of pseudonymisation to render it less likely to identify that person, and (ii) a series of unique online identifiers gathered about a data subject which may never have reached the point of actually allowing a controller to identify the person behind the data (pseudonymous data).

To promote data minimization, **the future framework should accommodate every legitimate business model relying on pseudonymous data – whether pseudonymous from the onset or following a "pseudonymisation" process**.

Automated processing and Profiling

The ability to process data to extract new actionable insights is absolutely essential to a knowledge-based economy, a key to building the information society, and is therefore at the heart of the EU Digital Agenda.

A risk-based approach needs to effectively protect the data subject whilst allowing legitimate and beneficial business activities that use advanced data processing techniques to continue and contribute to growth, jobs, entrepreneurship, innovation and competitiveness in Europe.

A differentiation between automated processing and automated processing that creates a profile, however, does not achieve such goal. This distinction is overly complex, not necessary for effective protection of data subjects, and could undermine the achievement of a genuine risk-based approach.

It is not clear what additional benefit further restrictions on automated processing, as distinct from profiling, would bring. **We therefore urge the Council to revert to the risk-based approach of the compromise achieved under the Irish Presidency including the Greek Presidency's proposal of February 17th**. In fact, it ensure further protections for data subjects compared to the 95/46 Directive by outlawing the use of profiling based on sensitive categories of data without suitable safeguards.

Furthermore, we underline the fact that those previous texts strengthened the legal threshold for impact on a data subject from legal effects to also include significant/ severe effects. The proposed threshold also reflects a risk-based approach encompassing the requirement for a negative effect on the data subject. This is a pragmatic move that should reduce the likelihood of many legitimate business practices (particularly from the e-commerce space) being subject to unnecessary restriction.

The current provisions on profiling are already capable of protecting data subjects against negative data processing practices. **We therefore urge the Council not to over-regulate automated processing as a general processing practice beyond what is outlined in Directive 95/46.** The distinction between automated processing and profiling is not at all easy to understand and adds unnecessary complexity to an already complex part of the Regulation. And there could be unforeseen consequences from restricting automated processing beyond the status quo *in addition to* profiling.

Moreover, we encourage the Council to promote data minimization processes and to **clarify that profiling based solely on the processing of pseudonymous data should be presumed not to produce legal effects or severely affect the data subject**. A profile based solely on the processing of pseudonymous data does not identify the individual directly and therefore does not pose the same degree of risk to the individual as do the practices identified under Article 20. Profiling based on

pseudonymous data should therefore be presumed to fall outside the scope of Article 20, and be governed by the general provisions of the Regulation.

Data Portability

While we welcome improvements brought to the Commission's proposal, some of the changes follow a broader trend that remains questionable. The most notable example is the intention to limit the scope of the data portability requirements to one specific segment of the economy, namely the information society sector.

We believe that the current legislative framework's robust protection has to be maintained in a way that does not undermine the digital single market. In this regard, it is of utmost importance that the **legislation remains technology neutral**. Indeed, the **95/46 Directive does not contain any carve outs or article designed to target a specific sector, industry or company size**.

The continuous demand for carve outs in the Regulation suggests that even the regulators recognize that some of the obligations are so onerous and/or prescriptive that they cannot be implemented by a large majority of the controllers and/or processors. This is highly problematic, as **any replacement of the current rules needs to remain technology neutral, workable, implementable and understandable to all.**

Data controller/ Processor

We believe that the **clearly-defined relationship between data controller and data processor is one of the major successes of the existing legal data protection framework in the EU**. The draft regulation has, unfortunately, blurred the fundamental distinction between data controllers and processors and their particular roles and liabilities. The controller defines the conditions within which the data processor should work and passes on those obligations to the processor contractually, according to the level of risk involved with each particular processing. The draft regulation would fundamentally change this concept, and inject confusion into well-settled contractual relations that will not serve the harmonization objectives of the reform and is an inappropriate solution to deal with the complexities of Cloud computing.

We **welcome the Council move towards a recognition that the core element of the processor is that it acts "on behalf of the controller", and that it is called to implement the instructions given by the controller** at least with regard to the purpose of the processing and the essential elements of the means. Therefore, it is indeed reasonable to limit many obligations, like impact assessment or prior authorization, to controllers only, as suggested by the Council. On the other hand, we remain concerned about the introduction of a vague liability clause, which would only create confusions for controllers, processors and data subjects alike. We are also note an important degree of prescriptiveness in the current proposal, as it puts unnecessary constraints on the contractual freedom of the parties. Examples range from mandating "returning" the data, as opposed to some other existing contractual

practices; to the "use only" provisions in the processor obligations chapter of the Regulation.

Centre for Information Policy Leadership
Hunton & Williams LLP

19 June 2014

A Risk-based Approach to Privacy: Improving Effectiveness in Practice

In January 2014, the Centre for Information Policy Leadership (the Centre) launched a multi-year project on the risk-based approach to privacy: The Privacy Risk Framework Project. This project elaborates on the Centre's earlier project on organisational accountability, particularly in seeking to develop the analytical framework and tools needed to implement certain key aspects of accountability. Specifically, the goals of this project are set forth in the following Project Vision Statement:

Principle-based data privacy laws often leave room for interpretation, leaving it both to organisations to make appropriate decisions on how to implement these principles and to regulators on how to interpret and enforce the law. The Privacy Risk Framework Project aims to bridge the gap between high-level privacy principles on one hand, and compliance on the ground on the other, by developing a methodology for organisations to apply, calibrate and implement abstract privacy obligations based on the actual risks and benefits of the proposed data processing. While certain types of risk assessments are already an integral part of accountable organisations' privacy management programs, they require further development. This project seeks to build consensus on what is meant by privacy risks to individuals (and society) and to create a practical framework to identify, prioritise and mitigate such risks so that principle-based privacy obligations can be implemented appropriately and effectively.

On March 20, 2014, the Centre held a workshop in Paris during which more than 50 privacy experts, industry representatives and regulators discussed their experiences and views with respect to the risk-based approach to privacy, the privacy risk framework and methodology, as well as goals and next steps in this project. This paper, titled "*A Risk-based Approach to Privacy: Improving Effectiveness in Practice*", is a developed version of the earlier discussion paper distributed to the participants of the workshop. It incorporates feedback from the Paris workshop and input received in subsequent consultations with Centre members and project participants.

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?

> "Harm" in this paper is not meant to be a technical term. It simply signifies any damage, injury or negative impact—whether tangible or intangible, economic, non-economic or reputational—to an individual that may flow from the processing of personal data. It extends to any denial of fundamental rights and freedoms. The Privacy Risk Framework Project will explore whether and (if so) how it should also extend to any harms to society at large.

2. At a time when the new information age challenges accepted privacy concepts and practices and strains our limited compliance and enforcement resources, organisations and regulators need to prioritise their activities and find new ways to turn abstract requirements into real and effective privacy protections. In Europe, the notion of data protection as a fundamental human right has been reaffirmed by the European Court of Justice. In other parts of the world, high-level privacy principles continue to be articulated by policy-makers, legislators, courts and commentators. Yet, it is no longer enough—or sufficiently meaningful—to say solely that privacy is a human right and that the laws exist to safeguard "fundamental rights and freedoms", nor that they are confined solely to existing privacy principles or fair information practices. New times call for new clarity and new pragmatism. A "Risk-based Approach to Privacy" can help deliver greater clarity and more effective data protection on the ground.

3. The risk-based approach goes beyond mere compliance with regulatory requirements. It goes to the heart of what responsible and accountable organisations seek to achieve, how they implement privacy requirements on the ground and how they demonstrate compliance. The risk-based approach may also help to clarify and communicate the underlying rationales for regulation.

4. As the pace of technological change outstrips the conventional thinking of law-makers, regulators and businesses, it is suggested that 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 collect, receive, store, use and share on a daily basis. These issues become more pressing as a greater number of companies seek to design, implement and demonstrate accountability through corporate privacy management programs and an ethical approach, often through programs of corporate and social responsibility. Increasingly, businesses, and their executives and boards need reassurances that their corporate programs are effective, and that they deliver required outcomes, both for the organisations themselves and for the individuals they seek to protect.

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 programs and other safeguards? Also, how can it be made easier for non-experts to understand what they should—and should not—be

doing? How can privacy officers effectively communicate "the do's and don'ts" of data privacy to an increasingly disparate audience of technologists, data scientists, privacy engineers and business leaders within their organisations?

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 give businesses more predictability and 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, less burdensome on businesses and individuals and take into account more precisely the risks to individuals and to the well-being of society, but without disenfranchising the individual?

8. The Centre's Risk Project follows up on our pioneering work on accountability over the past five years. The project seeks to answer some of these questions and to explore the benefits of taking a more "Risk-based Approach to Privacy". Specifically, this initial paper sets out issues and key learnings so far, with a first attempt to develop a framework to improve the ability of businesses to understand, identify, assess and manage privacy risks. This framework would also improve organisations' ability to demonstrate to a third party, including a regulator, their "accountability" by enabling them to show specifically how and why they have reached certain data processing decisions.

II. Emerging Thinking

9. A number of headline messages have started to emerge from various workshops and discussions held in the last couple of years on, or around, the scope for a more risk-based approach.[1]

10. In summary, the key messages and findings so far are as follows:

- A risk-based approach is worth exploring for several reasons, all ultimately focused on improving the effectiveness of privacy protections in practice.

- A risk-based approach should largely build on existing and emerging legislative provisions which already require consideration of privacy risks to individuals.

[1] In addition to the Centre's previously mentioned Risk workshop in Paris (*see* p. 1), these included the Centre's Accountability project workshops in Warsaw and Toronto, a session on risk at the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw and an informal workshop sponsored by The Privacy Projects in London. The reports of the "Data Use and Impact Global Workshop" and the "Data Protection Principles for the 21st Century" have both drawn attention to the need for greater focus on the risks attendant on the various uses of data. A risk discussion also features heavily in the May 2014 white paper of the World Economic Forum entitled "Rethinking Personal Data: A New Lens for Strengthening Trust". Further, on May 30, 2014, the Article 29 Data Protection Working Party adopted a "Statement on the role of a risk-based approach in data protection legal frameworks".

- The risk-based approach is not meant to replace or negate existing privacy regulation and data protection principles. The approach and risk framework methodology primarily aim to:

  a) complement the existing laws and regulations and facilitate the application of existing data protection principles and requirements;

  b) help implement the existing legal requirements and privacy principles in a particular context, with greater flexibility and more agility that is required in the new information age, by taking into account the risks to individuals; and

  c) improve the delivery of effective data protection in practice—benefitting individuals and organisations seeking more effective, systematic and demonstrable compliance.

- This means, in particular, providing clearer steers for accountable and responsible organisations that seek to "get it right" by preventing problems, often by going beyond compliance with legal requirements and regulators' expectations. This may be for reputational, commercial or other reasons of enlightened self-interest.

- A risk-based approach has considerable potential to interpret, elaborate and make meaningful requirements and fundamental data protection principles which inevitably are often cast in general terms. Here, it is especially important to meet the growing needs of non-experts in privacy or data protection —engineers, data scientists, clinicians and many others—who need to grapple with these requirements and principles and reflect on the prospective impact of the new technologies and services they are developing.

- While the risk-based approach may be used to calibrate obligations and compliance of organisations, it should not be seen as a dilution of individuals' rights, nor as a means of avoiding legal obligations.

- A risk-based approach is closely linked to the setting of priorities: "Selective to be Effective". It helps organisations and regulators to concentrate on what really matters and to avoid wasting scarce resources on less important or bureaucratic requirements that neither benefit individuals nor better protect their information.

- The primary focus should be on ***significant privacy risks*** for individuals. In other words, in a given situation, the question should be whether there is ***a significant likelihood that an identified threat could lead to a recognised harm with a significant degree of seriousness.***

- There is a particular benefit in developing a common and objective approach to risk management and an objective notion of harm or adverse impact to individuals that are acceptable and useful to as many businesses and regulators as possible.

- A similar approach might be applied to assessing risks and harms to society, although whether organisations can or should assess societal harms may require further consideration.

- Attempts to manage privacy risks should be integrated as closely as possible alongside well-established risk management processes ....

- .... but any approach must be kept as simple as possible and should be meaningful to SMEs (small and medium enterprises) and individuals as well as to large businesses, public bodies and regulators.

- As a risk-based approach will usually take the organisation beyond legal compliance in particular jurisdictions, it could be used as a tool to build and implement a consistent global program focused on the real priorities. More ambitiously, there is scope to improve the prospects for global inter-operability because following a common and consistent methodology to risk assessment would create harmonised practices and outcomes and, in turn, improve trust among regulators and individuals in different jurisdictions. It would also improve the ability of privacy authorities to cooperate on enforcement across borders.

- Any attempt to assess and manage risks in terms of impact on individuals and society would be novel. Hitherto, very few organisations or regulators have taken this as their rationale or motivation. Any structured encouragement for organisations to think in advance about the potentially negative impact of new developments should be welcome.

- Unsurprisingly, there is little agreement on what is meant by the "privacy risks" faced by individuals and society. The identification and classification of privacy risks must be settled before continuing work on how best to address them in a structured way.

- 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**.

III. Threats

11. When assessing threats, it is important to consider a whole lifecycle of information and data processing. Some threats will be visible at the time of collection, but some will emerge later, during the use or disclosure of data. It is important to note that the threats may also change during the lifecycle of information—old threats may disappear and new ones may become prominent.

12. Threats usually arise from processing personal data, which does or could relate to an identifiable individual. As anonymisation, however, becomes less absolute, all forms of data should be seen as capable of presenting privacy risks.

13. A wide approach to the threats arising over the lifecycle of data should therefore include both ***activities*** and ***characteristics***. It is suggested that the following should be considered as the threats arising from data processing:

    - unjustifiable or excessive collection of data;
    - use or storage of inaccurate or outdated data;
    - inappropriate use of data, including:

      a) use of data beyond individuals' reasonable expectations;

      b) unusual use of data beyond societal norms, where any reasonable individual in this context would object; or

      c) unjustifiable inference or decision-making, which the organisation cannot objectively defend;

    - lost or stolen data; and
    - unjustifiable or unauthorised access, transfer, sharing or publishing of data.

14. In each case of the above threats, objective judgments will be needed about the a) likelihood of a threat causing harm to individuals, and b) the severity of that impact if it materialises. This means that the assessment of a threat arising from data processing must always be ***contextual***. In other words, a flexibility is required that recognises context as an important factor in determining the level of threat and its potential to cause harm. In a risk-based environment, it is the ***use*** (including disclosure) of the information that arguably poses the greatest threat and where particular attention must be focused. This also has the advantage of avoiding the familiar practical problems of over-emphasis on collection solely, and of over-reliance on legalistic notice and consent, that result in information overload for individuals. Finally, this approach is also helpful in situations where there is no interface with individuals, or where the data are not collected directly from them.

15. Accordingly, neither information notification to the individual nor consent are by themselves a panacea. A use of personal information may be inappropriate or create significant privacy risks even though that use may have been specified or foreseen. 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 neither "small print" disclosure, nor apparent consent, can, by themselves, justify an "unusual" use.

IV. Harms

16. There are three types of harm[2] that any of the identified threats could present:

    - tangible damage to individuals;

[2] *See* explanation of the term "harm" on page 2.

- intangible distress to individuals; and
- societal.

17. **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.

18. **Intangible distress,** assessed objectively, includes:

    - 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.

19. 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).

20. While risk assessment involves tests of foreseeability, these must be objective descriptors of harm—it is 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. Finally, the test must again be context-driven, although information communicated to the relevant individuals, and any consent they have given, will again be factors.

21. **Societal harm** can arise directly from business activity. But it is more likely 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; and
    - loss of social trust ("who knows what about whom?").

V. A Matrix to Link Threats and Harms

22. Risk assessment and risk management call for judgment, based upon honest, well-informed and justifiable answers to structured questions about threats and harms. A framework is needed to identify, link and prioritise the various types of threat and harm, ideally in a way that can be easily understood by large and small businesses, by public bodies, by regulators and by individuals.

23. The two draft matrices suggested in Annex 1 demonstrate possible ways of how this might be accomplished in practice. They have been designed as a way of putting privacy on corporate risk radars and getting organisations at least to think about the impact of their activities on the individuals with whom they deal and on the wider community. A framework on these premises—using a common referential—could be initially tested in different contexts by different organisations, not least reflecting varying levels of sophistication and risk aversion. The framework might then mature into a standard template that may, in due course, receive some form of regulatory endorsement to signal a commonly agreed upon approach and become attractive for both organisations and regulators.

VI. A Matrix as an Organisational Risk Management Tool

24. It is envisaged that as a new service, product, technology or activity is developed, a business could use a matrix along the lines suggested in Annex 1 to raise questions and structure a series of judgments arising from each of its inter-sections. Each inter-section requires two specific judgments to be made. A numerical scale would add calibration and rigor:

    i. How **likely** could this harm arise from any relevant threat? Can this be sensibly quantified on a numeric scale?

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

25. Both judgments should be informed by as much hard data and evidence as possible, such as the nature and volume of the data, consumer complaints, consumer perception research or 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, including those affecting fundamental rights and freedoms. 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 judgments, 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.

26. Each intersection—How likely? How serious?—is a function of the level of the threat and the likelihood that the threat will cause harm. The key judgment 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 degrees of risk aversion. 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.

27. Where the judgment is made that there is a significant risk—typically as part of an on-going process of risk assessment—appropriate action is then needed to mitigate the risk and implement safeguards to protect individuals from these risks. This might, for example, involve a change of scope, specific safeguards for individuals, or the adoption of a new or improved comprehensive privacy program. A further, post-mitigation, assessment would then be required.

VII. Factoring in the Benefits

28. Not only are some threats to privacy more serious than others, privacy itself is not an absolute value, nor is it the only fundamental right. 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 public and commercial uses of personal information. The benefits may flow directly to the individuals concerned or they may accrue at a more societal level, e.g. medical research, law enforcement or improved living standards.

29. As part of the process of assessing the nature and extent of privacy risks, it is necessary to factor in the corresponding benefits because understanding the benefits can help to mitigate risks. Risk cannot be eliminated entirely; and even where it is judged that significant risks exist or remain, there will be situations wherethe benefits sufficiently outweigh the risks.

30. 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, unless those risks are mitigated and specific safeguards implemented. 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.

31. The accountable business must stand ready to demonstrate how that judgment was reached, producing, as appropriate, the relevant information and evidence upon which it relied.

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

32. Though regulators cannot do everything, their responsibilities and challenges are growing while 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. How should they set their priorities? How, in particular, do they decide which businesses or activities to target for preventative or enforcement intervention?

33. Here is where a risk management matrix may be useful as a tool for regulators. A consensus based on the language and methodology of a matrix could help regulators fix and communicate their own priorities for interpreting and enforcing the rules. This would be welcomed by businesses as it would give them improved predictability and a better idea of where to focus their own risk assessments. At a minimum, the businesses could adopt a "mirror-image" approach in their efforts to avoid regulatory trouble and exceed compliance requirements.

34. One could speculate on various possibilities for a regulator which adopts or endorses a matrix as its starting point:

    - The regulator could signal that it will use that matrix to target industry sectors, particular businesses or activities—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 regulatory attention on situations where a satisfactory exercise has ***not*** been conducted.

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

35. 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, for a regulator to state that, for a particular type of activity, a risk would be significant where the assessment score exceeds a prescribed level.

36. 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 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 especially exposed if the harm in fact materialises. In other situations, as the FTC has shown with imaginative use of consent decrees which impact on privacy programs, a regulator that finds fault with risk assessments is well placed to ensure constructively that its rulings have positive effects in the future.

37. Finally, a common and consistent use of a risk management matrix by regulators in different countries would lead to much needed consistency and even harmonisation of expected outcomes, even in situations where the underlying rules may not be always the same. The potential for the risk-based approach and risk management matrix to be used globally would be a powerful step forward towards global interoperability.

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

38. There is also scope for regulators and courts to use a 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.

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

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

X. Implications for Lawmakers

41. This paper focuses on a risk-based approach as a means of implementing and calibrating existing legal requirements and compliance in practice, to make them more effective. As such, the paper advocates adopting a risk-based approach 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 some more rigid and prescriptive, which may be judged as ineffective. This is not, however, the focus of this paper.

XI. Issues for Further Consideration

42. The above discussion raises a number of issues and questions that require further consideration as a part of the Centre's Privacy Risk Framework Project:

- Any methodology for risk assessment needs to have an agreed definition of "risk". Do we mean risk to privacy, or risk to personal data protection? Do we mean risk to individuals' other rights and freedoms?

- Can and should organisations consider societal harms in their risk assessments?

- Who decides what is "risky" and what is "harm"? When and how do they decide? Are there categories of processing that are considered *per se* risky or that are always considered harmful? Can the potential risks and harms associated with certain data processing be assessed by the controller without inserting too much subjectivity? If so, how do we ensure sufficient legal certainty, both for the organisation and for the individuals?

- What is the role of the affected individual in any risk assessment? How much and what kind of participation or transparency is required?
    - Do individuals need to be told about or allowed to participate in the risk assessment? Should companies share the outcomes of any risk assessment with individuals?
    - Should individuals be given an opportunity to object to the outcomes of a risk assessment? Should they have a right to object to processing despite a contrary risk assessment?
    - What is the role of consent in this context? Does consent trump risk assessment or vice-versa?
- What do we know about individuals' perception of risk and harm to themselves? Are there surveys and market research, and is there sufficient existing knowledge in the business community? What are other ways to obtain relevant information on this topic? Can we monitor the reaction of individuals over time? Can we use social media as a channel for such monitoring?
- We should not replace one bureaucracy with another. The proposed EU Data Protection Regulation aims to reduce bureaucracy. Would an elaborate and documented case-by-case risk assessment for every processing of personal data be impractical as well as cost and labor intensive? On the other hand, given that many privacy laws (including the EU Directive and the proposed EU Regulation) already require risk assessments in many instances—such as in the "legitimate interest" balancing test under the current EU Directive—a widely agreed upon risk assessment methodology may improve efficiency and reduce administrative burdens.
- Will the risk-based privacy framework be scalable for SMEs, who are some of the main drivers of innovation and new technologies and services?
- Companies already routinely assess privacy risks to themselves, such as non-compliance, reputational and litigation risks. How do these types of risk assessments relate to those that focus on risks to individuals, particularly where these may not overlap? How does an organisation integrate both risk assessments seamlessly?
- Risk assessment is an integral part of organisational accountability. How, exactly, will a risk-assessment methodology help demonstrate accountability and compliance with applicable legal requirements?
- What is the role of regulators *vis-à-vis* an organisation's decision to process data based on a risk analysis? The risk-based approach must not undermine a regulator's ability to challenge the validity of risk-analysis outcome. Can risk analysis outcomes be challenged even in the absence of harm?
- What is the role of technology and technologists in developing and implementing risk-based solutions to privacy protection?

- Any risk methodology and framework must be capable of being exported and used by technologists, data scientists, data anthropologists, engineers and many others who, normally, will not have an intuitive or developed understanding of privacy issues. How can we socialise the risk-analysis concept more broadly and work with nonprivacy practitioners to that end?

- Data ethics is a new discipline. How does an ethical decision-making model fit or should be reflected in any risk assessment methodology?

XII. Next Steps

43. The Centre will continue work towards a comprehensive privacy risk framework, drawing on the expertise of its members, project participants and privacy experts, including from academia and the regulators community. It will also seek to collaborate with other organisations interested in the risk-based approach to privacy.

44. Future work on the project may include:

- developing additional discussion papers based on further study of all issues identified in this paper or raised by the risk-based approach to privacy;

- holding further workshops to receive input and discuss our learnings;

- examining existing risk analysis practices to inform the development of the privacy risk framework;

- taking stock of current laws and regulatory schemes that require and incorporate risk analysis today;

- identifying new areas of potential use for the risk-based approach, such as in response to new and evolving privacy threats in the modern data economy;

- refining and developing the practical tools associated with risk analysis, such as the risk matrix, and thinking about practical implementation of the risk-based approach;

- undertaking case studies on applying the risk methodology under development in the present project, including the risk management matrix, to various real-life scenarios, such as in activities involving: health data, big data, anonymised/pseudonymised data; new products and services, etc.;

- considering individual participation and transparency issues;

- examining the potential uses of the risk-based approach by the different privacy stakeholders—organisations, regulators, and law and policy makers; and

- studying the potential of the risk-based approach to enable global interoperability.

To be evaluated

Version 1.0 06/2014	DRAFT - Risk Matrix									
	Unjustifiable Collection			Inappropriate Use Inaccuracies Not expected by individual Viewed as Unreasonable Viewed as Unjustified			Security Breach Lost Data Stolen Data Access Violation			Aggregate
Risks	**Likely**	**Serious**	**Score**	**Likely**	**Serious**	**Score**	**Likely**	**Serious**	**Score**	**Risk Rank**
Tangible Harm										
Bodily Harm	0	0	0	0	0	0	0	0	0	**0**
Loss of liberty or freedom	0	0	0	0	0	0	0	0	0	**0**
Financial loss	0	0	0	0	0	0	0	0	0	**0**
Other tangible loss	0	0	0	0	0	0	0	0	0	**0**
Intangible Distress										
Excessive surveillance	0	0	0	0	0	0	0	0	0	**0**
Suppress free speech	0	0	0	0	0	0	0	0	0	**0**
Suppress associations	0	0	0	0	0	0	0	0	0	**0**
Embarrassment/anxiety	0	0	0	0	0	0	0	0	0	**0**
Discrimination	0	0	0	0	0	0	0	0	0	**0**
Excessive state power	0	0	0	0	0	0	0	0	0	**0**
Loss of social trust	0	0	0	0	0	0	0	0	0	**0**

ANNEX I

Legend:
Rank 'Likely' from 10 (high) to 1 (low) based on the highest score for any component
Rank 'Serious' from 10 (high) to 1 (low) based on the highest score for any component

Aggregate Risk Rank:
Highest score is 300
Lowest score is 0

To be evaluated

Draft Risk Matrix

Proposed Processing:		THREATS											
		Unjustifiable Collection of Data		Inappropriate Use of Data						In Wrong Hands			
				Storage or use of inaccurate or outdated data		Use of data beyond individuals' reasonable expectations		Unusual use of data beyond societal norms, where any reasonable individual in this context would object		Unjustifiable inference or decision-making, that the organisation cannot objectively defend		Lost or stolen data		Data that is unjustifiably accessed, transferred, shared or published	
HARMS	**Tangible Harm**														
	Bodily harm	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Loss of liberty or freedom of movement	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX I

Draft Risk Matrix

	Damage to earning power	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?			
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?			
	Other significant damage to economic interests	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?			
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?			
	Intangible Distress																
	Detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?			
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?			
	Chilling effect on freedom of speech, association, etc.	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?			
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?			

ANNEX I

To be evaluated

Draft Risk Matrix

ANNEX I

	Reputational harm	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Personal, family, workplace or social fear, embarrassment or anxiety	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Unacceptable intrusion into private life	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Discrimination or stigmatisation	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

To be evaluated

Draft Risk Matrix

ANNEX I

	Societal Harm													
	Damage to democratic institutions (e.g. excessive state or police power	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Loss of social trust (Who knows what about whom?)	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

Annex 2: 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 (LA-IPPC) and Local Authority Pollution Prevention and Control (LAPPC) Risk Methodology.