Centre for
Information
Policy
Leadership
Hunton & Williams LLP

THREE SOLUTIONS FOR PROTECTING PRIVACY IN A WORLD OF BIG DATA

December 2015

The world of big data demands new and innovative solutions that simultaneously enable benefits from data-driven products and services and the protection of individuals and their personal information. This is a task facing all governments, regulators and business leaders as they devise appropriate policies, rules and practices. Without new solutions, we will not be able to realise the critical societal objectives of fostering a sustainable data-driven economy and digitally enabled society and protecting privacy. Any new solutions must be able to maximise each of these goals. Accomplishing this will require creativity and the will to re-think our traditional approaches to information management and privacy regulation. But the beginnings of the necessary solutions and new tools are already emerging. Once they are further developed and recognised, organisations that implement them should be permitted to engage in more flexible yet responsible data uses that enable the modern information age.

The Centre for Information Policy Leadership (CIPL) is working on a series of three white papers proposing three sets of solutions for protecting privacy in the modern information age of big data. Drafts of two of these papers are available at www.informationpolicycentre.com. The third discussion paper, as well as final versions of all three papers, will be released at a later date.

In its three papers, CIPL is proposing the following three solutions to the pressing issues identified above:

      (1) enhanced organisational accountability;
      (2) improved privacy risk management; and
      (3) new interpretation of core privacy principles and concepts.

The concept of organisational accountability must evolve into an **"enhanced accountability"** by further developing core elements of accountability, such a risk management and transparency, and adding additional elements and considerations, such as operationalising the principle of fair processing and data ethics. This enhanced accountability will herald an era of organisational digital responsibility and a data protection framework for contexts where express consent and granular individual control about specific data processing activities are not possible, such as in certain big-data-related contexts. It will help create sustainable virtuous data cycles between individuals, society and organisations where organisations are stepping up with responsible data management practices, individuals feel adequately empowered and confident in the modern digital environment, and society at large benefits from data driven innovation, products and services.

Privacy risk management, a core element of organisational accountability, has been a missing link in discussions on big data. It must not only be refined and further developed, but it must become the foundation on which responsible decisions on big data applications can be made by taking into account both the benefits and privacy risks / harms to individuals and implementing mitigations to reduce these harms. The work on this has begun in various corners but is far from complete. It will require an international collaborative effort by regulators, industry, civil society and academics to develop such a framework, based on a true science of data protection.

Finally, the rapid move towards an information society based on big data, the IoT, cloud computing and machine learning, requires us to be creative and innovate in the way we **interpret and apply long-standing data protection principles** and concepts, such as notice, consent and purpose specification and the definition of personal data. In this way we will ensure they remain technology neutral and will stand the test of time in an ever-changing technological and digital environment.