WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Bart van der Sloot
Sascha van Schendel

International and comparative legal study on Big Data

WORKING PAPER 20

International and comparative legal study on Big Data

This series consists of 'Working Papers' produced for the WRR that it regards as sufficiently significant and valuable to merit web publishing. The views and opinions expressed in these papers are those of the authors. A listing of all Working Papers can be found at www.wrr.nl.

The Netherlands Scientific Council for Government Policy
Buitenhof 34
PO Box 20004
2500 EA The Hague, The Netherlands
Phone +31 (0)70 356 46 00
Fax +31 (0)70 3564685
E-mail info@wrr.nl
Website www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

International and comparative legal study on Big Data

Bart van der Sloot & Sascha van Schendel

All publications of the The Netherlands Scientific Council for Government Policy (WRR) are available at www.wrr.nl.

Cover and paper design: Textcetera, Den Haag
Cover image: Textcetera, Den Haag
Working Paper number 20

ISBN 978-94-90186-29-6

WRR, The Hague 2016

INHOUD

PREFACE

WRR Working Paper 20 was written as part of the project 'Big Data, Privacy and Security', undertaken by the Netherlands Scientific Council for Government Policy (WRR) to investigate the consequences of the use of Big Data in the domain of security.

This background study, entitled *International and Comparative Legal Study on Big Data*, was written by Bart van der Sloot and Sacha van Schendel. Many countries experiment with Big Data processes, which are almost by definition transnational. The first part of the study is a quick scan of the Big Data policies, legislation and regulations in Australia, Brazil, China, France, Germany, India, Israel, Japan, South-Africa, the United Kingdom and the United States. The second part presents the findings of a survey among Data Protection Authorities (DPAs) in Europe. Both parts of the study focus on the relations between Big Data, security and privacy.

LLM. MPhil Bart van der Sloot is a researcher and doctoral candidate at the Institute for Information Law at the University of Amsterdam. During 2014 and 2015, he participated in the 'Big Data, Privacy and Security' project of the Netherlands Scientific Council for Government Policy. Sacha van Schendel (LLS), a Master's student of Law & Technology at Tilburg University, worked as a trainee in this project.

Responsibility for the information and views set out in this study lies entirely with the authors.

Prof. dr. André Knottnerus
Chairman WRR

Dr. Frans Brom
Secretary WRR

1 INTRODUCTION

1.1 BACKGROUND

The Dutch Minister of Security and Justice, on behalf of the Dutch government, asked The Scientific Council for Government Policy (WRR) to produce a report on the use of Big Data, particularly in relation to national security, including its effect on the right to privacy. The WRR is an independent advisory body to the government. Its role is to inform and advise the government on issues that are of significant importance for society. The opinions of the WRR are cross-sectoral, cross-departmental and multi-disciplinary. They are focused on the direction of government policy in the longer term.

In his request, the Minister formulated four main questions. The first was whether a clearer distinction should be drawn between access to and use of information in Big Data processes; this question was partly inspired by the transnational nature of many data processing activities. In particular, the Minister asked whether the mere collection and storage of personal data, without the data being analysed or used, should be limited by data protection legislation – this question should be answered in the light of the fact that in Big Data processes, the possibility cannot be ruled out that non-identifying data may become personal data at a later stage. This gives rise to the question of how great a role the state should play in the Big Data era in ensuring that the use of Big Data for the promotion of security meets relevant standards, for example in relation to purpose limitation and data minimization. The Minister also wanted to know whether – and if so how – these principles can still be maintained.

The second key question concerns the use of Big Data processes and techniques such as profiling and data mining. In particular, the Minister wished to ascertain how these techniques can be used in a transparent manner and how adequate checks and balances can be formulated to allow these techniques to be used safely and carefully.

Thirdly, the Minister referred to the emergence of quantum computing and asked whether encryption and anonymity can still be guaranteed in the future. In his fourth and final question, the Minister asked how the autonomy of citizens can be ensured in Big Data processes. This relates to the question of whether a focus on informed consent is still tenable, what possibilities citizens have for effective control over their data, what responsibility citizens have to contribute to the quality of the data in databases and, more generally, how the quality of the information can be maintained.

Since Big Data processes are almost by definition transnational, and since many other countries have gained more and wider experience in the use and regulation of Big Data processes, in preparing for its advisory report to the government, the WRR decided to carry out an indicative study of the laws and customs surrounding Big Data in countries outside the Netherlands. This study consisted of a quick scan of developments in selected countries and the responses to the survey sent to a number of Data Protection Authorities (DPAs) in Europe. As it was intended to serve as a preparatory stage for the WRR report to the government, the study aimed to cover a wide range of possibilities, approaches and applications of Big Data. It should be noted that this study was not exhaustive and was expressly intended as an indicative study.

1.2 RESEARCH AND RESEARCH METHODOLOGY

The research presented in this report was conducted in two phases. The first phase involved desk research and looked at Big Data policies, legislation and regulation in a number of countries. Second, a questionnaire was sent to several European DPAs. In the light of the request by the Minister, the core of both parts of the research comprised the relationship between Big Data, security and privacy.

The desk research examined eleven countries. These countries were selected on the basis of three criteria. The first was global coverage – the research sought to be as representative as possible to provide a full picture of global developments in relation to Big Data, which is by nature an international phenomenon. Therefore, at least one country from each continent (with the exception of Antarctica) was examined. The second criterion was an estimation of the potential value of the expected outcomes of the research – some countries are more innovative and ambitious than others in terms of technological developments such as Big Data. Thirdly, the role a country plays in international politics was taken into account; on that basis, China rather than South Korea was studied, even though the latter country is often in the forefront of technological developments. Based on these three criteria Australia, Brazil, China, France, Germany, India, Israel, Japan, South Africa, the United Kingdom and the United States were selected. The desk research focussed on two issues in particular. The first was, government policy decisions and initiatives on aspects such as using Big Data itself or stimulating the use of Big Data in the private sector either through financial support or by engaging in partnerships. Second, research was carried out on legislation and case law revolving around Big Data in the selected countries; relevant rulings of local DPAs are also discussed briefly. It should again be noted that this study is not exhaustive – there is undoubtedly a myriad of relevant laws, court cases and DPA reports that are not discussed here.

In studying the eleven countries, almost exclusive use was made of official sources, especially government websites. The reason for this is that it is often difficult to establish the reliability of foreign sources. This choice does however imply that this report mainly presents a picture of the governmental view of Big Data and of governmental regulation. Criticism of those initiatives and autonomous processes in the private sector remain largely undiscussed. This bias was accepted as a trade-off in order to guarantee the reliability of the sources studied. When discussing Israel, however, use was made of online newspaper articles from Israeli news sources and a published online interview. This is stated explicitly in the text and in the citation. The information from these sources was not available on government websites, but was nonetheless considered essential.

Publications on government websites and in press releases about new initiatives were selected by using terms related to Big Data, both in the official language of the country concerned and in English, such as 'data mining', 'data analytics', 'data projects', 'Big Data initiatives', etc. Several countries have a Ministry of Science and Technology or similar ministry. Those ministries were taken as the starting point of the research in those countries. General search engines were also used to scan government initiatives related to Big Data, by limiting the search to the national public domain of the country concerned. For case law and legislation, the official national search engines and general search engines were used. The search terms entered here were related to Big Data, privacy and data protection, such as 'data protection', 'privacy', 'surveillance', etc. This process yielded a list of government initiatives, legislation and relevant jurisprudence. The sources consulted and used are listed in this report.

A relatively short and simple questionnaire was designed for the survey, so as to increase the potential response of the DPAs. The accompanying email, as well as the introduction to the survey, briefly explained the goal of the survey. The accompanying email may be found as an appendix at the end of this report. The survey comprised six questions:

1. Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)
2. Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)
3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)
4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)
6. Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)

The DPAs in all 28 EU Member States were emailed with a request to complete the survey. Requests were also sent to the DPAs in three non-EU countries, namely Norway, Serbia and Switzerland, because a short preliminary study had shown that they might have specific expertise in relation to Big Data. DPAs that did not respond within the period specified in the initial request were sent a reminder; those that did not respond to this mail either were sent a final reminder. DPAs that did not respond were subsequently left out of this study. In most cases, the questionnaire was sent to the general contact address as posted on DPA's website. However, since the French website lists no general email address, personal contacts were used to email two specific employees of the CNIL. For three other DPAs (Germany, the Netherlands and Norway), in addition to an email to the general email address an email was also sent to a specific individual employee. For other DPAs, either no such personal contacts existed or they existed but it was not necessary to use them because a response had been received. Eventually, of the 31 DPAs included in the survey, 18 responded: Austria, Belgium, Croatia, Denmark, Estonia, Finland, France, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Slovakia, Slovenia, Sweden and the United Kingdom. Some of these were negative responses, stating that the DPA in question would not participate in the study. We nonetheless decided to include these emails, because they reflect the general approach of the DPA in question to Big Data. For example, the Austrian DPA did not wish to participate in the survey as it had not yet encountered any issues relating to Big Data and because there was no specific regulation in Austria for Big Data.

1.3 STRUCTURE OF THE REPORT

This report consists of three parts. Chapter 3 describes the desk research that was carried out with respect to the eleven selected countries. This chapter is primarily factual and descriptive, largely ignoring normative questions and critical reflections and serving mainly to provide background. It is divided into eleven sections, one on each country. These sections are each further divided into two subsections, one concerning government policies and initiatives, and the other focusing on relevant laws and case law. Section 12 of chapter 3 contains a list of sources consulted. Chapter 4 contains the responses of the 18 DPAs contacted. These have simply been copied, without further explanation or interpretation. The invitation email sent to the DPAs is included at the end of the chapter, as well as the lists of addresses used.

Chapter 2 contains an analysis and interpretation of the data presented in chapters 3 and 4. As this research was aimed in particular at sketching a broad range of possible (regulatory) approaches for the Dutch regulator, ten issues/questions are discussed in more detail: (1) What is the definition of Big Data? (2) Is Big Data an independent phenomenon? (3) Big Data: fact or fiction? (4) What is the scope of Big Data? (5) What are the opportunities for Big Data? (6) What are the dangers of Big Data? (7) Are the current laws and regulations applicable to Big Data? (8) Is there a need for new legislation for Big Data? (9) What concept should be central to Big Data regulation? (10) How should the responsibilities be distributed? These questions are partly based on those asked in the survey and partly follow from the desk research. Additional questions have been added in order to present the most interesting findings from both the desk research and the survey in an orderly fashion.

2 TEN QUESTIONS CONCERNING THE REGULATION OF BIG DATA

2.1 WHAT IS THE DEFINITION OF BIG DATA?

The first choice when it comes to regulating Big Data is to determine a definition and delineation of Big Data. The definition and delineation clearly influence the way in which it is perceived, what the risks and potential benefits are, whether new legislation is considered necessary, etc. This study shows that a large number of definitions and concepts are used, which vary in width and scope.

Four frequently cited definitions are given below:

- the *Article 29 Working Party* (Working Party 29) gives a description of this phenomenon in a report from 2013. "Big Data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics100) using computer algorithms. Big Data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals."[1];
- the *International Working Group on Data Protection in Telecommunications* builds on that definition: "Big Data is a term which refers to the enormous increase in access to and automated use of information. It refers to the gigantic amounts of digital data controlled by companies, authorities and other large organizations which are subjected to extensive analysis based on the use of algorithms. Big Data may be used to identify general trends and correlations, but it can also be used such that it affects individuals directly."[2];
- the *European Data Protection Supervisor* (EDPS) suggests on its website: "Big Data means large amounts of different types of data produced at high speed from multiple sources, whose handling and analysis require new and more powerful processors and algorithms. Not all of these data are personal, but many players in the digital economy increasingly rely on the large scale collection of and trade in personal information. As well as benefits, these growing markets pose specific risks to individual's rights to privacy and to data protection."[3];
- the *Gartner Report* focusses on three matters when describing Big Data: increasing volume (amount of data), velocity (speed of data processing), and variety (range of data types and sources). This is also called the 3V model or 3V theory.[4]

The desk research also showed that a number of countries apply their own definition of Big Data. Two of the more prominent definitions are those used in Germany and the United States:

– in Germany, Big Data is defined as "*das Synonym für den intelligenten Umgang mit solchen großen oder auch heterogenen Datenmengen"* (synonymous with the intelligent use of large or heterogeneous datasets);
– the Podesta Report (United States) builds on the Gartner definition: "There are many definitions of 'Big Data' which may differ depending on whether you are a computer scientist, a financial analyst, or an entrepreneur pitching an idea to a venture capitalist. Most definitions reflect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data. In other words, 'data is now available faster, has greater coverage and scope, and includes new types of observations and measurements that previously were not available.' More precisely, Big Datasets are 'large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future.'"

Finally, several DPAs also gave their own definition of Big Data when completing the survey. The most important ones are:

– the Estonian DPA described Big Data as "collected and processed open datasets, which are defined by quantity, plurality of data formats and data origination and processing speed.";
– the French DPA suggests that: "In August 2014, a definition of the term 'Big Data' was adopted by the French General Commission on terminology and neology (*Commission générale de terminologie et de néologie*). The official translation of this term in French is '*mégadonnées*' and the definition is "data, structured or otherwise, whose very large volume require appropriate analytical tools.";
– the DPA of Luxembourg gives the following definition: "Big Data stems from the collection of large structured or unstructured datasets, the possible merger of such datasets as well as the analysis of these data through computer algorithms. It usually refers to datasets which cannot be stored, managed and analysed with average technical means due to their size. Personal data can also be a part of Big Data but Big Data usually extends beyond that, containing aggregated and anonymous data.";
– the DPA from the Netherlands argues: "Big Data is all about collecting as much information as possible; storing it in ever larger databases; combining data that is collected for different purposes; and applying algorithms to find correlations and unexpected new information.";

– the DPA from Slovenia suggests: "Big Data is a broad term for processing of large amounts of different types of data, including personal data, acquired from multiple sources in various formats. Big Data revolves around predictive analytics – acquiring new knowledge from large data sets which requires new and more powerful processing applications.";
– the Swedish DPA discusses Big Data and holds that "the concept is used for situations where large amounts of data are gathered in order to be made available for different purposes, not always precisely determined in advance.";
– the DPA from the United Kingdom elaborates on the 3V model and suggests that what is essential to Big Data is "repurposing data; using algorithms to find correlations in datasets rather than constructing traditional queries; and bringing together data from a variety of sources, including structured and unstructured data."

It can be seen from this list of definitions that a number of components are regularly mentioned. Broadly, they relate to three states of Big Data processing, namely the collection, analysis and use of data. When it comes to collecting data, Big Data is about collecting large amounts of data (volume) from varied (variety) and often unstructured data sources. With regard to analysing the collected data, Big Data revolves around the speed (velocity) of the analyses and the use of certain instruments such as algorithms, machine learning and statistic correlations. The results are often predictive in nature (predictive analytics) and are formulated at a general or group level. The results are usually applied by means of profiling. Many of the definitions contain some of these concepts; none of them mention all of them. Consequently, none of these elements should be seen as essential – that is, if one or more of these elements do not apply, it does not follow that the phenomenon being studied is not Big Data. Rather, these elements should be seen as parameters; if none of the elements apply, the phenomenon is definitely not Big Data; if all the elements apply, the phenomenon being studied definitely is Big Data.

2.2 IS BIG DATA AN INDEPENDENT PHENOMENON?

The above overview of definitions already shows that Big Data should not be seen as an isolated phenomenon. It is a new phenomenon which by its nature is strongly connected to a number of technical, social and legal developments. This conclusion is supported by the desk research, which also found that Big Data is intertwined with several other terms. A number of these concepts will be mentioned briefly here.

Open Data

Lots of Big Data initiatives are linked to Open Data. As the name suggests, Open Data is the idea that (government) data should be placed in the public domain. Traditionally, it has been linked to efforts to increase transparency in the public sector and give more control over government power to media and/or citizens. In particular, the Estonian DPA is very explicit about the relationship between Open Data and Big Data. Big Data is defined as "collected and processed open datasets, which are defined by quantity, plurality of data formats and data origination and processing speed". The desk research also shows a clear link between the two concepts in some countries, such as Australia, France, Japan and the United Kingdom.

Re-Use

Linked to Open Data is the idea of re-use of data. Yet there is one important difference. While Open Data has traditionally been concerned with transparency of and control over government power, the re-use of (government) data is specifically intended to promote the commercial exploitation of the data by businesses and private parties. The re-use of Public Sector Information is fostered through the PSI Directive of the European Union.[5] More generally, re-use refers to the idea that data can be used for a purpose other than that for which they it was originally collected. The Norwegian DPA, for example, has suggested a relationship between Big Data and the re-use of data. The Norwegians use the definition of the Working Group 29, "but also add what in our opinion is the key aspect of Big Data, namely that it is about the compilation of data from several different sources. In other words, it is not just the volume in itself that is of interest, but the fact that secondary value is derived from the data through reuse and analysis." The desk research also showed a link between the two concepts. In France, for example, Big Data is primarily seen as a phenomenon based on the re-use of data for new purposes and on the combination of different data and datasets.

Internet of Things

The term 'Internet of Things' refers to the idea that more and more things are connected to the Internet – cars, lampposts, refrigerators, clothing, or all kinds of other objects. This opens the way for the development of smart devices – for example, a refrigerator that records when the milk has run out and automatically reorders. By fitting all objects with a sensor, large quantities of data can be collected. As a consequence, Big Data and the Internet of Things are often mentioned in the same breath. An example is the DPA of the United Kingdom, which notes "that Big Data may involve not only data that has been consciously provided by data subjects, but also personal data that has been observed (e.g. from Internet of Things devices), derived from other data or inferred through analytics and profiling."

Smart

Because of the applications of the Internet of Things and the constantly communicating devices and computers, the development of smart products and services has spiralled. Examples of such developments are smart cities, smart devices and smart robots. Our desk research indicates that a number of countries – for example the United States and the United Kingdom – make a link between such developments and Big Data systems. The Luxembourg DPA also emphasizes the relationship with smart systems, such as smart metering. "At a national level, a system of smart metering for electricity and gas has been launched. The project is however still in a testing phase. - The CNPD has not issued any decisions, reports or opinions that are directly dealing with Big Data. The Commission has however issued an opinion in a related matter, namely with regard to the problematic raised by smart metering. In 2013, the CNPD issued an opinion on smart metering. The main argument of the opinion highlights the necessity to clearly define the purposes of the data processing as well as the retention periods of the data related to smart metering."

Profiling

A term that is often associated with Big Data and is sometimes included as part of the definition of Big Data is 'profiling'. As increasingly large datasets are collected and analysed, the conclusions and correlations are mostly formulated at a general or group level. This mainly involves statistical correlations, sometimes of a predictive nature. Germany is developing new laws on profiling and a number of DPAs emphasize the relationship between Big Data and profiling, for example the DPAs of the Netherlands, Slovenia, the UK and Belgium. The latter argues: "The general data protection law applies, and we expect that de new data protection regulation will be able to provide a partial answer (profiling) to Big Data issues (legal interpretation of the EU legal framework)."

Algorithms

A term that recurs in very many definitions of Big Data is 'algorithms'. This applies to the definition by Working Party 29, the EDPS and a number of DPAs such as those of Luxembourg, the Netherlands and the UK. A number of countries also have a special focus on algorithms. In Australia, a 'Program Protocol' applies to certain cases – a report may be issued which contains the following elements: a description of the data; a specification of each matching algorithm; the anticipated risks and how they will be addressed; the means of checking the integrity of the data; and the security measures used.

Cloud computing

Cloud computing is also often associated with Big Data processes. In China and Israel, especially, the two terms are often connected to each other. For example, the Chinese vice-premier stressed that the government wants to make better use of

technologies such as Big Data and cloud computing to support innovation; according to the Prime Minister, mobile Internet, cloud computing, Big Data and the Internet of Things are integrated with production processes, and will thus be an important engine for economic growth. In Israel, the plan is for the army to have a cloud where all data is stored in 2015 – there is even talk of a 'combat computing cloud', a data centre that will make different tools available to forces on the ground. Some DPAs also suggest a relationship between cloud computing and Big Data; the Slovenian DPA, for example, states that "new concepts and paradigms, such as cloud computing or Big Data should not lower or undermine the current levels of data protection as a fundamental human right."

There are other terms that are often mentioned in connection with Big Data, such as machine learning, commodification of data, datafication, securitization and risk society. It goes beyond the scope of this report to discuss all these terms in depth. It is important to note that Big Data should be primarily viewed in its interrelationship and in conjunction with other phenomena. Big Data is a part of and in a certain sense the umbrella term for many of the technological and societal developments that are already taking place. This needs to be taken into account when regulating Big Data. It seems advisable for regulators to take a holistic approach to the regulation of Big Data and related phenomena.

2.3 BIG DATA: FACT OR FICTION?

There is still no clarity about the extent to which Big Data processes are already being used in practice. The reactions of a number of DPAs seem to suggest that Big Data is not yet an established practice. For example, the Austrian DPA declined to participate in the survey because it had encountered few if any Big Data processes; similar reactions were received from the DPAs of Latvia, Lithuania and Slovakia. The Belgian DPA suggests that there is currently a lack of clarity about Big Data and refers to Gartner's hype cycle.[6] It also adds: "Most Belgian projects seem to be still in a pilot phase and the visibility of Big Data in practice is still low."

However, other DPA responses show a different picture – they confirm that Big Data is a major trend, and that Big Data is playing an increasingly significant role. Some DPAs, such as Norway, have written a special report on the regulation of Big Data practices. The United Kingdom DPA has also issued a discussion paper on this topic. Furthermore, it emerged from the desk research that projects are under way in most countries that are connected to Big Data, although it should be noted that a fairly broad approach was taken in the desk research to what qualified as 'Big Data'.

The picture that emerges from all of the foregoing is one in which Big Data plays a minor role in most countries at present but is set to become increasingly important. Big Data should therefore not be seen as either an actual practice or as a fiction, a hype that will blow over, but rather as a trend that will play a major role in five years' time and will have a significant impact on the government sector, on business and on citizens' everyday life in the near future. This study mainly focuses on the attitude of governments and DPAs towards Big Data. What is clear from the desk research is that in most countries the government feels it is missing out on this important trend. While industry is investing billions in Big Data projects, many governments are – or feel they are – lagging behind. This is why many governments are now beginning to invest heavily in Big Data projects.

To give a few examples:

– In the United States, more than $200 million was reserved for a research and development initiative for Big Data, to be spent by six federal government departments;[7] the army invested the most in Big Data projects, namely $250 million;[8] $160 million was invested in a smart cities initiative, investing in 25 collaborative ventures focused on data usage.[9]
– In the United Kingdom, £159 million was spent on high-quality computer and network infrastructure,[10] there was £189 million in investments to support Big Data and to develop the UK's data infrastructure,[11] and £10.7 million will be spent on a centre for Big Data and space technologies.[12] In addition, £42 million will be spent on the Alan Turing Institute for the analysis and application of Big Data, £50 million will be set aside for the 'Digital Catapult', where researchers and industry are brought together to come up with innovative products;[13] and lastly, in February 2014 the Minister of Universities and Science announced a new investment of £73 million in Big Data. This money will be used for bioinformatics, open data projects, research and the use of environmental data.[14]
– In South Africa, the government has invested 2 billion South African Rand, approximately €126.8 million, in the Square Kilometre Array (SKA) project, which revolves around very large datasets;[15]
– In France, seven research projects related to Big Data were awarded a total of €11.5 million.[16]
– In Germany, the Ministry of Education and Research invested €10 million in Big Data research institutes and €20 million in Big Data research;[17] this Ministry will also invest approximately €6.4 million in Abida , a four-year interdisciplinary research project focusing on the social and economic impact of large data sets.[18]

These are just a few examples of what is being spent by the governmental sector. In the private sector, a multiple of these sums is being spent on Big Data projects. The expectation is that these Big Data projects will develop over the next five or

ten years. Only then will many of the effects of Big Data become apparent. Consequently, when designing Big Data regulations, the government should develop future-proof policies that follow and where possible anticipate this trend. If regulators only begin to regulate this phenomenon five or ten years from now, many of the projects will have already started. The negative impact will already have materialized and it will be difficult to adjust and alter projects and developments that have already flourished. It should also be remembered that good, clear regulation can contribute to innovation and the use of Big Data. Since the current framework applying for new Big Data projects is not always clear, some government agencies and private companies are reluctant to use new technologies for fear of violating the law. New regulation could provide more clarity.

2.4 WHAT IS THE SCOPE OF BIG DATA?

This study, and especially the desk research, shows that Big Data projects are initiated for very different purposes. In Brazil, for example, the Data Viva system was initially used mainly for the formulation of economic policy. In addition, the police in Sao Paulo use a system (Detecta) that is based on Big Data technology. Detecta is an intelligent system for monitoring crime. In the United Kingdom, too, Big Data is used to fight crime. The POSTnote about Big Data and crime and safety provides an example of the use of Big Data by the police. Software has been developed as part of a pilot to predict the location of burglaries, and two British police forces use software developed for predictive policing to predict the locations of crimes. The British tax and customs authority, HMRC, also uses a Big Data system, 'Connect', in which all the data held is aggregated and analysed. This Big Data system is used to detect tax fraud and tax evasion, and is said to have led to the recovery of £2.6 billion since April 2013. The system displays relevant information in searches that is otherwise difficult to find, allows complex analyses to be performed on the development of multiple datasets simultaneously and enables profiles to be constructed which can help uncover patterns that may indicate particular crimes.

In some countries, Big Data is primarily seen as a means for the government to increase its own service to citizens; prominent examples are Australia and China. Reference can also be made in this connection to the Aadhaar project that has been developed and carried out by the 'Unique Identification Authority' of India and which involves the collection of biometric and demographic data on residents of India. One of the uses of Aadhaar is 'micropayments', a means of identification which should help improve access to financial services for people living in rural areas. The identification number makes it possible to identify people in remote regions from a long distance and also reduces costs through economies of scale, making it easier for poorer people to obtain financial services. Other sectors where Aadhaar provides solutions include demographic planning, paying security social

benefits and improving the identification of beneficiaries by eliminating duplicate identities. Government administrative processes should become more efficient because the authorities now have access to all relevant information at a glance.

Several countries see Big Data mainly as a phenomenon that can help the private economy. Germany, for example, has launched a funding initiative to support the competitiveness of IT companies, and France also feels that Big Data is set to take off, especially in the private sector, through the growth of IT companies and start-ups which help to stimulate the economy and create jobs. There are also countries, such as Japan, Germany and the UK, where Big Data is approached primarily in relation to scientific research and innovation. Israel, finally, is unique in that it also uses new technological systems for facilitating the activities of the army. It also has to be borne in mind that many intelligence services are involved with Big Data-like projects; however, often little is known about these projects, other than what has been leaked by whistleblowers.

The picture that emerges from our research is that Big Data could be used in almost every sector and for almost any task. Generally, the use of Big Data can be divided into three types. Firstly, the use of Big Data for specific government tasks – examples include the use of Big Data by intelligence services, the police, tax authorities and other public bodies, for example in the context of formulating economic policies. Second, the use of Big Data by the private or semi-public sector, helping or facilitating them in achieving their specific tasks and/or goals. Examples include the use of Big Data by companies to create risk profiles, to find statistical correlations and to personalize services and advertisements, and the use of Big Data by universities and research institutes for research-related purposes. Big Data is also widely used in the medical sector; for instance, the UK has heavily promoted the use of Big Data in the healthcare sector, and the Israeli Ministry of Health has a large dataset containing medical data on the citizens of Israel and on the healthcare system. According to the Ministry, the potential benefits lie in the facilitation of a variety of healthcare functions (including assisting in the clinical decision-making process, in monitoring diseases and in proactive healthcare). Thirdly, Big Data is used by both governments and private sector companies to improve their service to citizens or customers; this might for example involve increasing the transparency of their activities, strengthening the control of citizens over data processing, etc.

These three categories should lead to different approaches to regulation. The last category is relatively unproblematic because it serves the interests of the citizen. Here, the current legislation on aspects such as the use of personal data should suffice. The situation is different when Big Data is used by governmental agencies to support their goals. It is important to distinguish between the different fields in which Big Data is used by the government. If Big Data is used for the development

of economic policies, for routinely inspecting fire installations or for epidemiological research, this should be relatively unproblematic. In these instances, general patterns and statistical correlations are used to promote the efficiency and effectiveness of public policy. However, if Big Data is used by the police, a different picture emerges – while Big Data is about processing large amounts of data and detecting general patterns, the police need to investigate and possibly arrest specific individuals on the basis of concrete facts. There is a particular danger of mismatches when general profiles are applied to specific individuals. When regulating Big Data, the potential impact on citizens must be taken into account; that impact will be greater when Big Data is used by the police, intelligence services and the army than when it is used for the development of general economic policies. It also appears from our survey that several DPAs are sceptical about the use of Big Data by the police, both because of the possible impact on the citizen and because of the potential for mismatches between general profiles and specific individuals.

Finally, the use of Big Data in the private sector can also be problematic. It emerged from this study that two things in particular need to be taken into account. First, use can be made of data or profiles that are based on sensitive information, such as data about race, medical conditions or religious beliefs; use can also be made of categories that appear neutral but are in fact based on these types of information – a practice known as redlining. Second, the consequences of the use of Big Data in the private sector may also be substantial, irrespective of whether or not sensitive information is used. Where advertisements are personalized through the use of Big Data-like applications, the impact will of course be relatively small; however, when Big Data is used to develop risk profiles on the basis of which banks decide who may be eligible for a loan and on what terms, or by health insurers to decide who they are prepared to insure and on what terms, the consequences can be significant.

Factors that could be taken into account when regulating Big Data are the impact of its use on the individual, the types of data and data analysis that are used and the potential danger of a mismatch between general profiles and specific individuals. A distinction could also be made between the type of organisation that uses Big Data and the specific purpose for which it is used. The general interest that is served by the use of Big Data naturally also has an impact on what should be considered legally admissible.

2.5 WHAT ARE THE OPPORTUNITIES FOR BIG DATA?

The underlying research for this report suggests that almost all experts agree that Big Data represents both significant opportunities and significant risks, although it must be said that the DPAs, by the nature of their work, are more keen on signalling

the latter than the former. For example, in 2013 , 'France Stratégie', an advisory body to the French Prime Minister, performed an analysis of the advantages and disadvantages of Big Data. It emphasized that on the one hand, Big Data provides for more knowledge and opportunities, but on the other may cause problems in relation to the protection of privacy and confidentiality. John Podesta also emphasized this duality. He published a blog on 1 May2014 on the results of the Working Group Review. In his blog, Podesta describes Big Data as a vital technology. He refers to the devastation and suffering caused by tornadoes and implicitly to the predictive powers of Big Data in preventing these adverse events. Big Data could provide opportunities for virtually every sector of the economy, Podesta suggests, and could make the government more efficient. However, the report of the Working Group's is more nuanced, recognizing that Big Data also carries risks: "…how we protect our privacy and other values in a world where data collection is increasingly ubiquitous and where analysis is conducted at speeds approaching real time".

The opportunities for Big Data can be discussed relatively briefly; they follow from the field of application as discussed earlier. The first opportunity that Big Data offers lies in improving the service to the citizen or customer, improving transparency in the public or private sector and giving more control to individuals. Second, particularly in the private sector, it is expected that Big Data will lead to substantial growth in the number of companies, especially start-ups, the number of jobs and the profits generated by those companies. For example, according to the roadmap developed by the *Comité de Pilotage de la Nouvelle France Industrielle* (Steering Committee of the New Industrial France) headed by the French Minister for Industry, Big Data activities in France represented €1.5 billion in 2014 and would reach approximately €9 billion in 2020, with Big Data activities also generating an additional 137, 000 jobs. The EDPS report on Big Data also stresses the economic potential of Big Data : "According to the OECD, 'Big Data related' mergers and acquisitions rose from 55 in 2008 to 134 in 2012. The internet sector is hugely successful with revenue per employee in 2011, among the top 250 companies, of over $900 – over twice as high as for the ICT industry overall (OECD). Internet companies could enjoy 'economies of scope', network effects of more data attracting more users attracting more data, culminating in winner-takes-all markets and near monopolies which enjoy increasing returns of scale due to the absolute 'permanence' of their digital assets."[19]

Finally, Big Data can also be used for achieving the specific objectives of organizations, institutions and government departments. Yet the question is to what extent Big Data is actually used within the public sector. The underlying research for this report seems to indicate that most countries and DPAs mainly recognize the opportunities for Big Data in the private sector, in relation to economic growth, stimulating businesses and increasing the number of jobs. The use of

Big Data by the government, and especially by governmental institutions in relation to maintain public order or protecting national security, is viewed with scepticism.

Several of the DPAs make this point:

- The Hungarian DPA, for example, emphasizes that "in the Hungarian business sphere more and more enterprises such as banks, supermarkets, media and telecommunication companies use and take advantage of the possibilities in Big Data."
- The DPA in Luxembourg states that: "To our knowledge there are no prominent examples of the use of Big Data in the law enforcement sector or by police or intelligence services in Luxembourg. There are however other actors which deal with Big Data."
- The Norwegian DPA argues along the same line: "There is, as far as we know, no usage of Big Data within the law enforcement sector in Norway. In 2014, the intelligence service addressed in a public speech the need to use Big Data techniques in order to combat terrorism more efficiently. However, politicians across all parties reacted very negatively to this request and no formal request to use such techniques has since been launched by the intelligence service. The companies that are most advanced when it comes to using Big Data may be found within the telecom (e.g. Telenor) and media (e.g. Schibsted and Cxence) sectors. The tax and customs authorities have also initiated projects in which they look at how Big Data can be used to enhance the efficiency of their work." The Norwegian DPA continues: "At the Norwegian DPA we are currently looking into how it affects our privacy when personal data is more and more turning into a valuable commodity in all sectors of the economy. We are writing a report on how Big Data is used within the advertising industry, and how the use of automated, personalised marketing triggers an enormous appetite for and exchange of personal data."
- The Slovenian DPA states: "We have thus far not seen prominent examples of the use of Big Data in our country. To our knowledge Big Data applications are mainly of interest in insurance, banking and electronic communications sector, mostly to combat fraud and other illegal practices. Another important field is scientific and statistical research. Law enforcement use is to our knowledge currently at development stages (e.g. in the case of processing Passenger Name Records), whereas information about the use of Big Data at intelligence services is either not available or confidential in nature."
- The Swedish DPA states that: "We have not carried out any specific supervision related to the concept of Big Data and do not have any statistics or specific information on how this is used. In our opinion, the law enforcement sector does not use Big Data. Their personal data processing is strictly regulated in terms of collection of data, limited purposes, etc."

– Finally, the DPA from the United Kingdom states: "We have not carried out a comprehensive market assessment of Big Data but, from our contacts with business and our desk research, our impression is that the take up of Big Data is still at a relatively early stage in the UK. Nevertheless, we know that companies are actively investigating the potential of Big Data, and there are some examples of Big Data in practice, such as the use of telematics in motor insurance, the use of mobile phone location data for market research, and the availability of data from the Twitter 'firehose' for analytics. We do not have any specific information on the use of Big Data in law enforcement or security. The UK Data Protection Act includes a wide-ranging exemption from the data protection principles where it is required for safeguarding national security."

Noteworthy is that many DPAs suggest that Big Data is used particularly in the private sector and less so in the public sector – in particular, the use of Big Data for security-related activities by the government is rejected. Only a few DPAs, such as the Dutch DPA, refer to the use of Big Data by the government for security purposes. Our desk research, however, reveals a different picture, showing that governments do indeed use Big Data technologies, including for security purposes. Australia is an example of a country that is already quite well advanced in using and applying Big Data processes. Among other things, it operates a prototype of the 'Border Risk Identification System' (BRIS). This system can be used at international airports to better estimate which travellers might cause problems. Reference can also be made to the 'Developmental Pathways Project', in which data on children from a variety of sources are linked. Among other things, an assessment will be made of the influence of factors relating to family and the environment on the health of children, the risk of juvenile delinquency, and education. Finally, there is a data tool, Vizie, which has been designed by the Commonwealth Scientific and Industrial Research Organisation (CSIRO), an Australian government corporate entity. This tool follows activity on social media and analyses social media behaviour. A number of government agencies and public sector actors would also like to use this tool, at least according to CSIRO. In addition, as indicated in the previous paragraph, countries such as Brazil, Israel and the United Kingdom promote the use of Big Data by the police, the intelligence and security services and the military.

All in all, no clear picture has yet emerged as to where the opportunities for the use of Big Data lie. It seems clear that both the public and private sectors agree that Big Data will be used in the private sector and will lead to economic and jobs growth. There is less certainty about both the desirability and effectiveness of the use of Big Data by the government, particularly for security-related purposes. This also applies for the questions that have already been raised regarding the effectiveness of Big Data-type data collections by intelligence services such as the NSA in the US in the fight against terrorism. Yet a number of countries have actually

implemented such projects involving the intelligence services, the armed forces and the police, for example in connection with predictive policing. In conclusion, regulators would need to make an assessment of the desirability and effectiveness of the use of Big Data in the public sector, especially when used for the promotion of national security or public order.

2.6 WHAT ARE THE DANGERS OF BIG DATA?

This study shows that the dangers of Big Data are mainly assessed along two lines: first, a possible violation of the right to privacy and/or the right to data protection, and second, the danger of discrimination and stigmatization. As regards the first point, most countries appear to be well aware of the risks Big Data might pose for the privacy of citizens. The DPAs are of course even more aware of this danger. Many DPAs indicate that some or even most of the principles of data protection are threatened by the development of Big Data. Both the Working Paper by the International Working Group on Data Protection in Telecommunications and the report from the Norwegian DPA provide a full overview of the impact Big Data has on the classical data protection principles. The Norwegian DPA, in response to the survey, summarizes the position as follows: "Big Data is challenging key privacy principles, in particular the principles of purpose limitation and data minimisation. The protection provided by these privacy principles is more important than ever at a time when an increasing amount of information is collected about us. The principles provide the foundation for safeguards against extensive profiling in an ever increasing array of new contexts. A watering down of key privacy principles, in combination with more extensive use of Big Data, is likely to have adverse consequences for the protection of privacy and other fundamental rights."

Some of the most prominent tensions between Big Data and the data protection principles are highlighted below.

Purpose and purpose limitation

The current legal framework is based on the principles of purpose and purpose limitation. Article 7 of the EU Data Protection Directive contains an exhaustive list of the legitimate grounds for processing ordinary personal data; Article 8 does the same with regard to the processing of sensitive personal data (e.g. about race, religion, sexual orientation, etc.). Article 6 states that personal data must be processed fairly and lawfully and must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. The prohibition on further processing for different purposes is also known as the 'purpose limitation principle', from which it follows that 'secondary use' is in principle not permitted. The results of both the desk research and the survey show that it is this principle (along with the data minimization principle) that is cited the most when it comes to the tension between Big Data and data protec-

tion. Big Data processes often have no fixed purpose – large amounts of data are simply collected and it may only become clear what the value or potential use of that data is after it has been collected. Moreover, in Big Data analysis, different kind of databases with different types of data are often linked or merged. The original purpose for which the data was collected is then lost.

- For example, the DPA of Luxembourg emphasises: "From a data protection point of view it can raise many concerns, when it contains personal data, such as the respect of data subjects' rights – for example in the context of data mining – and their ability to exercise control over the personal data or the respect fundamental principles of data protection such as that of data minimization or purpose limitation."
- The definition of Big Data by the Dutch DPA includes, among other elements, "combining data that is collected for different purposes", and it also states that: "Our key concern is that data protection should be about surprise minimisation, while Big Data entails the risk of surprise maximation. There is a real risk that those who are involved in the development and use of Big Data are ignoring the basic principles of purpose limitation, data minimisation and transparency. And an additional frightening fact is that the statistical information, even if the data used is properly anonymised, can lead to such precise results that it essentially constitutes re-identification."
- The Norwegian DPA states: "In other words, it is not just the volume in itself that is of interest, but the fact that secondary value is derived from the data through reuse and analysis. This aspect of Big Data, and the consequences it has, is in our opinion the most challenging aspect from a privacy perspective."
- Finally, the Swedish DPA states the following about Big Data: "As we see it, the concept is used for situations where large amounts of data are gathered in order to be made available for different purposes, not always precisely determined in advance."

Data minimization

The second principle that is often mentioned in the context of the dangers of Big Data is the undermining of the principle of data minimization. This principle means that as little data as possible should be collected, and that the amount of data should in any event not be excessive in relation to the purposes for which it is collected. Additionally, personal data must be removed once the goal for which it were gathered has been achieved, and data should be rendered anonymous when possible. This principle, which mainly follows from Article 6 of the Data Protection Directive, obviously clashes with Big Data. The core idea behind Big Data is that as much data as possible is collected and that new purposes can always be found for data already gathered. Data can always be given a second life. This also challenges the requirement that data should be deleted or anonymized when it is no longer needed for achieving the purpose for which it was collected. Almost all DPAs mention this principle when it comes to the dangers of Big Data. The

Luxembourg DPA, among others, refers to a decision in which it stressed the importance of a retention period for data storage. The Dutch DPA summarizes the tension between Big Data and data minimization in very clear terms: "Big Data is all about collecting as much information as possible".

Technical and organizational measures

Articles 16 and 17 of the Data Protection Directive espouse the principle that data should be treated confidentially and should be stored in a secure manner. Many DPAs also mention this principle when discussing the dangers of Big Data; this holds especially for countries and DPAs that establish a link between Big Data and Open Data. The Slovenian DPA states the following on this particular tension: "The principles of personal data accuracy and personal data being kept up to date may also be under pressure in Big Data processing. Data may be processed by several entities and merged from different sources without proper transparency and legal ground. Processing vast quantities of personal data also brings along higher data security concerns and calls for strict and effective technical and organisational data security measures."

Data quality

The current framework requires that the data that is collected is accurate and kept up to date. This ensures that profiles created for or applied to an individual person, and any decisions taken on the basis of them, are appropriate and accurate. This study shows that DPAs are concerned about how this principle can be maintained in Big Data processes. Often, Big Data applications do not revolve around individual profiles, but around group profiles; not retrospective analyses, but probability and predictive applications with a certain margin of error. Moreover, it is supposedly becoming less and less important for data processors to work with correct and accurate data about specific individuals, as long as a high percentage of the data on which the analysis is based provides a generally correct picture. Quantity over quality of data, so the saying goes, as more and more organizations become accustomed to working with 'dirty data'. In the public sector, too, it seems that working with contaminated data or unreliable sources is becoming more common. Examples include the use by government agencies of open sources on the Internet, such as Facebook, websites and discussion forums. The Dutch DPA, for example, states: "There has been a lot of media attention for Big Data use by the Tax administration (scraping websites such as Marktplaats [an eBay-like website] to detect sales, mass collection of data about parking and driving in leased cars, including use of ANPR data, and profiling people to detect potentially fraudulent tax filings."

Transparency

An important principle of the Data Protection Directive is transparency. It includes a right of the data subject to request information about whether data relating to him/her are processed, how and by whom; the controller has a duty to pro-

vide the data subject with this information on its own initiative. This principle is also at odds with the rise of Big Data, partly because data subjects often simply do not know that their data is being collected and are therefore not likely to invoke their right to information. This applies equally to the flipside of the coin: the transparency obligation for data controllers. For them, it is often unclear to whom the information relates, where the information came from and how they could contact the data subjects, especially when the processes entail the linking of different databases and the re-use of information. As the Slovenian DPA put it: "Big Data has important information privacy implications. Information on personal data processing may not be known to the individual or poorly described for the individual, personal data may be used for purposes previously unknown to the individual. The individual may be profiled and decisions may be adopted in automated and non-transparent fashion having more or less severe consequences for the individual."

Individual rights

The current legal system puts much emphasis on subjective individual rights and does so to an increasing degree. For example, the forthcoming Regulation[20] might potentially give data subjects additional individual rights, such as the right to be forgotten and the right to data portability. In their response to the survey, DPAs also frequently referred to the principle of informed consent. Individual rights traditionally also come with individual responsibility, namely to protect individual rights and to invoke them if they are undermined. The question is whether this focus can be maintained in the age of Big Data. It is often difficult for individuals to demonstrate personal injury or an individual interest in a case; individuals are often unaware that their rights are being violated and if they do know that their data has been gathered. In the Big Data era, data collection will presumably be so widespread that it is impossible for individuals to assess each data process to determine whether it includes their personal data, if so whether the processing is lawful, and if that is not the case, to go to court or file a complaint. The United Kingdom DPA states the following on this issue: "It may be difficult to provide meaningful privacy information to data subjects, because of the complexity of the analytics and people's reluctance to read terms and conditions, and because it may not be possible to identify at the outset all the purposes for which the data will be used. It may be difficult to obtain valid consent, particularly in circumstances where data is being collected through being observed or gathered from connected devices, rather than being consciously provided by data subjects."

Emphasis on legal regulation

The current system is primarily based on the legal regulation of rights and obligations. Big Data challenges this basis in several ways. Data processing is becoming increasingly transnational. This implies that more and more agreements must be made between jurisdictions and states. Making this legally binding is often

difficult due to the different traditions and legal systems. Rapidly changing technology means that specific legal provisions can easily be circumvented and that unforeseen problems and challenges arise. The legal reality is often overtaken by events and technical developments. The fact that many of the problems resulting from Big Data processes, as also highlighted by a number of DPAs, predominantly revolve about more general social and societal issues makes it difficult to address all the Big Data issues within specific legal doctrines, which are often aimed at protecting the interests of individuals, of legal subjects. That is why more and more national governments are looking for alternatives or additions to traditional black letter law when regulating Big Data – for example self-regulation, codes of conduct and ethical guidelines. The DPA of the United Kingdom states, for example: "It is notable however that there is some evidence of a move towards self-regulation, in the sense that some companies are developing what can be described as an 'ethical' approach to Big Data, based on understanding the customer's perspective, being transparent about the processing and building trust."

DPAs also place a good deal of emphasis on profiling and the risk of discrimination, stigmatization and inequality of power resulting from Big Data. The desk research shows that a number of countries specifically acknowledge this danger. The Dutch DPA states the following in respect of such dangers: "When Big Data is used to profile people, it has the potential of leading us on to a – predetermined and maybe sometimes dangerous – path. A path that may in the end undermine the values that underpin our democratic societies, by depriving people of their free choice, of their right to personal development and equal treatment." The best overview of these types of dangers is provided in the Working Paper 'Big Data and Privacy: Privacy principles under pressure in the age of Big Data analytics'[21] by the International Working Group on Data Protection in Telecommunications. Four of the points made in that paper are transcribed here verbatim.

"Power imbalance

Individuals, as a general rule, have limited power to influence how large corporations behave. Extensive use of Big Data analytics may increase the imbalance between large corporations on the one hand and the consumers on the other. It is the companies that collect personal data that extract the ever-growing value inherent in the analysis and processing of such information, and not the individuals who submit the information. Rather, the transaction may be to the consumer's disadvantage in the sense that it can expose them to potential future vulnerabilities (for example, with regard to employment opportunities, bank loans, or health insurance options).

Data determinism and discrimination

The 'Big Data-mindset' is based on the assumption that the more data you collect and have access to, the better, more reasoned and accurate decisions you will be able to make. But collection of more data may not necessarily entail more knowledge. More data may also result in more confusion and more false positives. Extensive use of automated decisions and prediction analyses may have adverse consequences for individuals. Algorithms are not neutral, but reflect choices, among others, about data, connections, inferences, interpretations, and thresholds for inclusion that advances a specific purpose. Big Data may hence consolidate existing prejudices and stereotyping, as well as reinforce social exclusion and stratification. Use of correlation analysis may also yield completely incorrect results for individuals. Correlation is often mistaken for causality. If the analyses show that individuals who like X have an eighty per cent probability rating of being exposed to Y, it is impossible to conclude that this will occur in 100 per cent of the cases. Thus, discrimination on the basis of statistical analysis may become a privacy issue. A development where more and more decisions in society are based on use of algorithms may result in a 'Dictatorship of Data', where we are no longer judged on the basis of our actual actions, but on the basis of what the data indicate will be our probable actions.

The Chilling effect

If there is a development where credit scores and insurance premiums are based solely or primarily on the information we leave behind in various contexts on the Internet and in other arenas in our daily life, this may be of consequence for the protection of privacy and how we behave. In ten years, our children may not be able to obtain insurance coverage because we disclosed in a social network that we are predisposed for a genetic disorder, for example. This may result in us exercising restraint when we participate in society at large, or that we actively adapt our behaviour – both online and elsewhere. We may fear that the tracks we leave behind in various contexts may have an impact on future decisions, such as the possibility of finding work, obtaining loans, insurance, etc. It may even deter users from seeking out alternative points of view online for fear of being identified, profiled or discovered. With regard to the authorities' use of Big Data, uncertainty concerning which data sources are used for collecting information and how they are utilised may threaten our confidence in the authorities. This in turn may have a negative impact on the very foundation for an open and healthy democracy. Poor protection of our privacy may weaken democracy as citizens limit their participation in open exchanges of viewpoints. In a worst case scenario, extensive use of Big Data may have a chilling effect on freedom of expression if the premises for such use are not revealed and cannot be independently verified.

Echo chambers

Personalisation of the web, with customised media and news services based on the individual's web behaviour, will also have an impact on the framework conditions for public debates and exchanges of ideas – important premises for a healthy democracy. This is not primarily a privacy challenge, but constitutes a challenge for society at large. The danger associated with so-called 'echo chambers' or 'filter bubbles' is that the population will only be exposed to content which confirms their own attitudes and values. The exchange of ideas and viewpoints may be curbed when individuals are more rarely exposed to viewpoints different from their own."[22]

It therefore appears that in addition to opportunities, there are significant risks associated with Big Data processes. It should be emphasized that these threats again vary with respect to their impact on citizens according to their application. Instances of discrimination are always problematic, but if the police discriminate, this may obviously be more serious than in the case of personalised advertisements. Consequently, when regulating Big Data, account should be taken of the likelihood and the magnitude of potential problems relating to privacy and/or discrimination, and this must be weighed against the potential benefits. It should be stressed that the right to privacy, the right to data protection and the right to freedom from discrimination are all fundamental human rights that may be constrained only in exceptional circumstances in a democratic society.

2.7 ARE THE CURRENT LAWS AND REGULATIONS APPLICABLE TO BIG DATA?

Both the desk research and the results of the survey show that in most countries, the current rules in the area of privacy and data protection, as developed in their respective jurisdictions, are applied to Big Data processes. There is Germany with its distinctive personality right, the United States without an umbrella law for the regulation of privacy, but with sectoral legislation, and most other countries with relatively similar rules concerning privacy and data protection. In addition, a number of countries have specific laws on telecommunications and special rules for organizations such as the intelligence services and archives. In Australia, for example, there is specific regulation covering data matching in terms of tax records by governmental agencies, in which protocols are established for linking this data. Government departments working with files from the tax department must fulfil the requirements of the 'Data-matching Program (Assistance and Tax) Act 1990'. There are also mandatory guidelines for the implementation of the data-matching programme.

It appears that current legislation is generally applied to Big Data projects, including in several court cases:

- In July 2015 the French Constitutional Court, the *Conseil Constitutionnel*, gave its opinion on the French law governing the intelligence and security services. In this ruling, the court specifically stated which provisions of this law are in line with the French Constitution and which parts or provisions of the law are not. Some provisions were declared unconstitutional, including a provision regarding the permission given by the Minister to monitor communications sent from abroad or received from abroad.
- In the United States, the case of the United States v Jones from 2011 is of importance because this lawsuit had a limiting effect on the large-scale data gathering of location data by the police. In ACLU v Clapper, the Second Circuit Court of Appeals ruled that the mass collection of metadata about phone records by the NSA is illegal – this activity is not covered by section 215 of the Patriot Act. Meanwhile, however, the Foreign Intelligence Surveillance Court has ruled that the collection of metadata may continue.
- In the United Kingdom, in the case of Google Inc. v Vidal-Hall & Others, the Court of Appeal was asked to rule on the interpretation of the Data Protection Act 1998. The case revolved around the complaint by users of Apple's Safari browser, who believed that Google was gathering data through that browser in violation of the Data Protection Act 1998. The Court ruled that browsing information may be personal information and abuse of personal information should be considered as a tort.

From the survey of DPAs it also seems that current legislation is considered to be generally applicable to Big Data. They often refer to the national implementation of the Data Protection Directive. Yet there are a number of countries with specific laws. Because the Estonian DPA sees Big Data as part of the Open Data movement, it refers to the Open Data legislation, namely the Public Information Act, which is currently pending in Parliament. In Hungary, the Information Self-Determination and Freedom of Information ('Privacy Act') applies. The Swedish DPA refers to special legislation for public services, such as the tax authorities, and to telecommunications law which partially constitutes an implementation of the European e-Privacy Directive.[23] The survey also shows that the current legislation is applied in legal cases by national courts and in the opinions of the DPAs. The Belgian DPA refers to its advice on profiling, the DPA of Luxembourg to a report on smart metering and the Dutch DPA to lawsuits regarding the Tax Authorities and the use of data collected by the police through traffic cameras operated by the Tax Authorities.

In conclusion, it seems that the current legislation is generally declared to be applicable to Big Data; both courts and DPAs have successfully applied current principles when assessing Big Data-related projects. This should be taken into

account when regulating Big Data. Replacing the current regulation with new 'Big Data' regulation would be to throw the baby out with the bathwater. It seems more logical to develop new rules that could be applied in addition to the current regulatory framework. Whether and to what extent there is a need for such additional legislation will be discussed next.

2.8 IS THERE A NEED FOR NEW LEGISLATION FOR BIG DATA?

It is evident from the foregoing sections that in most countries, Big Data initiatives are treated under existing legislation with regard to issues such as privacy and data protection. Furthermore, the DPAs are agreed that the current data protection principles must be maintained. The Slovenian DPA, for example, explicitly states: "Big Data brings substantial challenges for personal data protection and these challenges must firstly be well understood and adequately addressed. In our view new concepts and paradigms, such as cloud computing or Big Data should not lower or undermine the current levels of data protection as a fundamental human right. Existing central data protection principles, such lawfulness, fairness, proportionality, rights of the data subjects and finality should not be undermined with the advent of Big Data. The rights of the individuals to informational self-determination should be cornerstone in modern information society, protected by modern data protection framework delivering efficient data protection for the individual while allowing lawful and legitimate interests, often also in the interest of the individual, to be attained."

Yet most DPAs are also aware of the fundamental clash between Big Data and data protection principles, as already shown in section 2.6. In this spirit, the United Kingdom DPA asserts that the data protection rules apply to Big Data processes, but it also emphasizes the challenges involved: "In our work we have noted that Big Data poses a number of challenges to data protection, in particular: It may be difficult to provide meaningful privacy information to data subjects, because of the complexity of the analytics and people's reluctance to read terms and conditions, and because it may not be possible to identify at the outset all the purposes for which the data will be used. It may be difficult to obtain valid consent, particularly in circumstances where data is being collected through being observed or gathered from connected devices, rather than being consciously provided by data subjects. Big Data tends to use data for new and unexpected purposes, which may conflict with the purpose limitation principle. Big Data tends to use 'all the data', which may conflict with the data minimization principle."

It is remarkable that despite this fact, as of yet, little new legislation seems to be being developed that specifically addresses the new dangers posed by Big Data. Some DPAs refer to the forthcoming General Data Protection Regulation and indicate that they hope that those rules will help them to adequately curb the dangers

of Big Data. To refer again to the words of the UK DPA: "We note that the proposals for the new EU General Data Protection regulation incorporate some of the measures we have identified as being important in ensuring compliance in Big Data e.g. clearer privacy notices, privacy impact assessments and privacy by design. We welcome the fact that these measures are being foregrounded, although we are concerned that that they should not be seen as simply a bureaucratic exercise."

Still, the survey indicates that the Estonian parliament is discussing new legislation on Open Data (including Big Data). Also, a number of DPAs refer to co-regulation and self-regulation as a possible solution. The United Kingdom DPA states: "It is notable however that there is some evidence of a move towards self-regulation, in the sense that some companies are developing what can be described as an 'ethical' approach to Big Data, based on understanding the customer's perspective, being transparent about the processing and building trust." The Dutch DPA also refers to agreements with and by the private sector: "Our chairman has called for a fierce social dialogue, to make people aware of the risks to our intrinsic values that is posed by Big Data and to think together about how we can effectively address these risks and unwanted consequences." Finally, the DPA of France refers to a pending Bill: "At present, the French government is preparing a new law for a 'Digital Republic'. An online consultation was launched on the draft bill on September 2015 and the public was invited to suggest amendments to 30 proposed measures, ranging from net neutrality to open data (until 17 October 2015, www.economie.gouv.fr/projet-loi-numerique). The draft bill proposes in particular an open-data policy for the French state that would make official documents and public-sector research accessible to all online. The bill should be submitted to the parliament at the beginning of 2016."

The desk research supports the idea that governments are actively thinking about new legislation, partly because current laws are seen as hindering technological innovation. Japan may be a case in point here. In 2013, the Strategic Headquarters for IT produced an amendment to various statutory provisions on privacy and data protection: 'Directions on Institutional Revision for Protection and Utilization of Personal Data'. A summary containing the main points of its policy, issued in 2014, discusses technological developments, including Big Data, that have occurred since the introduction of the Data Protection Act of 2003. According to the Strategic Headquarters for IT, there are now several barriers to the use of personal data. Furthermore, even organizations that respect the law and do not infringe rights are worried about criticism over potential privacy violations and the use of personal data; as a consequence, data are not used optimally. The growth envisaged by the Japanese government can only be achieved if personal data is used optimally and if Big Data flourishes. That is why the government wants to remove these barriers.

An environment must be created in which violations of rights are prevented and in which personal information and privacy are protected, but in which, at the same time, personal information can be used for innovation.

The UK Parliament has commissioned a study on the legislative framework for sharing data between public authorities. In July 2014, a commission published its report with three recommendations, suggesting among other things that the legal reform should go beyond simply stipulating rules for the sharing of data between public authorities; it should also regard the sharing of information between government agencies and organizations with public tasks. Finally, reference can be made to Germany. The Minister of the Interior has proposed a new principle for forthcoming legislation: the minimization of risk. He has also announced that Germany will propose the inclusion of provisions about pseudonymisation and profiling.

Consequently, when answering the question of whether it is desirable to formulate new rules for Big Data processes, three specific issues seem important. First, almost all countries and DPAs acknowledge that Big Data poses new and fairly fundamental risks to the current regulatory framework, and in particular the underlying principles. Second, the current regulatory framework is perceived as being (too) restrictive in relation to the deployment of new technologies and technological innovation, particularly in the private sector. Thirdly, many stakeholders are unsure how the current regulatory framework should actually be applied and interpreted in relation to Big Data. Two dangers might follow from this: on the one hand stakeholders, for fear of breaking the law, might forgo many technological innovations and data uses that would in fact be legitimate. On the other hand, parties might use – or rather, abuse – the existing grey area to deploy certain technologies that would not be in accordance with the current regulatory framework. Whether and how a new regulatory framework might provide a solution for these challenges needs to be assessed carefully by regulators.

2.9 WHAT CONCEPT SHOULD BE CENTRAL TO BIG DATA REGULATION?

In short, a diffuse picture emerges with respect to the extent to which developing a special regulatory Big Data regime is necessary or even desirable. What is evident is that regulating Big Data will be especially difficult for two reasons. First, it is difficult to choose a good starting point for the regulation of Big Data; this will be discussed in this section. Secondly, it will be difficult to pinpoint a specific person or institution to serve as data controller or, more generally, a natural or legal person that is responsible for compliance with the regulatory principles in Big Data processes. This will be discussed in the next section. Regarding the starting point, it should be noted that the current regulation is primarily based on the individual

and their interests – this holds for human rights such as privacy and for data protection, which is based on the concept of 'personal data', i.e. data that enables someone to identify or individualize a natural person.

However, Big Data processes do not so much revolve around the storage and processing of data at an individual level – rather, the trend is to work increasingly with aggregated data, general patterns and group profiles. Consequently, it is questionable whether the focus on the individual, on personal data, can still be maintained in the Big Data era. The statistical correlations and group profiles do not qualify personal data, but can be used inter alia to alter, shape or influence the living environment of people to a great extent. Furthermore, the trend towards the use of metadata also ties into this problem, because it is unclear to what extent metadata will always qualify as personal data.

In addition, many DPAs point out that in Big Data processes, personal data or profiles may be created through the use, combination or analysis of data that do not qualify as personal data:

– The EDPS states explicitly that a lot of data is gathered in Big Data processes, but also suggests: "Not all of these data are personal, but many players in the digital economy increasingly rely on the large scale collection of and trade in personal information."
– The Working Party 29 states that: "In addition, Big Data processing operations do not always involve personal data. Nevertheless, the retention and analysis of huge amounts of personal data in Big Data environments require particular attention and care. Patterns relating to specific individuals may be identified, also by means of the increased availability of computer processing power and data mining capabilities."
– The DPA from Luxembourg suggests that Big Data "allows for the correlation of information which previously could not be linked. From a data protection point of view it can raise many concerns, when it contains personal data, such as the respect of data subjects' rights – for example in the context of data mining – and their ability to exercise control over the personal data or the respect fundamental principles of data protection such as that of data minimization or purpose limitation. Moreover practices such as linking separate databases or computer analytics can turn anonymous data or any kind of non-identifiable information into personal data which would need to be protected under data protection law."
– As a final example, reference can be made to the DPA from Slovakia, which argues: "As a research topic we would like to suggest examining boundaries between personal and non-personal information. In the Big Data environment you are able to connect non-personal information and based on this information identify the data subject which represents potential risk to rights of the data subjects."

Consequently, it is questionable whether the individual, individual interests and concepts such as personal data, which are explicitly linked to individual natural persons, still serve as a good starting point for building a regulatory framework in the Big Data era. Irrespective of whether the regulator chooses to leave the current legislation largely intact, whether it opts to amend current legislation or chooses to develop a new Big Data framework, it seems that at a certain point in time it will be necessary to address the fact that it is increasingly difficult to take 'personal data', or a related concept, as the basis for rules and obligations. It should finally be noted that the nature of the data is also becoming less and less static; rather, data increasingly goes through a lifecycle in which its nature might change constantly. While the current legal system is focused on relatively static stages of data, and linked to them specific forms of protection (e.g. for personal data, sensitive data, private data, statistical data, anonymous data, non-identifying information, metadata, etc.), in reality, data goes through a circular process: data is linked, aggregated and anonymized and then again de-anonymized, enriched with other data and profiles, so that it becomes personally identifying information again, and potentially even sensitive data, and is then once again pseudonymised, used for statistical analysis and group profiles, etc.

2.10 HOW SHOULD THE RESPONSIBILITIES BE DISTRIBUTED?

A final question that needs to be answered when regulating Big Data is who should bear responsibility for enforcing the rights and obligations, or in data protection terms, who should be the data controller. This issue exists irrespective of whether the regulator chooses to leave the existing legislation untouched, seeks to amend current legislation or opts to develop new Big Data legislation. The problem of allocating responsibility was prominent both in the desk research and the survey and in general manifests itself on three different levels.

Firstly, there was already a fair degree of awareness of the increasingly transnational nature of data processing activities – it should be noted that both the desk research and the survey were completed before the Safe Harbour decision of the Court of Justice.[24] The problem is that different countries have different levels of data protection. The danger is that private parties will settle in those countries where the regulatory pressure is low. But public sector organisations might act in similar ways as well. For example, in the Netherlands there is a court case pending on the cooperation between the Dutch intelligence services and their counterparts abroad.[25] Although the Netherlands limits the capacities of its intelligence services to collecting information about Dutch citizens, the US intelligence services, which are less constrained regarding the collection of data on Dutch nationals, might collect such data and then pass it on to the Dutch intelligence services. This might

work the other way around, too. Consequently, intelligence services might effectively circumvent the rules that apply to them, by cooperating with other international actors that are not bound by those rules.

Secondly, it is also apparent from the desk research that there is increasing cooperation between the public and the private sectors, voluntary or otherwise. For example, in Australia, there is collaboration between industry and academia; the Brazilian police use a system that was originally developed by Microsoft and the New York police; China stresses the need for cooperation between the public and the private sector; and the Estonian DPA refers to the cooperation between public and private parties with respect to the development of regional policies. Again, the question is which responsibilities should be borne by which party. Often, it is not clear at first sight what role an organization has played in the value chain of the data processing activity. Also, very different regulatory frameworks often apply to public sector and private sector institutions, as also noted by a number of DPAs in their response to the survey.

Thirdly and finally, there is also a trend towards sharing data and linking databases between governmental organisations. This implies that governmental agencies that have a limited legal capacity to gather and store data may still obtain a wealth of information from other governmental organisations that have a greater legal capacity to gather and store such data. For example, the Dutch DPA refers to a lawsuit that revolves around the use by the Tax Authorities of information gathered by the police. Again, the question is which party should bear responsibility for enforcing the legal regime and the restrictions it imposes. More generally, it should be noted that data flows are becoming more fluid and elusive, so that more and more organizations are involved and more and more parties share partial responsibility. This complicates the attribution of responsibilities.

Just as the lifecycle of data is becoming increasingly circular, so the division of responsibilities is a clearly shifting from a rather static reality, in which one party collects and processes data, is the main controller of the data and should therefore enforce the different rules and obligations encapsulated in the legislative framework, to a world in which different parties collect, share and link data, in which parties from the private and the public sectors cooperate, in which different governmental institutions share data and databases and in which international data flows are becoming increasingly common. Consequently, when regulating Big Data, it seems logical to make a choice regarding the distribution and attribution of responsibility. The regulator may, despite these developments, opt for a relatively static model in which one party is the main controller and is responsible for enforcing the legal obligations; or it could opt for a more dynamic model, in which the distribution and attribution of responsibilities is shared and might change as the nature of the data processing activities change. The Data Protection Directive

could provide a basis for the latter option, as it defines the controller as "the natural or legal person, public authority, agency or any other body which *alone or jointly* with others determines the purposes and means of the processing of personal data."

3 BIG DATA DESK RESEARCH

3.1 AUSTRALIA

3.1.1 GOVERNMENT INITIATIVES

As a part of the ICT strategy of the Australian public service, the government released the 'Australian Public Service Big Data Strategy' in 2013, under the responsibility of the Australian Department of Finance.[26] Parallel to this, a centre for the entire the government was set up, headed by the Department of Finance, for improving the data analytics capacity of the government.[27] The strategy is intended to advance the possibilities of Big Data while safeguarding the privacy of the individual. Improving the possibilities for Big Data analytics for the government should lead to improved services and better policy advice. In the report, the vision of the future is described as follows:

"The Australian Government will use Big Data analytics to enhance services, deliver new services and provide better policy advice, while incorporating best practice privacy protections and leveraging existing ICT investments. The Australian Government will be a world leader in the use of Big Data analytics to drive efficiency, collaboration and innovation in the public sector".[28]

In addition, principles with which the government complies are presented and concrete goals regarding Big Data are set.[29] These principles are: data is a national asset; to use privacy by design; integrity of data and transparency of the process; sharing of skills, resources and capacity; collaboration with the industry and academia; and fostering open data. The Australian government regards data as an asset, which increases in value due to Big Data.[30] In January 2015, the working group presented a new document for this research, a 'Better Practice Guide' for Big Data. In this, points of reference are offered to government institutions on how to handle Big Data, the Guide aims to inform government institutions that want to engage with Big Data how best to handle datasets and protect privacy.[31] The business aspects, implementing the capacity needed for Big Data, information management and Big Data, project management for Big Data and responsible data analytics are all examined.

The strategy discusses a number of specific projects which use a form of Big Data. For example, the 'Border Risk Identification System (BRIS)', from the Department of Immigration and Citizenship, a prototype of which is already being used. This system can be used at international airports to help in assessing which passengers could cause problems.[32] Or there is the 'Development Pathways Project', in which data from different sources about children are linked, among other things to help ascertain what influence factors regarding the person, family and environment

have on the increase or decrease in the health risks of the child, on the risk of juvenile delinquency and on education.[33] There is also a data tool, 'Vizie', designed by the Commonwealth Scientific and Industrial Research Organisation (CSIRO), an Australian government corporate entity.[34] This tool tracks social media activity and analyses social media behaviour. A few government institutions and actors in the public sector would be interested in working with this, according to CSIRO.[35]

3.1.2 LEGISLATION AND CASE LAW

The report on the strategy for Big Data lists the specific legislation which is relevant in the context of Big Data. Big Data is regulated like any other form of data or information. Therefore, the following laws are of importance: the Freedom of Information Act 1982;the Archives Act 1983;the Telecommunications Act 1997 and the Electronic Transactions Act 1999.[36] These laws are thus not specifically intended for Big Data, but each regulates a separate part of the data process. There is also specific regulation for data matching in the context of tax files by government departments, in which protocols are laid down for the combining of this data. For the tasks of government departments with files from the tax department, the obligations of the Data-matching Program (Assistance and Tax) Act 1990 must be complied with. Also, there are obligatory guidelines for executing the data matching program. In these cases a 'Program Protocol' must be drafted which includes all relevant information, such as on which legal ground the collection of personal information and transfer of the data takes place, why methods other than data matching were not an option, how the individual on which the data is based is informed and which security measures have been taken. This draft must subsequently be filed with the Information Commissioner.[37] When no tax files are involved, but government institutions match other data with data from other government institutions, with data from federal institutions or with data from private companies, voluntary guidelines are in place. Here a 'Program Protocol' can also be drafted and a report is delivered containing the following elements: a description of the data, a specification of each matching algorithm, the expected risks and how these will be dealt with, the means of verifying the integrity and the security measures to be used.[38]

Also of importance is the Privacy Act 1988, in which all phases of handling personal data are regulated.[39] In 2014, amendments made to this law, inter alia by introducing 13 privacy principles which apply to the public sector as well as the private sector, with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.[40] These principles include: securing personal data, open and transparent management of personal data, anonymity and pseudonymity, and notification of the collecting of personal data.[41] The Privacy Regulation 2013 also came into effect.[42] Big Data is not explicitly mentioned in the explanatory memorandum. However, as regards access to more information about credit applicants, risks are discussed

such as access by credit rating agencies to large databases, the use of credit information for purposes other than assessing solvency and the heightened risk of information not being correct due to the large amounts of data.[43]

3.2 BRAZIL

3.2.1 GOVERNMENT INITIATIVES

A government commission for strategic policy in one of the Brazilian states, Minas Gerais, is using a Big Data tool, 'DataViva'. DataViva combines data from databases belonging to three Ministries and a UN database on trade, concerning exports and imports, labour and education, from all over the country.[44] At first the aim of this Big Data tool was to help in drafting economic policy, but it became clear that it offered opportunities as a Big Data tool as such; the relationships and dynamics that the tool exposes provide an insight into the economy for public and private actors and support them in their decision-making.[45] The tool offers 11 different ways to create visualisations with the data from all these databases combined, to which filters can be applied to represent the desired data flows.[46]

The police in Sao Paulo are implementing a system based on Big Data technology: 'Detecta'. Detecta is an intelligent system for monitoring crime. Large datasets held by the Sao Paulo police are combined in this tool and subsequently Detecta makes connections between the data. This includes data from police reports, telephone calls to emergency services, surveillance footage, lists of stolen vehicles and systems for automated number plate recognition. The system is designed to aid in tracking down criminals and preventing crime. While making the connections between the data, the system automatically gives warning feeds to civil and military police, alerting them when the details of a person who is wanted enter the system and this person is thus detected somewhere by the system. Also, a warning is received when a crime is committed with the same characteristics as previous crimes. Searches can be conducted on a specific person whereby incidents related to that person are shown on a map, using data from the civil police as well as from the military policy and traffic police. With regard to prevention, the system reveals patterns in the crimes committed in the region, so that police forces can see where and when certain types of crimes are committed frequently. The system was originally developed by Microsoft and the New York policy force; the technology is being adapted for use in Brazil.[47]

3.2.2 LEGISLATION AND CASE LAW

An amendment to the legislation on data protection is currently being developed. The government has released a draft bill for this law, entitled: "On the processing of personal data to protect the personality and dignity of natural persons".[48] The bill regulates the following topics: legal grounds for processing personal data; principles for handling personal data; the rights of data subjects; communication

and combining data; international data transfer; responsibilities of the actors; and administrative sanctions.[49] There is a website specifically for the legislative proposal and public consultations and parliamentary debates are being held regarding the proposal.[50]

3.3 CHINA

3.3.1 GOVERNMENT INITIATIVES

In 2014, but especially in 2015, a lot of posts about Big Data appeared on the English website of the Chinese government. Li Keqjang, Premier of the Chinese State Council, gave a speech on 5 March 2014 before the National People's Congress about the work of the government, in which he announced that the government is working on Big Data:

"We will strive to catch up with and overtake advanced countries in areas of new-generation mobile communications, integrated circuits, Big Data, advanced manufacturing, new energy and new materials, and to guide the development of emerging industries."[51]

In the report by the government which was presented during the same session, it was announced that China is developing a social credit system and that sharing of government information is to be encouraged.[52] The new credit system is intended to create trust in the system and its integrity; the emphasis is on sharing data about people whose names appear on 'blacklists' with different companies and government agencies.[53]

During the 'Guiyang International Big Data Expo' on 26 May 2015, the Chinese Vice Premier emphasized that the government wants to make better use of technologies such as Big Data and cloud computing to support innovation and economic development, and is willing to cooperate with other countries to achieve this. He also pledged that the government would ensure cooperation between industry and providers of public services in applying Big Data.[54] On 17 June 2015, it was announced that the State Council had set up a coding system for credit ratings for legal entities. The old system was regarded as inefficient because the coding consisted of data from various sources and it was necessary to apply for multiple codings.; in the new system these have been merged.[55] On the same day, a meeting of the State Council took place in which the Prime Minister addressed the issue of Big Data. He stated that Big Data is important for reforming the government system of administrative approval; Big Data can provide better supervision and a more transparent government.[56] Again, the credit classification system was discussed: the data on market supervision and credit information held by companies must be shared between the different government institutions in the interests of society.[57]

On 1 July 2015, the Chinese State Council released an official report on Big Data. The document specifically refers to the Big Data technology used by the government to make government services more efficient. Big Data should support the administrative functions and lower the costs of government services and supervision. In line with previous announcements, this entails among other things more personalized service delivery by the government, greater efficiency in the administrative approvals process, with preference being given to companies with a good credit score and those with a poor credit rating being restricted. In addition, government information sources will become more open and data will be shared more openly, for example data concerning administrative approvals, and will increasingly be shared between the different government departments. The government is to set up a website for checking the credit status of a company, where all information from all government departments will be brought together and made public.[58]

The planned introduction of 'Internet Plus' was also announced in July: a proposal to integrate the Internet in every sector, including the more traditional sectors. According to the Prime Minister, mobile Internet, cloud computing, Big Data and the Internet of Things will be integrated into production processes, and thus constitute a major engine for economic growth. Further integration of the Internet into the economic and social sectors should be completed before 2018, and before 2025 'Internet Plus' will become a new economic model.[59]

Since July 2015, a provincial Big Data system has been rolled out by the government in the central Hubei region, where the provincial government which is accountable for the industrial and commercial sectors has made available data concerning companies, law enforcement reports, market supervision reports and complaints by consumers. Users can browse indicators for this region and extract more detailed data and use it to generate graphs. It is expected that more systems of this type will be rolled out in other parts of China over the coming period. One day after this announcement, the Supreme People's Court announced that all of China's judicial bodies (except military courts) are now linked to each other in a single judicial Big Data centre, in which citizens can search for information on court cases.[60]

On 19 August 2015 a meeting took place between the State Council and the Prime Minister at which among other things a guideline was adopted for Big Data development. According to this guideline, the government will for example encourage the sharing of data between government sources and public data sources.[61] According to the Prime Minister, government departments need to share more data with each other; more than ten data platforms have been set up, but as yet they are not linked to each other , and more data should be made accessible to

the public. The Prime Minister also stated that information security must be safeguarded and those who misuse data and violate the privacy of others must be punished severely.[62]

3.3.2 LEGISLATION AND CASE LAW

China does not have overarching privacy legislation such as that in many European countries. At the end of 2012, the Chinese parliament drafted a resolution consisting of 12 articles and regulating privacy and data protection: the 'Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data'. Among other things, this resolution is intended to provide better safeguards for the privacy of citizens online. Service providers and government institutions are not permitted to allow information on users to become public, nor to sell it to others. For example, the authorities must protect information that makes an individual recognizable or violates his or her privacy.[63] One of the articles sets out an identity management provision, stipulating that Internet users are obliged to provide their real name to the provider. The resolution includes obligations for service providers with regard to the collection and use of information on individuals; the provider has to state up front the purpose for which they are collecting or using the data, as well as how it will be used, how much data will be collected or used, and must obtain the permission of the user before collecting any data.[64]

3.4 FRANCE

3.4.1 GOVERNMENT INITIATIVES

In 2013, 'France Stratégie', an advisory body reporting to the French Prime Minister, published an analysis of the benefits and downsides of Big Data , an overview of investments in Be Data, and an inventory of a number of initiatives in other countries. According to France Stratégie Be Data is not just a temporary phenomenon but is here to stay. The amount of data is growing, and the analysis of that data is steadily improving. On the one hand, Big Data provides more knowledge and opens up new possibilities, whilst on the other hand it can also give rise to problems in relation to privacy and confidentiality. According to the report, the French government is currently making little use of empirical analysis, and public data is not yet being used optimally. It puts the limited use of data analysis to the fact that not enough data is yet being shared between the government and external parties, although the report does note that the sharing of data is growing and that there is an increasing move towards open data.[65]

In July 2014, the *Comité de Pilotage de la Nouvelle France Industrielle* (Steering Committee of the New Industrial France – CNIL), under the direction of the Minister for Industry, published a roadmap for Big Data.[66] Big Data is highlighted by the French government as one of the key developments for modern reforms in

French industry. The roadmap is one of the 34 initiatives launched in 2013, all by the aforementioned committee, to help France towards a new industry.[67] According to the roadmap, Big Data activities in France were valued at €1,5 billion in 2014 and are projected to be worth around €9 billion by 2020. It is also estimated that Big Data will provide 137,000 jobs.[68] One of the challenges highlighted in the roadmap is purpose limitation: Big Data is mainly based on the re-use of data for a different purpose or combinations with new data, which can cause problems with the 1978 law governing information technology, data files and civil liberties.[69] The specific steps suggested in the roadmap for the Big Data ecosystem as a whole are: training and education of data scientists; enhancing innovation by giving start-up businesses access to data and the infrastructure they need; supporting start-ups in accelerating innovation and Big Data projects; observing Big Data use, among other things through constant dialogue between the public and private sectors.[70] At sectoral level, projects will be set up in both the public and private sectors.[71] Thirdly, in the area of legislation, more attention will be given to the implementation of the French law on the protection of personal data, and CNIL will begin the certification of companies regarding the use of personal data.[72]

In March 2015 the French government announced plans to launch a project to digitalize the government administration.[73] The project is entitled VITAM (Valeurs Immatérielles Transmises aux Archives pour Mémoire) and is a collaborative venture between three government ministries: The Ministry of Foreign Affairs and International Development, the Ministry of Culture and Communication and the Ministry of Defence.[74] These ministries are jointly investing €15 million in the project. The pilot phase for the software is scheduled to start in 2016.[75] The aim is to develop software that makes it possible to create a digital archive that can be used by multiple government institutions. The archive could only be created as a collaborative venture between several Ministries because the costs are too high for one Ministry alone.[76] Making the information available electronically should help with indexing, making metadata verifiable, allow storage of the information, offer search functions and ensure the durability of the information.[77] This project has opened the way for collaboration between stakeholders in the public ecosystem and local authorities, whereby the integrity and anonymity of the information is guaranteed.[78]

The French government considered the future challenges for 2025 for the national mail delivery system. The research suggests that the government has five options for resolving these problems. One possible strategy is to focus the service delivery more on e-commerce and to use Big Data analytics to improve the chain of production. It is not yet clear which of these five directions is preferred.[79]

3.4.2 LEGISLATION AND CASE LAW

A law was introduced in France as long ago as 1978 in which data plays a major role: the 'Loi Informatique et libertés', which regulates the processing of personal data.[80] This law has since been amended several times. The current version includes provisions on the legal grounds for processing personal data, obligations for data controllers and the rights of data subjects, sanctions concerning the use of personal data, provisions specifically for personal medical data, provisions regarding data transfers outside the European Union and provisions concerning CNIL.[81]

The highest French constitutional court, the *Conseil Constitutionnel*, issued a ruling in July 2015 regarding the French law governing the intelligence and security agencies. In this ruling, the court declared specifically which provisions of this law are in accordance with the French Constitution and which provisions or parts of provisions are not. The court ruled that most of the provisions were in accordance with the French Constitution, and the methods of data collection, processing and use they contain are therefore allowed.[82] Parts of the provisions that were not deemed permissible include permission from the Minister for monitoring communications sent from or received in other countries, with a view to safeguarding fundamental national interests. What is for example permitted, subject to certain conditions, is the collection of data in real time in order to prevent terrorism, and obliging service providers to identify connections (the parameters of which are set out in the order) which suggest a terrorist threat.[83]

3.5 GERMANY

3.5.1 GOVERNMENT INITIATIVES

The German Federal Ministry for Education and Research (Bundesministerium für Bildung und Forschung) is the Ministry most concerned with Big Data. According to this Ministry, Big Data is synonymous with: "*den intelligenten Umgang mit solchen großen oder auch heterogenen Datenmengen* (intelligent use of large or heterogeneous datasets)".[84] This is therefore the terminology which the Ministry continues to use for Big Data. In 2013 the Ministry launched a funding project for Big Data projects, as a part of a funding programme for ICT running until 2020. Universities or research institutes were able to apply for funding for Big Data projects under this programme.[85] In 2014 the Ministry announced that it would be providing finance for the construction of two Big Data centres : the Berlin Big Data Centre and the Competence Center for Scalable Data Services in Dresden.[86]

In March 2015 the Ministry made a further important announcement regarding Big Data. According to the Ministry, Big Data provides great opportunities for the ICT sector but is also one of the major challenges of today. On the one hand, Big Data opens the way to scientific progress and innovation which will improve the competitive position of German business and science, but on the other hand

data and Big Data technology need to be used wisely.[87] In addition to building the two centres mentioned above, the Ministry will promote further research in support of Big Data, as illustrated for example by the funding initiative launched in 2013. Specifically, the Ministry will focus attention on 'Industry 4.0' projects and on the bio- and geosciences.[88] The Ministry emphasizes the need for sensible use of Big Data and has announced research specifically focusing on this aspect.[89] The German government refers to a 'fourth industrial revolution', in response to which it has launched the 'Industry 4.0' project. In the context of this project the Ministry of Education and Research has received funding from the government to invest in this type of industry, for example in Big Data.[90]

In May 2015 the Ministry issued a press release announcing a specific research project focusing on Big Data.[91] This project, dubbed ABIDA ('*Interdisziplinäre Analyse der gesamtgesellschaftlichen und wirtschaftlichen Folgen beim Umgang mit großen Datenmengen*'), will encompass interdisciplinary research into the social and economic impact of large datasets, and will seek to map Big Data clearly in order to demonstrate how best to handle Big Data. According to the Minister, the benefits and risks need to be made clear; technological progress must fit in with the social and legal order and the current system of values.[92] This four-year project is funded by the Ministry of Education and Research, in addition to the Big Data initiatives referred to above.

3.5.2 LEGISLATION AND CASE LAW

The central data protection legislation in Germany is the *Bundesdatenschutzgesetz*, originally dating from 1990. This law regulates the principles surrounding data protection, the legal grounds for data processing, the rights of data subjects, the setting up of a national data protection authority and the supervision of these processes. The law creates a clear distinction between data processing by the government and data processing by private actors or public institutions in a commercial setting, with separate provisions for the two categories.[93] The 'personality right' (*Persönlichkeit*), as enshrined in Article 2 of the German Constitution, is also relevant in the context of the right to privacy.[94]

In August 2014 the German Ministry of Internal Affairs organised an expert meeting with several parties to discuss the benefits and risks of Big Data. This meeting was held in the context of the *Digital Society Forum*.[95] The experts indicated that there are problems with the current data protection framework, especially regarding the principles of data minimization and purpose limitation. The Minister of Internal Affairs emphasized that the aim of data protection must be kept in mind, namely protecting privacy and the right to personality. These two aspects are also of importance in reforming the European legislation in the area of privacy and data protection, according to the Minister. He has proposed a new principle for the new

legislation: minimizing risk.[96] He has also announced that Germany will present proposals to include provisions concerning pseudonymization and profiling. This, it is hoped, could mitigate the risks of privacy violations.[97]

3.6 INDIA

3.6.1 GOVERNMENT INITIATIVES

The Indian Ministry of Science and Technology has started a Big Data initiative. The Ministry lists four focus areas for the development of a sustainable data analysis system: creating a strong pool of talent; creating collaborations between different types of organizations for data analysis to identify constraints and best practices; developing the capacity and skills needed for an innovation culture; and creating value in order to be able to measure the impact of analysis and create legitimacy within organizations. The Ministry believes that Big Data offers opportunities for generating high profits and that carving out a strong position for India in the area of data analytics can enhance the analytical capabilities of companies.[98] With this initiative, the government is seeking to achieve five goals: stimulating the use of Big Data nationwide as well as by the government; identifying the extent of Big Data in terms of market share, stakeholders and an optional policy framework, etc.; carrying out a survey to map out the scope for demand and skills in this area; carrying out an analysis to identify where skills and policy are still lacking; devising a strategy and formulating an action plan at microlevel to determine the most appropriate role for stakeholders.[99]

Aadhaar is a government-wide project being implemented by the Unique Identification Authority of India. It involves the collection of biometric and demographic data of the Indian population. Inhabitants of India who enrol in this system – enrolment is voluntary – receive a unique identification number from the government which can be used for all kinds of applications used for identification.[100] One use of Aadhaar is for establishing identity in relation to 'micro-payments', with a view to providing better access to financial services for of people living in rural areas. The Aadhaar identification number enables the identity of people in remote regions to be established at a distance, and also l the costs thanks to benefits of scale, making it easier to offer financial services to poorer people.[101] Other sectors where Aadhaar offers solutions include demographic planning, payment of social security benefits and improving the identification of welfare recipients by deleting duplicate identities.[102] The government's administrative processes should also become more efficient because government institutions now have access to all the relevant information in one place.[103]

3.6.2 LEGISLATION AND CASE LAW

Although there has been no specific legislation in the area of privacy and data protection in India for a long time, this has changed in the past few years. In 2010 the law which introduced the Aadhaar system came into force. In 2011 the Ministry of Communications and Information Technology (DeitY) published legislation governing the right to privacy and establishing rules regarding data protection: the "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011".[104] Since 2014 even more attention has been paid to this area of law and a draft bill has been added, the 'Privacy Bill 2014'. This is not officially accessible to the public, but according to the Indian Centre for Internet Society it has been leaked several times.[105] According to a government press agency this law, which is intended to protect individuals from an unlawful invasion of their privacy, is currently in the consultation phase.[106] In 2012 the Ministry of Science and Technology developed with a national policy for data sharing and accessibility. The government's aim with this policy is to make large amounts of non-sensitive data held by the government more accessible to society. The policy is being implemented by making datasets public on the website https://data.gov.in.[107]

3.7 ISRAEL

3.7.1 GOVERNMENT INITIATIVES

The Israeli Ministry of Health sent out a tender in August 2015 for a partner in Big Data analytics. The Ministry has an enormous dataset containing all the medical data on the Israeli population as well as data on the health care system. The Ministry wants to put this dataset to good use and to be able to translate it into specific recommendations.[108] According to the Ministry, the potential of this data lies in supporting health care functions (such as help in clinical decision-making processes, disease monitoring and proactive health care).[109]

Another government sector where Big Data plays an even greater role is defence. Attention was already being given in 2012 to expanding the digital communication and information system to improve the accessibility of the growing body of logistical data. Specific attention is being paid to the security of the data, as the amount of data increases and more of it is collected centrally.[110] In 2013 it was officially announced on the Israeli Defence Forces (IDF) blog that the cyber domain is now seen as a legitimate field of activity for the armed forces alongside the traditional domains of land, sea and air. The department responsible for this is the 'Lotem' unit, part of the 'C4i Technological Division'. C4i is the department of the IDF that is specifically engaged in information and computer technology.[111] An interview with the commander of this unit makes clear that it is no longer just about passing

on information to divisions of the armed forces. Rather, C4i should be seen as a tool which can be deployed in the area of Big Data analytics. The intention is that by 2015 the IDF will have a cloud in which all the data is stored.[112]

In February 2015 the Matzpen Unit, a software unit within the IDF which operates under the Lotem Unit, received compliments from the head of the IDF for the important role that software had played in the success of 'Operation Protective Edge'. The software unit is regarded as essential within the IDF, partly also due to earlier successes. One of the software programs used in this operation collects large amounts of data from various sources on one screen, following which a selection can be made of information that will be subjected to further analysis by senior officers. The system is appropriately called: 'Crystal Ball'.[113] Another system was also deployed, using GPS data, which enables the location of soldiers to be displayed along with information about the terrain and surroundings of that location to facilitate decisions as to which troops to deploy. The IDF has also made clear to the outside world that these systems, and a number of secret systems, are based on Big Data.[114] The troops in the field also wear sensors, and all this data is used in achieving optimum troop deployment , and to enable potential problems to be predicted and preventive action to be taken.[115] Following the success of the operations and the internal compliments received by the software unit, courses on these themes will be offered to students.[116]

In March 2015 the Lotem Unit announced to *The Jerusalem Post* that the Israeli army is working on the development of an intranet. It will be launched under the name *Jointness*. The idea is to share as much information as possible between different divisions of the armed forces. The focus is on making information available in real-time. There is even talk of a *combat computing cloud*, a data centre which will make various tools available to troops in the field. The intranet will also offer downloadable applications for IDF personnel. The need for such an intranet became clear due to the leading role played by technology successful Operation Protective Edge.[117]

3.7.2 LEGISLATION AND CASE LAW

The right to privacy is enshrined in Section 7 of the Basic Law on Human Dignity and Liberty.[118] In 1981 a law was also introduced which is tailored specifically to this right, the Protection of Privacy Law 5741 – 1981.[119] This law has four main topics: infringements of the right to privacy; protection of privacy in databases; possible defences and exceptions for violations of privacy; and the provision of information or data by government institutions.[120] To implement this law, special legislation was drafted governing data flows from Israel to other countries, for example stipulating that the country that receives the data must be able to guarantee an adequate level of data protection.[121] In 2010 an amendment to the privacy legislation was introduced, adding provisions relating to the security of databases.[122]

3.8 JAPAN

3.8.1 GOVERNMENT INITIATIVES

The Japanese Prime Minister delivered a speech at the 'New Economy Summit' in 2014, in which he stated that in order to achieve its economic goals the Japanese government was among other things making changes to optimize the IT sector. The law on the protection of personal data would be changed to make it easier to use personal information as part of Big Data.[123] In 2001 the 'IT Strategic Headquarters' was set up established within the Japanese Cabinet.[124] In 2012 this agency published an open data strategy for the government, in which it argued that government data is a public asset and that the sharing and use of that asset should be encouraged. The strategy discussed existing initiatives in this area, mainly relating to the sharing of data and making government data accessible in the light of the aftermath of the major earthquake in 2011. It is also stated that sharing of data between governments and private parties could improve government service delivery.[125]

The Japan Science and Technology Agency (JST) is the body responsible for implementing the technology policy of the Japanese government. One of JST's research programmes, 'CREST', involves team-based research to achieve the strategic goals of the government. Programme carries out a great deal of research on Big Data, under the auspices of two main projects: 'Advanced Application Technologies to Boost Big Data Utilization for Multiple-Field Scientific Discovery and Social Problem Solving' and 'Advanced Core Technologies for Big Data Integration'.[126]

3.8.2 LEGISLATION AND CASE LAW

The Act on the Protection of Personal Information was adopted in Japan as long ago as 2003.[127] In 2013 the IT Strategic Headquarters published an amendment involving various legal provisions governing privacy and data protection, entitled 'Directions on Institutional Revision for Protection and Utilization of Personal Data'. In 2014 the Headquarters also published a summary of the main points of this policy.[128] The explanation of the main points includes a discussion of the technological developments which have taken place since the data protection law of 2003, including Big Data. According to the IT Strategic Headquarters, there are currently obstacles to the use of personal data. It also felt that organizations which abide by the law and do not violate rights would be concerned about the critique on privacy violations and the use of personal data, giving rise to a grey area and leading to sub-optimum use of the data.[129] In practice, however, the growth envisaged by the Japanese government requires the optimum use of personal data and facilitating the development of Big Data.

The government therefore wishes to remove these obstacles. In parallel with this, the government believes that violations of rights should be prevented and that an environment should be created in which personal data and privacy are safeguarded but in which this personal data can also be used for innovation.[130] Specifically, there are four areas that need to be addressed : first, action needs to take to tackle the grey area, where there is a great need for clarity ; second, in order to facilitate swift action it is necessary to look at other solutions besides legislation, which proceeds at a slow pace ; third, the system needs to be enforced ; fourth, there is a need for international harmonization of the system of data sharing.[131] The new framework brings changes on three main points: creating a system in which personal data can be used without the consent of the data subject; establishing a system for voluntary action and for facilitating initiatives by private actors; and setting up a system of enforcement with independent third-party supervision.[132]

3.9 SOUTH AFRICA

3.9.1 GOVERNMENT INITIATIVES

With the Square Kilometre Array (SKA), a large multi-radio telescope project, South Africa is seeking to put itself on the map as a Big Data hub. Further goals of this project are to reduce poverty and improve the country's economic competitiveness. The Minister of Science and Technology has stated the following in this regard:

"We hope that, through human capital development, innovation, value addition and industrialisation in alignment with STISA, we will be able to uplift large sections of Africa's people. Diversifying our economies and broadening our sources of growth and sustenance will help us to address poverty and foster both social transformation and economic competitiveness on the continent."[133]

Part of this project will involve building the largest radio telescope in the world, two parts of the system that are responsible for receiving signals are being built in South Africa and one part in Australia. Satellites have been built since 2013 , which together will form the MeerKAT in 2016. This radio telescope will be incorporated in the SKA later. It is an enormous project, on which a total of eight African countries are working together.[134] The South African government believes the project is ambitious:

"The amounts of data being collected and transmitted by the SKA in a single day would take nearly two million years to play back on an iPod. This means the project requires supercomputing power and Big Data management and analytics capabilities on an unprecedented scale." [135]

According to the government, the development of human capital as a consequence of this project is according to the government already apparent: students are being trained to give them the necessary skills and knowledge in this area. There is also an 'African SKA Human Capital Development Programme', which has already provided hundreds of scholarships. In addition , the project has created many jobs.[136]

The data science capacity that comes with the SKA project must be provided by a network of universities, grouped together in the 'Inter-University Institute for Data-Intensive Astronomy (IDIA)', which was launched in September 2015. This network brings together research in the fields of, astronomy, computer science, statistics and 'eResearch' technologies. According to the Minister of Science and Technology, this collaborative data research and educational project has an impact that extends beyond astronomy alone, and should foster innovation in Big Data outside this field as well. It will also contribute to the research expertise of South Africa. Professors at the universities forming part of this network also emphasize that local know-how and capacity are being developed and that local infrastructure for Big Data is also being built, giving South Africa the opportunity to play a part on the global stage in data-intensive research with data processing and its universities.[137]

3.9.2 LEGISLATION AND CASE LAW

The right to privacy is explicitly enshrined in Article 14 of the South African Constitution.[138] South Africa introduced a law in 2013 to protect personal information, the Protection of Personal Information Act 2013.[139] The preamble of this Act states that the right to privacy is laid down in Article 14 of the South African Constitution and emphasizes that the right to privacy also includes "a right to protection against the unlawful collection, retention, dissemination and use of personal information". In this model of legislation the right to privacy and data protection are inextricably linked. This Act contains provisions regarding the minimum conditions for the processing of personal data, the supervisory authority for data protection, which drafts codes of conduct, the rights of individuals regarding spam and automated decision-making, and provisions on flows of personal data to other countries.[140]

3.10 UNITED KINGDOM

3.10.1 GOVERNMENT INITIATIVES

In 2013 the British government announced that it regarded eight technologies as extremely important, including Big Data.[141] According to the government, these eight technologies are crucial for the United Kingdom because they are technologies in which the UK plays a leading role in research, have applications in several industries and are technologies which offer scope for advances in the commercial sector.[142] The British government also published a strategy for Big Data: 'Seizing

the data opportunity. A strategy for UK data capability'.[143] In the foreword to this strategy , the Minister for Universities and Science and the Minister for Skills and Enterprise state the following about the increasing importance of data:

"Governments around the world must change the way they engage with citizens, the way they develop policy and deliver services, and the way they are held to account.(…) The UK government is determined to position the UK to make the most of the data revolution."[144]

With regard to Big Data and the decision to include it as one of the eight key technological developments, they state that: "(…)its potential impact is so significant that it could transform every business sector and every scientific discipline".[145] Consequently, the Minister of Universities and Science announced a new investment of £73 million in Big Data in February 2014.[146] These investments are as follows: The Medical Research Council is investing in bio-informatics for the processing of biological data, which among other things will lead to a better understanding of diseases; the Arts and Humanities Research Council is investing in a number of open data projects, whereby large datasets are made accessible to the public; the Economic and Social Research Council is investing in four new research centres, in which data held by private companies and local authorities that has not previously been made available is made accessible for research; the Natural Environment Research Council is using the investments to fund 24 projects to help researchers obtain environment data.[147] In addition , the government invested £159 million in high-grade computer and network infrastructure in 2011; £189 million in Big Data and energy-efficient computing in 2012; £10.7 million in a centre for Big Data and space technologies in 2013; £42 million in an Alan Turing Institute in 2014 for the analysis and application of Big Data; and £50 million in the 'Digital Catapult', in which researchers and the business sector are working together to develop innovative products.[148]

The 'Big Data for Law' is an interesting project, for which the National Archives receive financial support from the Arts and Humanities Research Council for use on Big Data. This project is aimed at bringing the government's online search engine for legislation into line with the digital era, including downloadable data, online tools and open source tools. The data research infrastructure for legislation which will result from this project will open the way for Big Data research on legislation.[149]

The UK Information Commissioner's Office (ICO), the body responsible for overseeing privacy and data protection, published a paper on Big Data in 2014,[150] in which it describes which of the provisions set out in the Data Protection Act 1998 are specifically relevant for Big Data. According to the ICO, the advantages of

Big Data and the principles of data protection can both be maintained.[151] Since this is a general paper on the topic, not a ruling by the ICO in a specific case, this paper will be discussed on the next sub-section.

The Parliamentary Office of Science and Technology carried out research on Big Data and public policy on Big Data in several sectors in 2014. This led to the publication of nine 'POSTnotes', documents consisting of a few pages and focusing on Big Data in various sectors. The topics addressed in these short information documents are as follows: an overview and explanation of Big Data; social media and Big Data; Big Data and business; Big Data and crime and security; biobanks; Big Data and open data in transport; smart metering of energy and water; Big Data and public health; and environmental citizen science. Each POSTnote gives an explanation of the potential of Big Data in that specific sector; some of them also detail specific applications of the government or private sector, as well as the risks.[152]

The POSTnote focusing on Big Data and crime and security gives an example of the use of Big Data by the police. As part of a pilot study, software has been developed to predict the locations of burglaries. Two British police forces are using software developed for 'predictive policing' to predict the locations of crimes.[153] The British tax and customs authority, HMRC, uses a Big Data system, 'Connect', which combines and analyses all the data held by HMRC. This Big Data system is deployed to detect tax fraud and evasion and is claimed to have led to the recouping of £2.6 billion in unpaid taxes. The system reveals relevant information during searches which would have been much harder to identify otherwise. Complex analysis can be performed on multiple datasets simultaneously and profiles can be constructed which reveal patterns that point to a certain type of crime.[154]

In the area of transport, Big Data analysis is used on 'smart motorways' by the government agency responsible for motorways. Traffic is managed using data from cameras and sensors which calculate the ideal speed for optimum traffic flow. This data is also shared with private parties, for example using the government's open data website.[155]

The use of biobanks is, in which all kinds of biological and medical data is stored, is at an advanced stage in the United Kingdom. One such biorepository' is the UK Biobank, in which medical data and samples are stored from about 500,000 volunteers for later use in research on all manner of diseases.[156] One of the funders of this biobank is the British Department of Health. Research using this data is now under way.[157]

3.10.2 LEGISLATION AND CASE LAW

The Data Protection Act 1998 is the UK legislation that is relevant for privacy and personal data protection. There is also the Human Rights Act 1998, Section 8 of which enshrines the right to protection of personal and family life, including the right to protection of correspondence. For telecommunications data, the 2000 Regulation of Investigatory Powers Act' is of importance, while the Intelligence Services Act 1994 is relevant for the intelligence and security agencies.[158] After the European Data Retention Directive was declared invalid, the Data Retention and Investigatory Powers Act came into force in 2014. This Act will expire in 2016.[159]

In 2014, amendments were made to legislation in the area of intellectual property, for example the Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations 2014.[160] These Regulations intro an exception to copyright for data mining,[161] allowing researchers to make a copy of a copyright-protected work provided they intend to use this copy for data mining without commercial gain.[162]

The British Parliament has asked the Law Commission, the body that advises the government on legal reforms to review the legal framework for sharing data between public bodies. In July 2014 the Commission released its report containing three recommendations. First, it recommended reforming the law completely to create a clear legal structure for data sharing, including modernisation and simplification of the current provisions regulating the sharing of data. Second, the Commission recommended that the reforms should go beyond data sharing between public bodies to include the sharing of information between public bodies and other organisations carrying out public functions. Finally, the reforms should be carried out in collaboration between the Law Commission of England and Wales, the Scottish Law Commission and the Northern Ireland Law Commission. Aside from these recommendations, the Commission also advised making use of 'soft law', offering advice and training to personnel and sharing best practices between government agencies.[163]

In 2015, the case of Google Inc v Vidal-Hall & Others was heard by the Court of Appeal. The case related to data protection and the Data Protection Act 1998;[164] users of Apple's Safari browser argued that the Data Protection Act 1998 had been infringed because Google was collecting information via the browser.[165] The Court ruled that browser information can be regarded personal data and that abuse of personal data should be regarded as a tort.[166] In previous cases, such as Douglas v Hello!, a tendency was already visible towards greater safeguarding of privacy by judicial precedent.[167] With regard to data protection, the High Court pronounced a verdict in July 2015 in the case of Davis & Others v SSHD in relation to the Data Retention and Investigatory Powers Act 2014. In this case the Court declared this law partially invalid due to conflicts with European law, and specifically the section

in which the competence is established to request telecommunications service providers to retain communications data. According to the Court, there are no clear rules limiting the access to and use of this data for the purpose of dealing with serious crime. In addition, there is no independent judicial or administrative supervision to check in advance whether the access to the data meets this purpose.[168]

3.11 UNITED STATES

3.11.1 GOVERNMENT INITIATIVES

In March 2012 the Obama Administration launched the 'Big Data Research and Development Initiative'. Under this initiative, six federal government departments and agencies announced the investment of 200 million dollars in additional improvements to the processing of enormous volumes of data.[169] In the factsheet dated 29 March 2012, 'Big Data Across the Federal Government', dozens of ongoing government projects and partnerships related to Big Data are mapped, in all sectors.[170] On 17 January 2014 the US president ordered the Administration to conduct '90-day review of Big Data and privacy'; the results were published in May 2014.[171]

The review produced five overarching conclusions. First, more research must be carried out on the protection of privacy, and action should be taken in the area of legislation on the protection of privacy. The Consumer Bill of privacy Rights is seen as particularly important in this context.[172] Second, there should be more attention for the responsible handling of data collected in the context of education, especially data regarding children.[173] Third, the federal government is advised to be on its guard for discrimination of citizens, which can be caused by Big Data analytics.[174] Fourth, the authorities responsible for enforcement and safety are advised to make maximum use of the legal possibilities for Big Data analytics.[175] Finally, the review concludes that government data should be regarded as a national resource and should as far as possible be published and shared with the public.[176]

Linked to this, a study was conducted by the President's Council of Advisors on Science and Technology. The results of this were published in a report in May 2014, and again five recommendations were made: policies should devote more attention to the use of Big Data rather than the analysis and collection of data; policy should be technology-neutral; there should be more research on privacy-related technologies; education and training concerning privacy protection should be encouraged; and the United States should take charge in polices that promote privacy-protecting technologies.[177]

The above initiative was not only directed at the government, but also appealed to others to engage in the possibilities of Big Data:

"We also want to challenge industry, research universities, and non-profits to join with the Administration to make the most of the opportunities created by Big Data. Clearly, the government can't do this on its own. We need what the President calls an "all hands on deck" effort".[178]

John Podesta, responsible for the research by the Obama Administration, published a blogpost on 1 May 2014 on the results of the Working Group Review. In his blog he describes Big Data as a technology of vital importance. Podesta refers to the destruction and suffering caused by tornados and implicitly to the predictive power of Big Data to prevent potential damage.[179] Big Data, he argues, offers possibilities for each sector and, specifically, could potentially save lives, allow the economy to function better, and make the government more efficient.[180] However, his report of the findings of the Working Group is more nuanced. It acknowledges that Big Data also carries risks: "…how we protect our privacy and other values in a world where data collection is increasingly ubiquitous and where analysis is conducted at speeds approaching real time".[181] Specific concerns are whether a system of notifying users and asking permission to collect and use data about them is sufficient. Another specific concern is the possibility of discriminatory outcomes of analysis and the opportunity to evade the protection of rights of citizens.[182]
The president announced the review on 17 January 2014 during a speech to the Justice Department. The speech was mainly focused on the way forward for the intelligence agencies.[183] In his speech the president stated that the processes of the intelligence agencies devote attention to the privacy of citizens. Specifically, he went into the reasons why a review of Big Data had been started:

"…look how the challenges inherent in Big Data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security."[184]

Some examples can also be found of trials with Big Data in the area of security in the United States. For example, police forces used Big Data analytics to predict the odds that an individual will become involved in criminal activity.[185] An example is Philadelphia, where the police used a tool to predict the chance of repeated offences.[186]

3.11.2 LEGISLATION AND CASE LAW

The United States does not have an overarching law for the regulation of privacy, and certainly not for the specific regulation of Big Data. Besides the constitutional protection, the United States has a system of sector-specific regulation of privacy risks, for example in the area of healthcare[187] and the collection of data by federal agencies.[188] In 2012 more attention was given to integrated privacy legislation. The White House published a privacy blueprint, including a Consumer Bill of Privacy

Rights. This is not legislation in the sense of being enforceable, but more of a guideline for the business sector. The government acknowledged that the amount of data being collected today creates a need for more clarity for citizens and more safeguards to protect privacy. For example, section 3 (c) of the guideline states that:

"There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. This growth has the potential for great benefits to human knowledge, technological innovation, and economic growth, but also the potential to harm individual privacy and freedom."[189]

Although the term 'Big Data' is not explicitly mentioned here, this provision demonstrates that the government acknowledges that processes such as Big Data analysis create opportunities but also require more legal protection of the privacy and freedom of the citizen. A court case on limiting the effects on large-scale location data collection by the police was The United States v. Jones from 2011. The Supreme Court ruled in this case that following a person and collecting data through GPS constitutes a search and a warrant is therefore needed before this can take place.[190]

Another interesting case is Sorrell v. IMS Health Inc., which was also heard by the Supreme Court in 2011.[191] This case concerned a law of the State of Vermont governing the confidentiality of medical prescriptions. Pharmacies were selling information about the prescription behaviour of physicians to parties specialising in data mining, who subsequently drafted reports based on this data for pharmaceutical companies. However, according to the Vermont legislation, permission is needed from the prescribing physician before this information can be sold by pharmacies, made public for marketing by pharmacies, or used for marketing by pharmaceutical companies. According to the companies which engaged in data mining and the pharmaceutical companies, this provision violated their freedom of expression. The Supreme Court ruled in their favour, stating that this state law did indeed violate their freedom of expression.[192] In this scenario, involving the commercial use of medical data, there is scope for large-scale data collection and analysis.

Recently, of course, there have also been several court cases which have ruled against data collection by the National Security Agency (NSA). One of those cases was ACLU v. Clapper, which was heard by the Second Circuit Court of Appeals. According to this Court, this case demonstrates how hard it is to strike the right balance between state security and the privacy of the citizen given the current surveillance capabilities. On 7 May 2015, the Court ruled that the large-scale collection of metadata concerning telephone records by the NSA is unlawful; these procedures are not covered by Section 215 of the Patriot Act.[193] However, this Act expired on 1 June 2015.[194] it was replaced on 2 June by the Freedom Act 2015, but

this Act stipulated that the collection of metadata could only continue after 180 days.[195] At the same time, the Foreign Intelligence Surveillance Court ruled that the collection of metadata could continue.[196] The debate concerning the admissibility of large-scale data collection and processing by intelligence and security agencies has thus not ended yet.

As far as we are aware, there is no single national data protection authority in the United States akin to those found in many European countries, but the Federal Trade Commission can take on cases relating to Big Data, for example cases concerning data brokers which do business with credit providers. According to the Federal Trade Commission, these are for example cases where credit providers buy data on consumers from data analysis companies and from data brokers, in order to use this data to help in making decisions whether or not to provide credit. The Federal Trade Commission has dealt with over 100 cases in relation to the Fair Credit Reporting Act. The outline of these cases is that these types of scenarios will fall within the scope of this law.[197] Cases can also come before the Federal Trade Commission based on the Equal Credit Opportunity Act, when Big Data is used in such a way that certain persons are excluded from credit on the basis of gender or race, for example.[198] No examples are given of specific cases coming before the Federal Trade Commission in relation to Big Data and one of these two laws. According to the chairman of the Federal Trade Commission, efforts should go beyond merely enforcing the existing legislation, and elaborate privacy and data security regulation is needed.[199]

3.12 REFERENCES

3.12.1 AUSTRALIA

Reports

- Australian Government, 'Australian Public Service Better Practice Guide for Big Data', 2015: www.finance.gov.au/sites/default/files/aps-Better-Practice-Guide-for-Big-Data.pdf?v=1.
- Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013: www.finance.gov.au/sites/default/files/Big-Data-Strategy_0.pdf.

Websites, blogs & online articles

- Australian Government, ComLaw, Guidelines for the Conduct of the Data-Matching Program, 1994: www.comlaw.gov.au/Details/F2009B00268.
- Australian Government, Office of the Australian Information Commissioner, Guidelines on Data Matching in Australian Government Administration, June 2014: www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/data-matching-guidelines-2014.

- Australian Government, Office of the Australian Information Commissioner, 'Privacy Law': www.oaic.gov.au/privacy-law/.
- Australian Government, Office of the Australian Information Commissioner, 'Privacy fact sheet 17: Australian Privacy Principles', January 2014: www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.
- CISRO, 'Vizie: Connecting with customers through social media': www.csiro.au/en/Research/dpf/Areas/The-digital-economy/Digital-service-delivery/Vizie.

Legislation

- Privacy Act 1988: www.comlaw.gov.au/Details/C2015C00534.
- Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum: http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728%22.

3.12.2 BRAZIL

Websites, blogs & online articles

- DataViva, 'About the Visualizations': http://en.dataviva.info/about/apps/about/.
- DataViva: http://en.dataviva.info/about/contact/.
- Microsoft, 'Microsoft and São Paulo government partner to release crime monitoring system', 16 April 2014: http://blogs.microsoft.com/blog/2014/04/16/microsoft-and-so-paulo-government-partner-to-release-crime-monitoring-system/.
- Ministry of Labor and Employment, 'RAIS': http://en.dataviva.info/about/data/rais/.
- Pensando o Direito, 'Debate, Proteção de Dados Pessoais': http://pensando.mj.gov.br/dadospessoais/english-information/.
- Pensando o Direito, 'Proteção de Dados Pessoais': http://pensando.mj.gov.br/dadospessoais/.
- Secretaria de Segurança Pública do Estado de São Paulo, 'SP ganha nova etapa do Detecta, sistema de monitoramento criminal', 16 April 2014: www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=33930.

Legislation

- Draft law, 'On the processing of personal data to protect the personality and dignity of natural persons': http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/02/Brazil_pdp_bill_Eng1.pdf.

3.12.3 CHINA

Reports

- Li Keqiang Premier of the State Council, 'Report on the work of the government, Delivered at the Second Session of the Twelfth National Peoples Congress on March 5, 2014': http://online.wsj.com/public/resources/documents/2014GovtWorkReport_Eng.pdf.

Websites, blogs & online articles

- The National People's Congress of the People's Republic of China, 'Xinhua Insight: China considers boosting credit system', 8 March 2014: www.npc.gov.cn/englishnpc/Special_12_2/2014-03/08/content_1843931.htm.
- The National People's Congress of the People's Republic of China, 'China's legislature adopts online info rules to protect privacy', 5 January 2013: www.npc.gov.cn/englishnpc/news/Legislation/2013-01/05/content_1750014.htm.
- The State Council of the People's Republic of China, 'Big Data plays bigger role in China's administration management', 5 July 2015: http://english.gov.cn/news/top_news/2015/07/05/content_281475140856686.htm.
- The State Council of the People's Republic of China, 'China to develop modern circulation, Big Data industries', 19 August 2015: http://english.gov.cn/premier/news/2015/08/19/content_281475171439937.htm.
- The State Council of the People's Republic of China, 'China unveils 'Internet Plus' action plan to fuel growth', 4 July 2015; http://english.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm.
- The State Council of the People's Republic of China, 'New social credit code system to increase administrative efficiency', 17 June 2015: http://english.gov.cn/policies/latest_releases/2015/06/17/content_281475129090642.htm.
- The State Council of the People's Republic of China, 'Opinion released on use of Big Data', 1 July 2015: http://english.gov.cn/policies/latest_releases/2015/07/01/content_281475138273106.htm.
- The State Council of the People's Republic of China, 'Premier asks govt departments to implement Big Data plan', 20 August 2015: http://english.gov.cn/premier/news/2015/08/20/content_281475171811356.htm.
- The State Council of the People's Republic of China, 'Premier promotes Big Data', 18 June 2015: http://english.gov.cn/premier/news/2015/06/18/content_281475129712178.htm.
- The State Council of the People's Republic of China, 'Vice-premier stresses importance of Big Data development', 27 May 2015: http://english.gov.cn/state_council/vice_premiers/2015/05/27/content_281475115610715.htm.

3.12.4 FRANCE

Reports

- Commisariat général à la stratégie et à la prospective, 'La Note d'Analyse', no. 8, November 2013: www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/2013-11-09-Bigdata-na008.pdf.
- Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data Feuille de route', 2 July 2014: www.economie.gouv.fr/files/files/pdf/Feuille-de-route_big-data151214.pdf.

Websites, blogs & online articles

- Direction Générale des Enterprises, 'Etude prospective sur les mutations des services postaux': www.entreprises.gouv.fr/services/etude-prospective-sur-mutations-des-services-postaux#_ftnref3.
- Direction Générale des Enterprises, 'Évolutions technologiques, mutations des services postaux et développement de services du futur', 1 July 2013: www.entreprises.gouv.fr/etudes-et-statistiques/evolutions-technologiques-mutations-des-services-postaux-et-developpement-ser.
- Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data : la feuille de route entre en action', 19 December 2014: www.economie.gouv.fr/big-data-feuille-route-en-action.
- Le Comité de Pilotage de la Nouvelle France Industrielle, 'La Nouvelle France Industrielle, phase 2': www.economie.gouv.fr/nouvelle-france-industrielle.
- Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

Legislation

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés: www.legifrance.gouv.fr/affichTexte.do?cidTexte=jorftext000000886460.

Jurisprudence

- Conseil Constitutionnel 23 juli 2015, Décision n° 2015-713 DC, Communiqué de presse: www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/communique-de-presse.144139.html.
- Conseil Constitutionnel 23 juli 2015, Décision n° 2015-713 DC: www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html

3.12.5 GERMANY

Websites, blogs & online articles

- Bundesministerium des Innern, 'Expert group on Big Data as a challenge for data protection', 21 August 2014: www.bmi.bund.de/SharedDocs/Kurzmeldungen/en/2014/09/expert-group-on-big-data-as-a-challenge-for-data-protection.html.
- Bundesministerium für Bildung und Forschung, 'Bekanntmachung', 20 February 2013: www.bmbf.de/foerderungen/bekanntmachung.php?B=824.
- Bundesministerium für Bildung und Forschung, 'Big Data - Management und Analyse großer Datenmengen': www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html.
- Bundesministerium für Bildung und Forschung, 'Big Data': www.softwaresysteme.pt-dlr.de/de/big-data.php.
- Bundesministerium für Bildung und Forschung, 'Die Macht von Big Data entschlüsseln und steuern', 6 May 2015: www.bmbf.de/de/die-macht-von-big-data-entschluesseln-und-steuern-1033.html?hilite=big+data.
- Bundesministerium für Bildung und Forschung, 'Forschung zu Big Data und IT-Sicherheit neu aufgestellt', 10 March 2014: www.bmbf.de/de/forschung-zu-big-data-und-it-sicherheit-neu-aufgestellt-463.html.
- PRNewswire, 'German Government Announces "Production Intelligence": Funding for Jedox's Big Data Project', 13 April 2015: www.prnewswire.com/news-releases/german-government-announces-production-intelligence-funding-for-jedoxs-big-data-project-499530121.html.

Legislation

- Bundesdatenschutzgesetz 2009: www.gesetze-im-internet.de/englisch_bdsg/index.html.
- Grundgesetz für die Bundesrepublik Deutschland: www.bundestag.de/bundestag/aufgaben/rechtsgrundlagen/grundgesetz/gg_01/245122.

3.12.6 INDIA

Reports

- Unique Identification Authority of India, Planning Commission, Government of India, 'Advancing Development Agenda with Aadhaar': https://uidai.gov.in/images/Aadhaar-English.pdf

Websites, blogs & online articles

- Department of Science & Technology, 'Big Data Initiative': www.dst.gov.in/big-data-initiative-1.
- Press Information Bureau, Government of India, 'Right to Privacy Bill', 13 August 2015: http://pibmumbai.gov.in/scripts/detail.asp?releaseId=E2015pr2086.

- The Centre for Internet & Society, 'Leaked Privacy Bill: 2014 vs. 2011', 31 March 2014: http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011.
- Unique Identification Authority of India, 'Aadhaar Usage': https://uidai.gov.in/aadhaar-usage.html.
- Unique Identification Authority of India, 'Aapka Aadhaar': https://uidai.gov.in/aapka-aadhaar.html.

Legislation

- Ministry of Communications and Information Technology, *THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i)*, 11 April 2011: http://deity.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.
- Ministry of Science & Technology, 'National Data Sharing and Accessibility Policy (NDSAP)', 2012: www.dst.gov.in/sites/default/files/nsdi_gazette_0.pdf.

3.12.7 ISRAEL

Websites, blogs & online articles

- A. Rapaport, 'C4I is Shaping the Operational Reality', *Israel Defense*, 2 February 2015: www.israeldefense.co.il/en/content/c4i-shaping-operational-reality.
- D. Shamah, 'IDF winning the war with Big Data', *The Times of Israel*, 24 February 2015: www.timesofisrael.com/winning-the-war-with-big-data/.
- F. Shoihet, 'IDF continues to implement digital communication', *Israel Defense Forces*, 14 October 2012: www.idf.il/1283-17301-en/Dover.aspx.
- *Israel Defense Forces*, 'Hackers Beware: The IDF's Digital Battleground', 9 October 2013: www.idfblog.com/blog/2013/10/09/hackers-beware-idfs-digital-battleground/.
- Ministry of Health, 'Israel's Ministry of Health Big Data Opportunity: Vendor Highlights', Tender 10/2015, August 2015: www.health.gov.il/services/tenders/doclib/com10_2015_19082015.pdf.
- Y. Lappin, 'IDF setting up an operational Internet', *The Jerusalem Post*, 30 March 2015: http://new.jpost.com/landedpages/printarticle.aspx?id=395600.

Legislation

- Basic Law: Human Dignity and Liberty 1992: www.knesset.gov.il/laws/specia L/eng/basic3_eng.htm.
- Draft for the Protection of Privacy Regulations (Information Security in Databases), 5770-2010: http://index.justice.gov.il/En/Units/ilita/Pages/Legislation-and-other-documents.aspx.
- Protection of Privacy (Transfer of Data Abroad) Regulations: http://index.justice.gov.il/En/Units/ilita/Pages/Legislation-and-other-documents.aspx.

– Protection of Privacy Law, 5741 – 1981: http://index.justice.gov.il/En/Units/ilita/Pages/Legislation-and-other-documents.aspx.

3.12.8 JAPAN

Reports

– IT Strategic Headquarters, 'Open Government Data Strategy', 4 July 2012: http://japan.kantei.go.jp/policy/it/20120704/text.pdf.
– IT Strategic Headquarters, 'Policy Outline of the Institutional Revision for Utilization of Personal Data', 24 June 2014: http://japan.kantei.go.jp/policy/it/20140715_2.pdf.

Websites, blogs & online articles

– CREST, 'Advanced Application Technologies to Boost Big Data Utilization for Multiple-Field Scientific Discovery and Social Problem Solving': www.jst.go.jp/kisoken/crest/en/research_area/ongoing/areah25-5.html.
– CREST, 'Advanced Core Technologies for Big Data Integration': www.jst.go.jp/kisoken/crest/en/research_area/ongoing/areah25-6.html.
– IT Strategic Headquarters website: http://japan.kantei.go.jp/policy/it/index_e.html.
– Prime Minister of Japan and His Cabinet, 'New Economy Summit 2014', 9 April 2014: http://japan.kantei.go.jp/96_abe/actions/201404/09nes.html.

Legislation

– Act on the Protection of Personal Information, Act No. 57 of May 30, 2003: www.japaneselawtranslation.go.jp/law/detail/?id=130&vm=04&re=02.

3.12.9 SOUTH-AFRICA

Websites, blogs & online articles

– 'SKA a game changer for African tech', *Business Tech*, 21 September 2013: http://businesstech.co.za/news/columns/45930/ska-a-game-changer-for-african-tech/.
– Naledi Pandor, 'speech 2nd Ministerial Meeting of the Square Kilometre Array (SKA) African Partner Countries', Pretoria, 25 March 2015: www.ska.ac.za/releases/20150409speech.php.
– SKA, 'Everything you wanted to know about the SKA': www.ska.ac.za/qa/.
– SKA, 'The SKA project': www.ska.ac.za/about/project.php.
– *University of Cape Town*, 'Big Data institute will boost SKA', 3 September 2015: www.uct.ac.za/dailynews/?id=9342.

Legislation

– Constitution of the Republic of South Africa, 1996: www.saflii.org/za/legis/num_act/cotrosa1996423/.

– Protection of Personal Information Act 2013: www.saflii.org/za/legis/num_act/popia2013380.pdf.

3.12.10 UNITED KINGDOM

Reports

– HM Government, 'Seizing the data opportunity. A strategy for UK data capability', October 2013: www.gov.uk/government/uploads/system/uploads/attachment_data/file/254136/bis-13-1250-strategy-for-uk-data-capability-v4.pdf.
– Information Commissioner's Office, 'Big Data and data protection', 28 July 2014: https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf.
– Parliamentary Office of Science & Technology, POSTnote, 'Biobanks', July 2014: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-473.
– Parliamentary Office of Science & Technology, POSTnote, 'Big and Open Data in Transport', July 2014: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-472.
– Parliamentary Office of Science & Technology, POSTnote, 'Big Data, Crime and Security', July 2014: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-470#fullreport.

Websites, blogs & online articles

– Biobank, 'About UK Biobank': www.ukbiobank.ac.uk/about-biobank-uk/.
– Department for Business, Innovation & Skills, 'Eight great technologies: infographics', 9 October 2013: www.gov.uk/government/publications/eight-great-technologies-infographics.
– Department for Business, Innovation & Skills, The Rt Hon David Willetts Arts and Humanities Research Council, Economic and Social Research Council, Medical Research Council, Natural Environment Research Council, '£73 million to improve access to data and drive innovation', 6 February 2014: www.gov.uk/government/news/73-million-to-improve-access-to-data-and-drive-innovation.
– Department for Business, Innovation and Skills, E. Vaizet, 'ICT: Written question – 214448', 17 November 2014: www.parliament.uk/written-questions-answers-statements/written-question/commons/2014-11-17/214448.
– Information Commissioner's Office, 'Big Data': https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/.
– Intellectual Property Office and Viscount Younger of Leckie, 'New exceptions to copyright reflect digital age', 1 June 2014: www.gov.uk/government/news/new-exceptions-to-copyright-reflect-digital-age.
– Law Commission 'Data Sharing between Public Bodies': www.lawcom.gov.uk/project/data-sharing-between-public-bodies/.

- Parliamentary Office of Science & Technology, 'Big Data': www.parliament.uk/mps-lords-and-offices/offices/bicameral/post/work-programme/big-data/.
- The National Archives, 'Big Data for Law': www.legislation.gov.uk/projects/big-data-for-law.

Legislation
- The Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations 2014: www.legislation.gov.uk/ukdsi/2014/9780111112755.

Jurisprudence
- England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening): www.bailii.org/ew/cases/EWCA/Civ/2015/311.html.
- England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening), *The Incorporated Council of Law Reporting for England & Wales*: http://cases.iclr.co.uk/Subscr/search.aspx?docID=WLRD2015-156.
- High Court of Justice Queen's Bench Division Divisional Court 17 July 2015, Davis & Ors v SSHD: www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf.

3.12.11 THE UNITED STATES

Reports
- Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
- Executive Office of the President & President's Council of Advisors on Science and Technology, 'Report to the President Big Data and Privacy: a Technological Perspective', May 2014: www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Websites, blogs & online articles
- Edith Ramirez , 'Protecting Privacy in the Era of Big Data', *International Conference on Big Data from a Privacy Perspective, Hong Kong,* 10 June 2015: www.ftc.gov/system/files/documents/public_statements/671661/150610era_bigdata.pdf.
- *Executive Office of the President*, 'Big Data Across the Federal Government', 29 March 2012: www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_fact_sheet_final_1.pdf.

– Geoffrey C. Barnes, Jordan M. Hyatt, 'Classifying Adult Probationers by Forecasting Future Offending. Final Technical Report', March 2012: www.ncjrs.gov/pdffiles1/nij/grants/238082.pdf.
– J. Podesta, *Whitehouse blog*, 'Findings of the Big Data and Privacy Working Group Review', 1 May 2014: www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.
– National Insitute of Justice, 'Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise', *NIJ Journal, 271*, February 2013: www.ncjrs.gov/pdffiles1/nij/240696.pdf.
– The President, *Whitehouse*, 'Remarks by the President on Review of Signals Intelligence', 17 January 2014: www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
– *Whitehouse blog*, 'Big Data is a Big Deal', 29 March 2012: www.whitehouse.gov/blog/2012/03/29/big-data-big-deal.

Legislation
– Consumer Privacy Bill of Rights Act of 2015 (draft): www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
– Patriot Sunset Extension Act of 2011: www.gpo.gov/fdsys/pkg/PLAW-112publ14/content-detail.html.
– Privacy Act 1974 (2015 edition): www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.
– U.S.A. Freedom Act 2015: www.congress.gov/bill/114th-congress/house-bill/2048/text.

Jurisprudence
– Foreign Intelligence Surveillance Court 2 June 2015, Memorandum of Law, no. 15 -75: http://cdn.arstechnica.net/wp-content/uploads/2015/06/15-01-Memo.pdf.
– Supreme court 23 June 2011, Sorrell v IMS Health inc: www.supremecourt.gov/opinions/10pdf/10-779.pdf.
– Supreme court 8 November 2011, United States vs Jones: www.scotusblog.com/case-files/cases/united-states-v-jones/.
– United States Court of Appeals for the Second Circuit 7 May 2015, ACLU v. Clapper: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf.

4 SURVEY

4.1 SURVEY FOR DPA'S ACROSS EUROPE (AUSTRIA)

Dear Mr. van der Sloot,

thank you very much for your e-mail.

Since the Austrian DPA was not confronted with Big Data cases so far and since there is no specific regulation of Big Data in Austria, the DPA will refrain from responding to your request.

Best regards
Dr. Matthias Schmidl

Stv Leiter der Datenschutzbehörde/Deputy Head of the Austrian Data Protection Authority
Hohenstaufengasse 3
1010 Wien
Tel.: +43 1 53115 – 202493
Fax: +43 1 53109 – 202690
E-Mail: matthias.schmidl@dsb.gv.at

4.2 SURVEY FOR DPA'S ACROSS EUROPE (BELGIUM)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

Yes

We have no official national definition. However we follow closely the definitions; The EDPS states on its website "Big Data means *large amounts of different types of data produced at high speed from multiple sources, whose handling and analysis require new and more powerful processors and algorithms. Not all of these data are personal, but many players in the digital economy increasingly rely on the large scale collection of and trade in personal information. As well as benefits, these growing markets pose specific risks to individual's rights to privacy and to data protection"* (https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/big_data)

Also, the Working Party 29 has issued a general statement on Big Data. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf)

The Consultative Committee of the Convention 108 has appointed an expert that has to write a report on Big Data, expected to become public in 2016 (www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/OJ_TPD32(2015)_11%2006%2015_Fr.asp)

2. Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)

Not to our knowledge for the indicated sectors in the strict meaning (there is no obligation to notify our DPA of such projects in these sectors). However in the approach of the fiscal and social fraud, the projects and discussion on the use of Big Data or the steps in this process (profiling, data mining,…) exist since 2012. We have addressed several opinions since 2012 that address a part of the Big Data issue (mainly data mining and profiling)

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

On profiling by facebook : Aanbeveling 04/2015 van 13 mei 2015 uit eigen beweging met betrekking tot 1) Facebook, 2) de gebruikers van internet en/of Facebook alsook 3) de gebruikers en aanbieders van Facebook diensten, inzonderheid social plug-ins, gepubliceerd op www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_04_2015.pdf

At the request of our Commission the inter-university research center EMSOC/ SPION (see www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation) conducted a detailed study into the way in which Facebook deals with its members' personal data. And that of citizens who do not use Facebook or who explicitly opted out of its service.

On profiling of energy and water clients : Advies nr. /2015 van 17 juni 2015 betreffende Hoofdstuk II van het Ontwerp van wet houdende diverse bepalingen, betreffende de verbruiksgegevens van nutsbedrijven en distributiebeheerders

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

We have no judgment yet in the facebook case. We expect that the main discussion will be on the competence of our DPA.

See the media of 15 june 2015 (www.theguardian.com/technology/2015/jun/15/belgium-facebook-court-privacy-breaches-ads).

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)

No. The general data protection law applies, and we expect that de new data protection regulation will be able to provide a partial answer (profiling) to Big Data issues (legal interpretation of the EU legal framework)

6. Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)

Most Belgian projects seem to be still in a pilot phase and the visibility of Big Data in practice is still low (competition issue). Often, the practice is still labeled differently (data mining, profiling,…) Conclusions seem to be premature at this stage until more experience has been obtained on the practical uses of this new practice. (Gartner's 2013 Hype Cycle for Emerging Technologies, www.gartner.com/newsroom/id/2819918). Follow-up research seems necessary.

Thank you to share your findings !

4.3 SURVEY FOR DPA'S ACROSS EUROPE (CROATIA)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

The Republic of Croatia is familiar with the concept of Big Data, and a definition / explanation with which we most agree is from the text "What is really Big Data and where is it used?" By Luka Stepinac from 12. May 2014. published at the www.ictbusiness.info in which stands „Definition that we can find the most often refers to "3V": Volume - a large amount of data collected, processed and made available for analysis; Velocity - continuous collection of large amounts of data in real time; Variety - the data are available in various forms and sources, and in fact are usually unstructured, or, in one sentence, Big Data is a technology that enables the collection and processing of large amounts of structured and unstructured data in real time. "

It is necessary to point out that the Republic of Croatia regularly monitors technological innovations which in most cases allows the use of information from the field of Big Data, and most often in commercial purposes.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

At this moment we do not have an appropriate/adequate information.

3. **Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)**

No.

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words**)

At this moment we do not have an appropriate/adequate information.

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

At the moment, in Republic of Croatia, there is no separate regulations governing the area of the Big Data, but certainly in the part referring to the personal data of natural persons, applies the Law on Protection of Personal Data.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

No.

4.4 SURVEY FOR DPA'S ACROSS EUROPE (DENMARK)

By e-mails dated the 8th of June and 25th of August 2015 the Netherlands Scientific Council for Government Policy has made an inquiry about Big Data practice in Europe.

The Danish Data Protection Agency does not have the resources to answer the questionnaire.

Kind regards,

Morten Tønning
Head of Section, LL.M.

THE DANISH DATA PROTECTION AGENCY
Borgergade 28, 5. sal, 1300 Copenhagen K, Denmark
Tel.: +45 3319 3200, Fax: +45 3319 3218
E-mail: dt@datatilsynet.dk, Internet: www.datatilsynet.dk

4.5 SURVEY FOR DPA'S ACROSS EUROPE (ESTONIA)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

Estonian Data Protection Inspectorate is familiar with the debate on Big Data. In our opininion Big Data could be defined as collected and processed open datasets, which are defined by quantity, plurality of data formats and data origination and processing speed.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

Yes, some public sector authorities in cooperation with the private sector (e.g. mobile operators) and universities have applied Big Data to their analysis. For example, *Bank of Estonia* (Eesti Pank) and *Statistics Estonia* on turism statistics, *Ministry of the Interior* with municipalities have used Big Data in the development of regional policy. Based on open datasets, private company *Big Data Scoring* provides background information to loan companies.

3. **Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)**

No.

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)**

Inspectorate is not aware of legal cases/judgements by a court, related to Big Data practices in Estonia.

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

Estonian Data Protection Inspectorate consider Open Data as a part of Big Data. General requirements of Open Data processing are described in the Public Information Act, which new draft bill is in the parliament.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

No additional comments.

4.6 SURVEY FOR DPA'S ACROSS EUROPE (FINLAND)

Dear Sir,

In answer to your enquiry below, please be informed of the following:

Office of the Data Protection Ombudsman, Finland (Finnish DPA) is familiar with the debate on Big Data.

Finnish DPA participates the work of the International Working Group on Data Protection in Telecommunications (see www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt). This Working Group has prepared in 2014 a recommendation concerning Big Data (Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics). We have taken part in the preparations of this recommendation and share the views and opinions expressed in it. The Finnish DPA has not issued its own guidelines etc. on the topic so far.

As far as we know, there are no special legal cases/judgments by the Finnish Courts with regard to violations following from Big Data practices. There is no special legal regime for Big Data either.

The Finnish Ministry of Transport and Communications (www.lvm.fi) set in 2014 a working group relating to use of Big Data. This Working Group prepared in 2014 a report which includes a draft national strategy on Big Data and draft measures to

increase the exploitation of large data sets in Finland. The goal of the strategy is the extensive and progressive use of large data sets that will promote economic growth and transparency in society. Should you wish to get further information about this project, please contact the Ministry in question (e-mail: kirjaamo@lvm.fi).

Yours sincerely,
Hanna Lankinen
senior inspector
Office of the Data Protection Ombudsman, Finland

4.7 SURVEY FOR DPA'S ACROSS EUROPE (FRANCE)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

The CNIL is familiar with the debate on Big Data and is actively working on the subject.

In August 2014, a definition of the term 'Big Data' was adopted by the French General Commission on terminology and neology (*Commission générale de terminologie et de néologie*). The official translation of this term in French is '*mégadonnées*' and the definition is 'structured data or not whose very large volume require appropriate analytical tools'. The Gartner definition is also a reference: 'Big Data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making and process automation'. With reference to this definition, three 'Vs' are generally associated with Big Data: volume, variety and velocity. Our Data protection authority (DPA), as other actors, considers that other 'Vs' are also relevant, in particular value and veracity.

Many examples of Big Data operations involve processing of personal data, in various business sectors. The projects have different goals and use different categories of data. But, beyond this diversity of projects and objectives, the notion of 'Big Data' reveals a new approach of the data, appeared with the development of new storage and analytical capacities. And privacy challenges are associated to Big Data because, thanks to sophisticated algorithms, Big Data can ultimately be used to identify profiles, predict the behavior of individuals or groups of individuals and take decision affecting them.

2. Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)

There are various examples of the use of Big Data in France, for instance in the fields of marketing, insurance, credit scoring, antifraud mechanisms, tourism or research. Data controllers can use specific compliance tools *i.e.* simplified standards or single authorizations that allow interconnecting databases (See AU39 fraud detection in insurance sector for a recent example www.cnil.fr/documentation/deliberations/deliberation/delib/318/).

Regarding the law enforcement sector, different data processing operations can be considered as Big Data analysis. For example, opinions of the CNIL on such processing operations are available on our website (www.cnil.fr/nc/linstitution/actualite/article/article/publication-de-lavis-sur-le-projet-de-loi-relatif-au-renseignement/; www.cnil.fr/documentation/deliberations/deliberation/delib/302/).

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

At this stage, there is no report on the use of Big Data drafted by our DPA. However, different presentations were made during conferences on this topic as well as analytical articles (see, for example, the article '*Big Data et protection des données personnelles : quels enjeux ?*', Sophie Vulliet-Tavernier, Revue Statistique et société www.statistique-et-societe.fr). The CNIL also participated in the elaboration of International opinions (Statement of the WP29 on the impact of the development of Big Data on the protection of individuals with regard to the processing of the personal data in the EU; Working paper on Big Data and Privacy of the International Working Group on Data Protection in Telecommunications, Berlin Group).

Besides, in 2011, the CNIL issued a warning against the company *Pages Jaunes* (*deliberation n° 2011-203, September 21, 2011*), for having obtained personal data contained in profiles available on different social media websites, without data subjects' knowing. This online directory proposed a 'webcrawl' function on its website enabling to add information from the accounts of web users to the search results provided by the directory. About 25 million people were concerned and the captured data included the names and first names, pseudonyms, photographs, the names of their school, the names of their employer, their geographical location… In particular, the CNIL considered that the fact that the data were public on the internet did not authorize a third party to massively, repetitively and indiscriminately collect such data without informing the data subjects before posting these information on its website. Consequently, the collection of the personal data was unfair. Moreover, it was difficult for the data subjects to exercise their rights.

Pages Jaunes (Solocal Group) introduced an appeal before the *Conseil d' État* against the warning of the CNIL but the Supreme Court for administrative justice confirmed the analysis of the CNIL (*Conseil d'État, 10ème et 9ème sous-sections réunies, 12/03/2014, 353193*).

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

Please refer to the aforementioned case.

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)

Like the WP29, the CNIL considers that the EU and national legal framework for data protection is applicable to the processing of personal data in Big Data operations, even if the challenges of Big Data might require, in some cases, innovative thinking on how some of the key data protection principles are applied in practice.

Regarding the discussions at the national level to introduce new legislation to regulate Big Data operations, we can mention the works relating to a new law for a 'Digital Republic' and a report published by the French Digital Council.

At present, the French government is preparing a new law for a 'Digital Republic'. An online consultation was launched on the draft bill on September 2015 and the public was invited to suggest amendments to 30 proposed measures, ranging from

net neutrality to open data (until 17 October 2015, www.economie.gouv.fr/projet-loi-numerique). The draft bill proposes in particular an open-data policy for the French state that would make official documents and public-sector research accessible to all online. The bill should be submitted to the parliament at the beginning of 2016.

The French Digital Council (*Conseil national du numérique, CNNum*) is an independent advisory commission. The Council issues independent opinions and recommendations on any question relating to the impact of digital technologies on economy and society. The government can consult the Council on new legislation or draft regulations. The Council's thirty members come from across the digital spectrum, and include researchers and activists.

In its report handed over on 13 June 2014 to Arnaud MONTEBOURG (Minister of Economy, of Productive Recovery and of the Digital) and to Axelle LEMAIRE, (Secretary of State charged of the Digital), the French Digital Council held an expanded approach to the neutrality principle: consecrate Internet neutrality and take in account the digital platforms, that became the new entrance doors of the digital society. The report recommends to establish guidelines on transparency in the way services operate, in particular algorithms. The relevance criteria and governing principles of algorithms should be explained to users as part of a digital literacy effort. The report is available in English on the website of the French Digital Council (www.cnnumerique.fr/wp-content/uploads/2014/06/PlatformNeutrality_VA.pdf).

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

4.8 SURVEY FOR DPA'S ACROSS EUROPE (HUNGARY)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the

practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

The Hungarian National Authority for Data Protection and Freedom of Information accepts the Big Data definition of the International Working Group on Data Protection and Telecommunications. According to the Working Group's Working Paper on Big Data and Privacy: "Big Data is a term which refers to the enormous increase in access to and automated use of information. It refers to the gigantic amounts of digital data controlled by companies, authorities and other large organizations which are subjected to extensive analysis based on the use of algorithms." Big Data is, to a certain extent, used to analyze data in order to identify and predict trends and correlations.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

As far as we know, there are no prominent examples in Hungary for the use of Big Data in law enforcement sector, by the police or intelligence services.

3. **Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)**

The Hungarian National Authority for Data Protection and Freedom of Information has not issued any decision, report or opinion on the use of Big Data so far.

Besides that our Authority participated in the drafting of the working paper on Big Data by the International Working Group on Data Protection and Telecommunications. It is available online on the following address: www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)**

As far as we know there hasn't been any legal cases or judgments by Hungarian court with regard to violation following from Big Data practices so far.

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

In Hungary Act CXII of 2011 on Information Self-Determination and Freedom of Information ("Privacy Act") should be applied to any data protection issues including data protection problems concerning Big Data. Neither the aforementioned act nor other law includes special regulation on Big Data, so the general legal regulation on data protection and privacy should be applied. There aren't any plans or discussion now in the parliament to introduce special legislation for Big Data practices.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

We would like to raise to attention that according to the working paper on Big Data by the International Working Group on Data Protection and Telecommunications the application of Privacy-by-Design principles are crucial for legitimate Big Data practices in most cases. Furthermore a Privacy Impact Assessment could be also recommended and effective before the installation and use of Big Data services in order to avoid future privacy incidents.

Furthermore we would like to point out that in Hungarian business sphere more and more enterprises such as banks, supermarkets, media and telecommunication companies use and take advantage of the possibilities in Big Data. Moreover several international conferences are being organized in Budapest in the topic.

4.9 SURVEY FOR DPA'S ACROSS EUROPE (IRELAND)

Dear Mr. van der Sloot,

I refer to your email of 08/07/2015 requesting our participation in the attached survey and I apologise for the delay in responding to you on the matter.

I regret to advise that this office is not in a position to participate in this survey on this occasion.

Yours Sincerely

Stewart Fennell
Information Officer
Office of the Data Protection Commissioner Canal House Station Road Portarlington Co. Laois

4.10 SURVEY FOR DPA'S ACROSS EUROPE (LATVIA)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government.The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

We do not have a specifically determined definition for Big Data, even though we are familiar with the debate on it.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

No, there aren't.

3. **Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)**

No, we have not.

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)**

We do not have such information.

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

We do not have information on this issue at this point.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

No. But we would like to be informed on the outcome of this survey.

4.11 SURVEY FOR DPA'S ACROSS EUROPE (LITHUANIA)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

The State Data Protection Inspectorate is involved in discussions on Big Data, in so far as regards the performance of supervisory functions.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

In Lithuania there is a Home Affairs Information System, which is a system performing data processing in which on the basis of the joint infrastructure of information technology and telecommunications operates the state and institutional registers and information systems (Criminal Offences register, Police information systems and etc.) managed by the MI and instutions under the MI.

3. **Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)**

Not yet.

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)**

Not yet.

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

Not yet.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

4.12 SURVEY FOR DPA'S ACROSS EUROPE (LUXEMBOURG)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the

practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

Big Data stems from the collection of large structured or unstructured datasets, the possible merger of such datasets as well as the analysis of these data through computer algorithms. It usually refers to datasets which cannot be stored, managed and analysed with average technical means due to their size. Personal data can also be a part of Big Data but Big Data usually extends beyond that, containing aggregated and anonymous data. It allows for the correlation of information which previously could not be linked. From a data protection point of view it can raise many concerns, when it contains personal data, such as the respect of data subjects' rights – for example in the context of data mining – and their ability to exercise control over the personal data or the respect fundamental principles of data protection such as that of data minimization or purpose limitation. Moreover practices such as linking separate databases or computer analytics can turn anonymous data or any kind of non-identifiable information into personal data which would need to be protected under data protection law.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

To our knowledge there are no prominent examples of the use of Big Data in the law enforcement sector or by police or intelligence services in Luxembourg. There are however other actors which deal with Big Data. At a national level, a system of smart metering for electricity and gas has been launched. The project is however still in a testing phase. At the level of the University of Luxembourg, the Luxembourg Centre for Systems Biomedicine uses Big Data in the health sector. The Interdisciplinary Center for Security, Reliability and Trust (SnT) is also involved in Big Data projects. A partnership with Choice Technologies allows the SnT to conduct research into the new analytical methods in the domain of "Big Data". Moreover there are private companies that use Big Data. NeXus for example is, a company "which surfs the wave of Big Data and security by develop-

ing services that fall in the pure concept of "Industry 4.0". "With objects, people and data in constant move, neXus creates a dynamic identity for each end point and keeps track, connects and provides security to the information shared."[200]

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

The CNPD has not issued any decisions, reports or opinions that are directly dealing with Big Data. The Commission has however issued an opinion in a related matter, namely with regard to the problematic raised by smart metering.

In 2013, the CNPD issued an opinion on smart metering (Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif aux modalités du comptage de l'énergie électrique et du gaz naturel, Délibération n° 566/2013 du 13 décembre 2013 (www.cnpd.public.lu/fr/decisions-avis/2013/12/comptage-energie-gaz/566_2013_Deliberation_Ministere-Economie_avis-prj-rgd-comptage-energie-electrique-et-gaz-naturel.pdf). The main argument of the opinion highlights the necessity to clearly define the purposes of the data processing as well as the retention periods of the data related to smart metering.

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

No

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)

There is no legislation directly addressing Big Data. The general data protection legislation applies (Amended Act of 2 August 2002 concerning the protection of individuals with regard to the processing of personal data). To our knowledge there are no plans in Parliament to introduce new legislation to regulate Big Data practices.

6. Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)

4.13 SURVEY FOR DPA'S ACROSS EUROPE (NETHERLANDS)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

Yes, we are familiar with the broad concept of Big Data. Big Data is all about collecting as much information as possible ; storing it in ever larger databases ; combining data that is collected for different purposes ; and applying algorithms to find correlations and unexpected new information.

We refer to the speech of our chairman on Big Data, at URL: https://cbpweb.nl/sites/default/files/atoms/files/2._speech_jko_panel_ii_privacy_with_no_territorial_bounds.pdf

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

Yes, there are examples of the use of Big Data in the Netherlands. There has been a lot of media attention for Big Data use by the Tax administration (scraping websites such as Marktplaats to detect sales, mass collection of data about parking and driving in leased cars, including use of ANPR-data, and profiling people to detect potentially fraudulent tax filings, see for example the interview with the general manager of the IRS, at https://decorrespondent.nl/2720/Baas-Belastingdienst-over-Big-Data-Mijn-missie-is-gedragsverandering/83656320-f6e78aaf). Next to that, there are many pilots currently being conducted by different municipalities to combine different statistical, social care and medical care data, related to a shift in financial responsibility for social care duties. Recently, an interview was given by

high ranking police officers describing the introduction of datamining tools for preventive policing. See URL: www.politieacademie.nl/ kennisenonderzoek/ kennis/mediatheek/pdf/89539.pdf

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

Next to the speech of our chairman, we refer to international opinions and resolutions from The International Working Group on Data Protection and Telecommunications (www.datenschutz-berlin.de/attachments/1052/ WP_Big_Data_final_clean_675.48.12.pdf?1407931243

The Article 29 Working Party (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf) and The resolution from the International Commissioners conference (https:// cbpweb.nl/sites/default/files/atoms/files/resolution_big_data.pdf).

Our key concern is that data protection should be about surprise minimisation, while Big Data entails the risk of surprise maximation. There is a real risk that those who are involved in the development and use of Big Data are ignoring the basic principles of purpose limitation, data minimisation and transparency. And an additional frightening fact is that the statistical information, even if the data used is properly anonymised, can lead to such precise results that it essentially constitutes re-identification.

When Big Data are used to profile people, it has the potential of leading us on to a - predetermined and maybe sometimes dangerous - path. A path that may in the end undermine the values that underpin our democratic societies, by depriving people of their free choice, of their right to personal development and equal treatment.

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

Yes, there has been a court procedure in two instances about access to parking data for the IRS (case number HD 200.139.173/01, URL: http:// uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSHE:2014:2803).

Furthermore, complaints about the use of police data from traffic camera's for the investigation of road vehicle usage in compliance with tax law have led to complaints and court cases. In March 2015, the Court of Appeal in Den Bosch ruled that

the data that is collected with road surveillance camera's of the police, that are installed for safety purposes, may be used by the tax authorities to monitor compliance with the law on road vehicle tax. (The ANPR data case, See: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSHE:2015:1087)

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

The current data protection regime also applies to the use of Big Data, but enforcement of the key values cannot be solely made dependent of the supervisory authority. Our chairman has called for a fierce social dialogue, to make people aware of the risks to our intrinsic values that is posed by Big Data and to think together about how we can effectively address these risks and unwanted consequences.

With regard to the security and intelligence services, a Bill has been consulted publicly and will be introduced to parliament soon to extend powers to allow for mass interception of communications data.

With regard to scientific and academic research, sector specific rules apply. For example the law on higher education and scientific research.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

4.14 SURVEY FOR DPA'S ACROSS EUROPE (NORWAY)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

The Norwegian DPA issued a report on Big Data in 2013. The report was very well received and we have been giving talks on this topics for representatives from all sectors, covering finance, health, law enforcement, marketing, telecom etc. In the report we use the definition of Big Data as it was phrased by the the Article 29 Group:[201]
Big Data is a term that refers to the enormous increase in access to and automated use of information: It refers to the gigantic amounts of digital data controlled by companies, authorities and other large organisations which are subjected to extensive analysis based on the use of algorithms. Big Data may be used to identify general trends and correlations, but it can also be used such that it affects individuals directly.

We use this definition as a basis, but also add what in our opinion is the key aspect of Big Data, namely that it is about the compilation of data from several different sources. In other words, it is not just the volume in itself that is of interest, but the fact that secondary value is derived from the data through reuse and analysis. This aspect of Big Data, and the consequences it has, is in our opinion the most challenging aspect from a privacy perspective.

2. Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)

There are, as far as we know, no usage of Big Data within the law enforcement sector in Norway. In 2014, the intelligence service addressed in a public speech the need to use Big Data techniques in order to combat terrorism more efficiently. However, politicians across all parties reacted very negatively to this request and no formal request to use such techniques has since been launched by the intelligence service.

The companies that are most advanced when it comes to using Big Data may be found within the telecom (eg. Telenor) and media (eg. Schibsted and Cxence) sector. The tax and customs authorities have also initiated projects in which they look at how Big Data can be used to enhance the efficiency of their work.

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

The Norwegian DPA published a report on Big Data in 2013. In 2014 we drafted a working paper on Big Data for the International Working Group on Data Protection in Telecommunications (aka the Berlin Group). Following on from this work we were later responsible for drafting a Resolution on Big Data for the 36th International Conference of Data Protection Authorities and Privacy Commissioners.

Report on Big Data: www.datatilsynet.no/Global/04_planer_rapporter/big-data-engelsk-web.pdf

Working Paper on Big Data and Privacy: www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Resolution on Big Data: http://privacyconference2014.org/media/16602/Resolution-Big-Data.pdf

Our main argument in the report can be summarized as follows:
"Big Data is challenging key privacy principles, in particular the principles of purpose limitation and data minimisation. The protection provided by these privacy principles is more important than ever at a time when an increasing amount of information is collected about us. The principles provide the foundation for safeguards against extensive profiling in an ever increasing array of new contexts. A watering down of key privacy principles, in combination with more extensive use of Big Data, is likely to have adverse consequences for the protection of privacy and other fundamental rights."

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)**

There are no legal cases

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

There are no special regimes for Big Data in Norway or plans to introduce new legislation. We rely on the national "Personal Data Act" which builds on the European Data Protection Directive.

6. Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)

Knowledge and awareness of the privacy challenges associated with Big Data are important among the enterprises that implement the technology. We urge the trade organisations to place these challenges on their agendas, and provide training in how they can be handled, for example through the use of privacy by design. Knowledge of data protection and the privacy challenges associated with the use of Big Data should be part of the curriculum for universities and colleges where data analysis or data science are taught. It is also crucial that supervisory authorities possess the necessary knowledge and awareness of the potential that lies in Big Data. This is important so that they can function as efficient and effective enforcers of the regulations that have been established to protect key societal assets. Research on the social and privacy consequences of Big Data is also of great importance. Big Data is still a relatively new phenomenon. It will be important to research how access to ever- increasing volumes and additional types of data will affect how we make decisions and organise our society in the future.

At the Norwegian DPA we are currently looking into how it affects our privacy when personal data is more and more turning into a valuable commodity in all sectors of the economy. We are writing a report on how Big Data is used within the advertising industry, and how the use of automated, personalised marketing triggers an enourmous appetite for and exchange of personal data.

4.15 SURVEY FOR DPA'S ACROSS EUROPE (SLOVAKIA)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the

practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

We are following the debate, but we have not adopted any definition yet.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

We are not aware of special example of the use of Big Data in Slovakia.

3. **Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)**

No, we have not issued any documents about the use of Big Data yet.

4. **Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)**

We have no knowledge about the case or judgements about the Big Data in our country to this date.

5. **Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)**

We have no special regime for Big Data so far. General data protection law will apply when the personal data will be processed within the Big Data.

We are not planning to issue a new legislation connected with Big Data practices yet.

6. **Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)**

We think that the issue of Big Data is a very challenging topic. Finding the right balance between protection of personal data and the business models based on Big Data will need to be examined and legislated.

As a research topic we would like to suggest examining boundaries between personal and non-personal information. In the Big Data environment you are able to connect non-personal information and based on this information identify the data subject which represents potential risk to rights of the data subjects

4.16 SURVEY FOR DPA'S ACROSS EUROPE (SLOVENIA)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

The Information Commissioner is closely following the debate on Big Data. In terms of definitions of Big Data we believe that established definitions and descriptions (e.g. Wikipedia) adequately describe the issue.

Big Data is a broad term for processing of large amounts of different types of data, including personal data, acquired from multiple sources in various formats. Big Data revolves around predictive analytics – acquiring new knowledge from large data sets which requires new and more powerful processing applications.

Big Data has important information privacy implications. Information on personal data processing may not be known to the individual or poorly described for the individual, personal data may be used for purposes previously unknown to the individual. The individual may be profiled and decisions may be adopted in automated and non-transparent fashion having more or less severe consequences for the individual. Decisions about the individual may be biased, discriminatory and even adopted on grounds of statistics, averages and predictions that could have little or even nothing to do with individual's actual data. Such uses could have severe

consequences for the individual particular when used by law enforcement, but also in other sensitive fields, such as health services and health insurance, social transfers, employment and in particularly situations where processing of sensitive personal data may be involved. The principles of personal data accuracy and personal data being kept up to date may also be under pressure in Big Data processing. Data may be processed by several entities and merged from different sources without proper transparency and legal ground. Processing vast quantities of personal data also brings along higher data security concerns and calls for strict and effective technical and organisational data security measures.

2. Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)

We have thus far not seen prominent examples of the use of Big Data in our country. To our knowledge Big Data applications are particularly of interest in insurance, banking and electronic communications sector, mostly to battle fraud and other illegal practices. Another important field is scientific and statistical research. Law enforcement use is to our knowledge currently at development stages (e.g. in the case of processing Passenger Name Records), whereas information about the use of Big Data at intelligence services is either not available or of confidential nature.

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

So far, given that the use of Big Data in our country has not attained greater acceptance we have not issued particular papers on Big Data at national level. On the other hand we co-operate in international fora of privacy advocates and supervisory authorities, such as Article 29 Working Party[202], International Working Group on Data Protection in Telecommunications[203], European and International Privacy Commissioners conference[204], which have already provided their views on the issues surrounding Big Data in resolutions, working papers and opinions.

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

Not to our knowledge.

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)

There is no special regime for Big Data. If processing of personal data is involved then Personal Data Protection Act applies with its existing provisions. To our knowledge there are no plans to introduce new legislation to regulate Big Data practices. The Information Commissioner has the competence to issue non-binding decisions regarding proposals for new legislation and will and would be able to comment on such proposals.

6. Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)

Big Data brings substantial challenges for personal data protection and these challenges must firstly be well understood and adequately addressed. In our view new concepts and paradigms, such as cloud computing or Big Data should not lower or undermine the current levels of data protection as a fundamental human right. Existing central data protection principles, such lawfulness, fairness, proportionality, rights of the data subjects and finality should not be undermined with the advent of Big Data. The rights of the individuals to informational self – determination should be cornerstone in modern information society, protected by modern data protection framework delivering efficient data protection for the individual while allowing lawful and legitimate interests, often also in the interest of the individual, to be attained.

Further research issues could cover the following topics:

Understanding and managing privacy risks arising from the concept of Big Data.

Adequacy and effectiveness of the notion of consent in the age of Big Data.

Benefits and pitfalls of the notion of "legitimate interests" as legal ground for processing personal data in Big Data environments.

The principle of finality vis a vis exploiting the benefits offered by Big Data.

Privacy by design and privacy enhancing technologies in connection with Big Data.

Accountability and other notions of demonstrative and effective data protection vis a vis Big Data.

Automated decision making and profiling – which privacy safeguards are needed?

4.17 SURVEY FOR DPA'S ACROSS EUROPE (SWEDEN)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data?**

We are familiar with the debate on Big Data but we have not produced any definition of this concept ourselves. As we see it, the concept is used for situations where large amounts of data are gathered in order to be made available for different purposes, not always precisely determined in advance.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services?**

We have not carried out any specific supervision related to the concept Big Data and do not have any statistics or specific information on how this is used.

In our opinion, the law enforcement sector does not use Big Data. Their personal data processing is strictly regulated in terms of collection of data, limited purposes etc.

3. **Have you issued any decisions/reports/opinions on the use of Big Data?**

No

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country?

No

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in Parliament to introduce new legislation to regulate Big Data practices?

Personal data processing in general is regulated in the Personal Data Act, which in principle applies to all sectors of society. However, many public agencies have their own personal data legislation which is specifically adapted to each agency's particular activity and needs. To the extent that public agencies collect large amounts of data, this is therefore usually specifically regulated (e.g. the Tax authority which processes data for taxation purposes but also for population register purposes). Telecom and Internet service providers' collection of data may involve collection of large amounts of data and this is specifically regulated in an act that implements the e-Privacy directive. This personal data processing does not fall under our supervision but instead under supervision of the National Post and Telecom Agency.

It might also be worth noting that further to the aim to strengthen the right to privacy, the Swedish Constitution was amended in 2010 and now explicitly mentions the right to protection against privacy infringements by surveillance or mapping of the individual's personal circumstances without his/her consent. This means that the creation of large databases which contain information that provides a comprehensive image of an individual person, must be specifically permitted in an Act by the Parliament.

We are not aware of any specific plans for Big Data regulation.

6. Are there any final remarks you want to make/suggestions you have for further research?

4.18 SURVEY FOR DPA'S ACROSS EUROPE (UNITED KINGDOM)

The Netherlands Scientific Council for Government Policy (WRR) is an independent advisory body for the Dutch government. The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices, etc. Via this short survey, we hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public.

1. **Are you familiar with the debate on Big Data? If so, how would you define Big Data? (max. 500 words)**

We are familiar with current debates on Big Data and have contributed to them.

We consider that the accepted Gartner definition based on the "three V's" (volume, variety and velocity) provides a useful starting point for defining Big Data. We also consider that other key characteristics of Big Data analytics include: repurposing data; using algorithms to find correlations in datasets rather than constructing traditional queries; and bringing together data from a variety of sources, including structured and unstructured data.

Furthermore, we note that Big Data may involve not only data that has been consciously provided by data subjects, but also personal data that has been observed (eg from Internet of Things devices), derived from other data or inferred through analytics and profiling.

Given the range of features listed here, we think that it is difficult to produce a comprehensive definition of Big Data which fits all use cases. It is better to see Big Data as a phenomenon, rather than a specific technology.

In our discussions with companies about Big Data, they have tended to see the defining characteristics of Big Data as the use of new data sources (eg social media data) and the use of existing data for new purposes, rather than simply the volume of data.

2. **Are there prominent examples of the use of Big Data in your country, especially in the law enforcement sector, by the police or by intelligence services? (max. 500 words)**

We have not carried out a comprehensive market assessment of Big Data but, from our contacts with business and our desk research, our impression is that the take up of Big Data is still at a relatively early stage in the UK. Nevertheless, we know that companies are actively investigating the potential of Big Data, and there are some examples of Big Data in practice, such as the use of telematics in motor insurance, the use of mobile phone location data for market research, and the availability of data from the Twitter 'firehose' for analytics.

We do not have any specific information on the use of Big Data in law enforcement or security. The UK Data Protection Act includes a wide-ranging exemption from the data protection principles where it is required for safeguarding national security.

3. Have you issued any decisions/reports/opinions on the use of Big Data? If so, could you provide us with a reference and your main argument? (max. 500 words)

In July 2014 we published a discussion paper on Big Data and data protection. We invited feedback on this and in April 2015 we published a summary of feedback, together with our response.

In our work we have noted that Big Data poses a number of challenges to data protection, in particular:

It may be difficult to provide meaningful privacy information to data subjects, because of the complexity of the analytics and people's reluctance to read terms and conditions, and because it may not be possible to identify at the outset all the purposes for which the data will be used.

It may be difficult to obtain valid consent, particularly in circumstances where data is being collected through being observed or gathered from connected devices, rather than being consciously provided by data subjects.

Big Data tends to use data for new and unexpected purposes, which may conflict with the purpose limitation principle.

Big Data tends to use "all the data", which may conflict with the data minimization principle.

Nevertheless, we have stressed that the data protection principles still apply in the world of Big Data; it is not a game that is played by different rules. We have said that organisations need to carry out a realistic assessment of what they are trying

to achieve, and balance the benefits of the analytics to the organisation, to the individual and to society against the impact on data privacy. They also need to be innovative in seeking new ways to provide privacy notices.

We think that privacy impact assessments (PIAs) have an important role to play in helping to ensure that Big Data analytics meets data protection requirements. We are currently doing further work with organisations to explore how PIAs can be used in the context of Big Data, as part of privacy by design approach.

We also advocate that, wherever possible and appropriate, the data used for the analytics should be anonymised, so that it can no longer be considered to be personal data.

We are planning to publish a new version of our Big Data paper later this year.

4. Are there any legal cases/judgements by a court with regard to (privacy/data protection) violations following from Big Data practices in your country? If so, could you provide us with a reference and the main consideration of the court? (max. 500 words)

We are not aware of any cases specifically to do with Big Data. This may be due to the fact that Big Data analytics can be opaque to the data subject, and so people do not necessarily realise how their data is being used.

5. Which legal regimes are applied to Big Data/ is there a special regime for Big Data in your country? Are there any discussions/plans in parliament to introduce new legislation to regulate Big Data practices? (max. 500 words)

There is no specific legal regime for Big Data, other than the Data Protection Act.

It is notable however that there is some evidence of a move towards self-regulation, in the sense that some companies are developing what can be described as an 'ethical' approach to Big Data, based on understanding the customer's perspective, being transparent about the processing and building trust.

6. Are there any final remarks you want to make/suggestions you have for further research? (max. 500 words)

We note that the proposals for the new EU General Data Protection regulation incorporate some of the measures we have identified as being important in ensuring compliance in Big Data eg clearer privacy notices, privacy impact assessments

and privacy by design. We welcome the fact that these measures are being foregrounded, although we are concerned that that they should not be seen as simply a bureaucratic exercise.

4.19 INVITATION MAIL AND LIST OF ADDRESSES

4.19.1 INVITATION MAIL

Dear sir/madam,

I am writing to you on behalf of the Netherlands Scientific Council for Government Policy (WRR). The WRR is an independent advisory body for the Dutch government. The task of the WRR is to advise the government on issues that are of great importance for society in the intermediate and longer term. The reports of the WRR are not tied to one policy sector but rather touch on various terrains and policy sectors; they are concerned with the direction of government policy for the longer term. The members of the WRR are established university professors who have often worked on policy related subjects and/or have made tracks in public administration themselves.

The Dutch government has requested the WRR to advise on the regulation of Big Data, taking into account how privacy and security should be assessed in the deployment of Big Data analytics in security related policies. Questions that should be addressed include whether a distinction needs to be made between access to and use of data, how transparency and individual rights can be guaranteed in Big Data practices and what the likely impact of the emergence of quantum computing will be. In addition to the policy advice, published in the form of a report for the Dutch government, we are planning to publish a short survey, sent to European Data Protection Authorities. We hope to get input from all DPAs across Europe on the practice and regulation of Big Data in their country. This helps us to signal potential problems, and distill Best Practices from the different approaches offered. The survey will be published on the internet and will be open to the public. Please find the survey attached.

We whole-heartedly hope you agree to contribute to this project. If you have any questions, please do not hesitate to contact me via email or phone on the number mentioned in my signature. If you decide to participate in this survey, we hope you would have time to send us your answers within 6 weeks.

Thanks in advance,

Yours sincerely,

Bart van der Sloot, Research Fellow WRR

www.wrr.nl/en/home/
e-mail: sloot@wrr.nl
Tel.: +31 (0)70-3564612
Website: www.wrr.nl/bureau/staf/article/bart-van-der-sloot/

4.19.2 LIST OF ADDRESSES

- **Austria: Österreichische Datenschutzbehörde**
  - E-mail: dsb@dsb.gv.at
  - Website: www.dsb.gv.at/site/7749/default.aspx

- **Belgium: Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)**
  - E-mail: commission@privacycommission.be
  - Website: www.privacycommission.be/

- **Bulgaria: Commission for Personal Data Protection**
  - E-mail: kzld@cpdp.bg
  - Website: www.cpdp.bg/en/index.php?p=home&aid=0

- **Croatia: Croatian Personal Data Protection Agency**
  - E-mail: azop@azop.hr
  - Website: www.azop.hr/cpage.aspx?page=default.aspx&PageID=47

- **Cyprus: Commissioner for Personal Data Protection**
  - E-mail: commissioner@dataprotection.gov.cy
  - Website: www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument

- **Czech Republic: The Office for Personal Data Protection (Urad pro ochranu osobnich udaju)**
  - E-mail: posta@uoou.cz
  - Website: www.uoou.cz/en/

- **Denmark: Datatilsynet**
  - E-mail: dt@datatilsynet.dk
  - Website: www.datatilsynet.dk/english/

- **Estonia: Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)**
  - E-mail: viljar.peep@aki.ee
  - Website: www.aki.ee/en

- **Finland: Office of the Data Protection Ombudsman**
  - E-mail: tietosuoja@om.fi
  - Website: www.tietosuoja.fi/en/index.html

- **France: Commission Nationale de l'Informatique et des Libertés (CNIL)**
  - Geen email.
  - Website: www.cnil.fr/english/

- **Germany: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**
  - E-mail: poststelle@bfdi.bund.de
  - Website: www.bfdi.bund.de/DE/Home/home_node.html

- **Greece: Hellenic Data Protection Authority**
  - E-mail: contact@dpa.gr
  - Website: www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL

- **Hungary: Data Protection Commissioner of Hungary**
  - E-mail: peterfalvi.attila@naih.hu
  - Website: www.naih.hu/general-information.html

- **Ireland: Data Protection Commissioner**
  - E-mail: info@dataprotection.ie
  - Website: www.dataprotection.ie/viewdoc.asp?DocID=4

- **Italy: Garante per la protezione dei dati personali**
  - E-mail: garante@gpdp.it
  - Website: www.garanteprivacy.it/web/guest/home_en

- **Latvia: Data State Inspectorate**
  - E-mail: info@dvi.gov.lv
  - Website: www.dvi.gov.lv/en/

- **Lithuania: State Data Protection Inspectorate**
  - E-mail: ada@ada.lt
  - Website: www.ada.lt/go.php/lit/English

- **Luxembourg: Commission nationale pour la protection des données**
  - E-mail: info@cnpd.lu
  - Website: www.cnpd.public.lu/fr/index.html

- **Malta: Office of the Data Protection Commissioner**
  - E-mail: commissioner.dataprotection@gov.mt; idpc.info@gov.mt
  - Website: http://idpc.gov.mt/

- **Nederland: College bescherming persoonsgegevens**
  - E-mail: info@cbpweb.nl
  - Website: https://cbpweb.nl/nl

- **Poland: The Bureau of the Inspector General for the Protection of Personal Data**
  - E-mail: sekretariat@giodo.gov.pl
  - Website: www.giodo.gov.pl/168/j/en/

- **Portugal: Comissão Nacional de Protecção de Dados**
  - E-mail: geral@cnpd.pt
  - Website: www.cnpd.pt/english/index_en.htm

- **Romania: The National Supervisory Authority for Personal Data Processing**
  - E-mail: anspdcp@dataprotection.ro
  - Website: www.dataprotection.ro/index.jsp?page=home&lang=en

- **Slovakia: Office for Personal Data Protection of the Slovak Republic**
  - E-mail: statny.dozor@pdp.gov.sk
  - Website: http://dataprotection.gov.sk/uoou/en

- **Slovenia: Information Commissioner**
  - E-mail: gp.ip@ip-rs.si
  - Website: www.ip-rs.si/?id=195

- **Spain: Agencia de Protección de Datos**
  - prensa@agpd.es
  - E-mail: internacional@agpd.es
  - Website: www.agpd.es/portalwebAGPD/LaAgencia/index-iden-idphp.php

- **Sweden: Datainspektionen**
  - E-mail: datainspektionen@datainspektionen.se
  - Website: www.datainspektionen.se/in-english/

- **United Kingdom: The Information Commissioner's Office**
  - E-mail: International.Team@ico.org.uk
  - Website: https://ico.org.uk/

Non-EU countries

- **Switzerland**: Federal Data Protection and Information Commissioner (FDPIC)
  - Email: webmaster@edoeb.admin.ch.
  - Website: www.edoeb.admin.ch/?lang=en

- **Norway: The Norwegian Data Protection Authority**
  - Email: postkasse@datatilsynet.no
  - Website: www.datatilsynet.no/English/

- **Serbia: Commissioner for Information of Public Importance and Personal Data Protection**
  - E-mail: office@poverenik.rs
  - Website: www.poverenik.rs/en.html

NOTES

1 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

2 www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf.

3 https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/big_data See also: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf.

4 http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

5 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.Directive 2013/37/EU of the European Parliament and the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

6 www.gartner.com/technology/research/methodologies/hype-cycle.jsp.

7 www.whitehouse.gov/blog/2012/03/29/big-data-big-deal

8 www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release.pdf.

9 www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help.

10 www.parliament.uk/written-questions-answers-statements/written-question/commons/2014-11-17/214448.

11 http://researchbriefings.files.parliament.uk/documents/POST-PN-468/POST-PN-468.pdf.

12 www.parliament.uk/written-questions-answers-statements/written-question/commons/2014-11-17/214448.

13 www.parliament.uk/written-questions-answers-statements/written-question/commons/2014-11-17/214448.

14 www.gov.uk/government/news/73-million-to-improve-access-to-data-and-drive-innovation.

15 www.gov.za/about-government/government-programmes/square-kilometre-array-ska.

16 www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/2013-11-09-Bigdata-NA008.pdf, see p. 10.

17 www.bmbf.de/press/3580.php.

18 www.bmbf.de/press/3787.php?hilite=big+data.

19 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf.

20 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) /* COM/2012/011 final - 2012/0011 (COD) */.

21 www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf.

22 www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf.

23 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

24 Court of Justice, Maximillian Schrems v. Data Protection Commissioner, C-362/14.

25 Rechtbank 's-Gravenhage 23 juli 2014 Zaaknummer: C/09/455237 / HA ZA 13-1325.

26 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013.

27 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 6.

28 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 19.

29 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 21 -25.

30 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 5.

31 Australian Government, 'Australian Public Service Better Practice Guide for Big Data', 2015, p. 1.

32 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 14.

33 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 15.

34 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 13.

35 CISRO, 'Vizie: Connecting with customers through social media': www.csiro.au/en/Research/DPF/Areas/The-digital-economy/Digital-service-delivery/Vizie.

36 Department of Finance and Deregulation, Australian Government Information Management Office, 'The Australian Public Service Big Data Strategy', 2013, p. 10.

37 Australian Government, ComLaw, Guidelines for the Conduct of the Data-Matching Program, 1994: www.comlaw.gov.au/Details/F2009B00268.

38 Australian Government, Office of the Australian Information Commissioner, Guidelines on Data Matching in Australian Government Administration, June 2014: www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/data-matching-guidelines-2014.

39 Privacy Act 1988.

40 Australian Government, Office of the Australian Information Commissioner, 'Privacy Law': www.oaic.gov.au/privacy-law/.

41 Australian Government, Office of the Australian Information Commissioner, 'Privacy fact sheet 17: Australian Privacy Principles', January 2014: www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.

42 Australian Government, Office of the Australian Information Commissioner, 'Privacy Law': www.oaic.gov.au/privacy-law/.

43 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, p. 15.

44 Ministry of Labor and Employment, 'RAIS': http://en.dataviva.info/about/data/rais/.

45 DataViva: http://en.dataviva.info/about/contact/.

46 DataViva, 'About the Visualizations': http://en.dataviva.info/about/apps/about/.

47 Microsoft, 'Microsoft and São Paulo government partner to release crime monitoring system', 16 April 2014: http://blogs.microsoft.com/blog/2014/04/16/microsoft-and-so-paulo-government-partner-to-release-crime-monitoring-system/; Secretaria de Segurança Pública do Estado de São Paulo, 'SP ganha nova etapa do Detecta, sistema de monitoramento criminal', 16 April 2014: www.ssp.sp.gov.br/noticia/lenoticia.aspx?id=33930.

48 Pensando o Direito, 'Debate, Proteção de Dados Pessoais': https://participacao.mj.gov.br/dadospessoais/english-information/.

49 Draft law, 'On the processing of personal data to protect the personality and dignity of natural persons'.

50 Pensando o Direito, 'Proteção de Dados Pessoais': https://participacao.mj.gov.br//dado-spessoais/.

51 Li Keqiang Premier of the State Council, 'Report on the work of the government, Delivered at the Second Session of the Twelfth National Peoples Congress on March 5, 2014', p. 24.

52 The National People's Congress of the People's Republic of China, 'Xinhua Insight: China considers boosting credit system', 8 March 2014: www.npc.gov.cn/englishnpc/Special_12_2/2014-03/08/content_1843931.htm.

53 The National People's Congress of the People's Republic of China, 'Xinhua Insight: China considers boosting credit system', 8 March 2014: www.npc.gov.cn/englishnpc/Special_12_2/2014-03/08/content_1843931.htm.

54 The State Council of the People's Republic of China, 'Vice-premier stresses importance of Big Data development', 27 May 2015: http://english.gov.cn/state_council/vice_premiers/2015/05/27/content_281475115610715.htm.

55 The State Council of the People's Republic of China, 'New social credit code system to increase administrative efficiency', 17 June 2015: http://english.gov.cn/policies/latest_releases/2015/06/17/content_281475129090642.htm.

56 The State Council of the People's Republic of China, 'Premier promotes Big Data', 18 June 2015: http://english.gov.cn/premier/news/2015/06/18/content_281475129712178.htm.

57 The State Council of the People's Republic of China, 'Premier promotes Big Data', 18 June 2015: http://english.gov.cn/premier/news/2015/06/18/content_281475129712178.htm.

58 The State Council of the People's Republic of China, 'Opinion released on use of Big Data', 1 July 2015: http://english.gov.cn/policies/latest_releases/2015/07/01/content_281475138273106.htm.

59 The State Council of the People's Republic of China, 'China unveils 'Internet Plus' action plan to fuel growth', 4 July 2015: http://english.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm.

60 The State Council of the People's Republic of China, 'Big Data plays bigger role in China's administration management', 5 July 2015: http://english.gov.cn/news/top_news/2015/07/05/content_281475140856686.htm.

61 The State Council of the People's Republic of China, 'China to develop modern circulation, Big Data industries', 19 August 2015: http://english.gov.cn/premier/news/2015/08/19/content_281475171439937.htm.

62 The State Council of the People's Republic of China, 'Premier asks govt departments to implement Big Data plan', 20 August 2015: http://english.gov.cn/premier/news/2015/08/20/content_281475171811356.htm.

63 The National People's Congress of the People's Republic of China, 'China's legislature adopts online info rules to protect privacy', 5 January 2013: www.npc.gov.cn/englishnpc/news/Legislation/2013-01/05/content_1750014.htm.

64 The National People's Congress of the People's Republic of China, 'China's legislature adopts online info rules to protect privacy', 5 January 2013: www.npc.gov.cn/englishnpc/news/Legislation/2013-01/05/content_1750014.htm.

65 Commisariat général à la stratégie et à la prospective, 'La Note d'Analyse', no. 8, November 2013, p. 10 & 11.

66 Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data : la feuille de route entre en action', 19 December 2014: www.economie.gouv.fr/big-data-feuille-route-en-action.

67 Le Comité de Pilotage de la Nouvelle France Industrielle, 'La Nouvelle France Industrielle, phase 2': www.economie.gouv.fr/nouvelle-france-industrielle ; Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data : la feuille de route entre en action', 19 December 2014: www.economie.gouv.fr/big-data-feuille-route-en-action.

68 Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data Feuille de route', 2 July 2014, p. 3.

69 Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data Feuille de route', 2 July 2014, p. 3.

70 Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data Feuille de route', 2 July 2014, p. 4.

71 Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data Feuille de route', 2 July 2014, p. 4.

72 Le Comité de Pilotage de la Nouvelle France Industrielle, 'Big Data Feuille de route', 2 July 2014, p. 5.

73 Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

74 Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

75 Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

76 Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

77 Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

78 Secrétariat Géneral pour la Modernisation de l'Action Publique, 'Vitam : vers un socle d'archivage électronique commun à toute l'administration', 18 March 2015: www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/vitam-vers-un-socle-d-archivage-electronique-commun-toute-l-administration.

79 Direction Générale des Enterprises, 'Etude prospective sur les mutations des services postaux': www.entreprises.gouv.fr/services/etude-prospective-sur-mutations-des-services-postaux#_ftnref3; Direction Générale des Enterprises, 'Évolutions technologiques, mutations des services postaux et développement de services du futur', 1 July 2013: www.entreprises.gouv.fr/etudes-et-statistiques/evolutions-technologiques-mutations-des-services-postaux-et-developpement-ser.

80 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

81 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

82 Conseil Constitutionnel 23 July 2015, Décision n° 2015-713 DC, Communiqué de presse.

83 Conseil Constitutionnel 23 July 2015, Décision n° 2015-713 DC.

84 Bundesministerium für Bildung und Forschung, 'Big Data': www.softwaresysteme.pt-dlr.de/de/big-data.php.

85 Bundesministerium für Bildung und Forschung, 'Bekanntmachung', 20 February 2013: www.bmbf.de/foerderungen/bekanntmachung.php?B=824.

86 Bundesministerium für Bildung und Forschung, 'Forschung zu Big Data und IT-Sicherheit neu aufgestellt', 10 March 2014: www.bmbf.de/de/forschung-zu-big-data-und-it-sicherheit-neu-aufgestellt-463.html.

87 Bundesministerium für Bildung und Forschung, 'Big Data - Management und Analyse großer Datenmengen': www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html.

88 Bundesministerium für Bildung und Forschung, 'Big Data - Management und Analyse großer Datenmengen': www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html.

89 Bundesministerium für Bildung und Forschung, 'Big Data - Management und Analyse großer Datenmengen': www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html.

90 PRNewswire, 'German Government Announces "Production Intelligence": Funding for Jedox's Big Data Project', 13 April 2015: www.prnewswire.com/news-releases/german-government-announces-production-intelligence-funding-for-jedoxs-big-data-project-499530121.html.

91 Bundesministerium für Bildung und Forschung, 'Die Macht von Big Data entschlüsseln und steuern', 6 May 2015: www.bmbf.de/de/die-macht-von-big-data-entschluesseln-und-steuern-1033.html?hilite=big+data.

92 Bundesministerium für Bildung und Forschung, 'Die Macht von Big Data entschlüsseln und steuern', 6 May 2015: www.bmbf.de/de/die-macht-von-big-data-entschluesseln-und-steuern-1033.html?hilite=big+data.

93 Bundesdatenschutzgesetz 2009.

94 Grundgesetz für die Bundesrepublik Deutschland.

95 Bundesministerium des Innern, 'Expert group on Big Data as a challenge for data protection', 21 August 2014: www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/09/expert-group-on-big-data-as-a-challenge-for-data-protection.html.

96 Bundesministerium des Innern, 'Expert group on Big Data as a challenge for data protection', 21 August 2014: www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/09/expert-group-on-big-data-as-a-challenge-for-data-protection.html.

97 Bundesministerium des Innern, 'Expert group on Big Data as a challenge for data protection', 21 August 2014: www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/09/expert-group-on-big-data-as-a-challenge-for-data-protection.html.

98 Department of Science & Technology, 'Big Data Initiative': www.dst.gov.in/big-data-initiative-1.

99 Department of Science & Technology, 'Big Data Initiative': www.dst.gov.in/big-data-initiative-1.

100 Unique Identification Authority of India, 'Aapka Aadhaar': https://uidai.gov.in/aapka-aadhaar.html.

101 Unique Identification Authority of India, 'Aapka Aadhaar': https://uidai.gov.in/aapka-aadhaar.html.

102 Unique Identification Authority of India, Planning Commission, Government of India, 'Advancing Development Agenda with Aadhaar'.

103 Unique Identification Authority of India, Planning Commission, Government of India, 'Advancing Development Agenda with Aadhaar'.

104 Ministry of Communications and Information Technology, *THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i)*, 11 April 2011.

105 The Centre for Internet & Society, 'Leaked Privacy Bill: 2014 vs. 2011', 31 March 2014: http://cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011.

106 Press Information Bureau, Government of India, 'Right to Privacy Bill', 13 August 2015: http://pibmumbai.gov.in/scripts/detail.asp?releaseId=E2015PR2086.

107 Ministry of Science & Technology, 'National Data Sharing and Accessibility Policy (NDSAP)', 2012.

108 Ministry of Health, 'Israel's Ministry of Health Big Data Opportunity: Vendor Highlights', Tender 10/2015, August 2015: www.health.gov.il/services/tenders/doclib/com10_2015_19082015.pdf.

109 Ministry of Health, 'Israel's Ministry of Health Big Data Opportunity: Vendor Highlights', Tender 10/2015, August 2015: www.health.gov.il/services/tenders/doclib/com10_2015_19082015.pdf.

110 F. Shoihet, 'IDF continues to implement digital communication', *Israel Defense Forces*, 14 October 2012: www.idf.il/1283-17301-en/Dover.aspx.

111 *Israel Defense Forces*, 'Hackers Beware: The IDF's Digital Battleground', 9 October 2013: www.idfblog.com/blog/2013/10/09/hackers-beware-idfs-digital-battleground/.

112 A. Rapaport, 'C4I is Shaping the Operational Reality', *Israel Defense*, 2 February 2015: www.israeldefense.co.il/en/content/c4i-shaping-operational-reality.

113 D. Shamah, 'IDF winning the war with Big Data', *The Times of Israel*, 24 February 2015: www.timesofisrael.com/winning-the-war-with-big-data/.

114 D. Shamah, 'IDF winning the war with Big Data', *The Times of Israel*, 24 February 2015: www.timesofisrael.com/winning-the-war-with-big-data/.

115 D. Shamah, 'IDF winning the war with Big Data', *The Times of Israel*, 24 February 2015: www.timesofisrael.com/winning-the-war-with-big-data/.

116 D. Shamah, 'IDF winning the war with Big Data', *The Times of Israel*, 24 February 2015: www.timesofisrael.com/winning-the-war-with-big-data/.

117 Y. Lappin, 'IDF setting up an operational Internet', *The Jerusalem Post*, 30 March 2015: http://new.jpost.com/landedpages/printarticle.aspx?id=395600.

118 Basic Law: Human Dignity and Liberty 1992.

119 Protection of Privacy Law, 5741 – 1981.

120 Protection of Privacy Law, 5741 – 1981.

121 Protection of Privacy (Transfer of Data Abroad) Regulations.

122 Draft for the Protection of Privacy Regulations (Information Security in Databases), 5770-2010.

123 Prime Minister of Japan and His Cabinet, 'New Economy Summit 2014', 9 April 2014: http://japan.kantei.go.jp/96_abe/actions/201404/09nes.html.

124 IT Strategic Headquarters website: http://japan.kantei.go.jp/policy/it/index_e.html.

125 IT Strategic Headquarters, 'Open Government Data Strategy', 4 July 2012.

126 CREST, 'Advanced Application Technologies to Boost Big Data Utilization for Multiple-Field Scientific Discovery and Social Problem Solving': www.jst.go.jp/kisoken/crest/en/research_area/ongoing/areah25-5.html; CREST, 'Advanced Core Technologies for Big Data Integration': www.jst.go.jp/kisoken/crest/en/research_area/ongoing/areah25-6.html.

127 Act on the Protection of Personal Information, Act No. 57 of May 30, 2003.

128 IT Strategic Headquarters, 'Policy Outline of the Institutional Revision for Utilization of Personal Data', 24 June 2014.

129 IT Strategic Headquarters, 'Policy Outline of the Institutional Revision for Utilization of Personal Data', 24 June 2014, p. 6.

130 IT Strategic Headquarters, 'Policy Outline of the Institutional Revision for Utilization of Personal Data', 24 June 2014, p. 6 & 7.

131 IT Strategic Headquarters, 'Policy Outline of the Institutional Revision for Utilization of Personal Data', 24 June 2014, p. 7 -9.

132 IT Strategic Headquarters, 'Policy Outline of the Institutional Revision for Utilization of Personal Data', 24 June 2014, p. 9 – 12.

133 Naledi Pandor, 'speech 2nd Ministerial Meeting of the Square Kilometre Array (SKA) African Partner Countries', Pretoria, 25 March 2015: www.ska.ac.za/releases/20150409speech.php.

134 SKA, 'Everything you wanted to know about the SKA': www.ska.ac.za/qa/.

135 'SKA a game changer for African tech', *Business Tech*, 21 September 2013: http://businesstech.co.za/news/columns/45930/ska-a-game-changer-for-african-tech/.

136 SKA, 'The SKA project': www.ska.ac.za/about/project.php.

137 *University of Cape Town*, 'Big Data institute will boost SKA', 3 September 2015: www.uct.ac.za/dailynews/?id=9342.

138 Constitution of the Republic of South Africa, 1996.

139 Protection of Personal Information Act 2013.

140 Protection of Personal Information Act 2013.

141 Department for Business, Innovation & Skills, 'Eight great technologies: infographics', 9 October 2013: www.gov.uk/government/publications/eight-great-technologies-infographics.

142 Department for Business, Innovation & Skills, 'Eight great technologies: infographics', 9 October 2013: www.gov.uk/government/publications/eight-great-technologies-infographics.

143 HM Government, 'Seizing the data opportunity. A strategy for UK data capability', October 2013.

144 HM Government, 'Seizing the data opportunity. A strategy for UK data capability', October 2013, p. 3.

145 HM Government, 'Seizing the data opportunity. A strategy for UK data capability', October 2013, p. 3.

146 Department for Business, Innovation & Skills, The Rt Hon David Willetts Arts and Humanities Research Council, Economic and Social Research Council, Medical Research Council, Natural Environment Research Council, '£73 million to improve access to data and drive innovation', 6 February 2014: www.gov.uk/government/news/73-million-to-improve-access-to-data-and-drive-innovation.

147 Department for Business, Innovation & Skills, The Rt Hon David Willetts Arts and Humanities Research Council, Economic and Social Research Council, Medical Research Council, Natural Environment Research Council, '£73 million to improve access to data and drive innovation', 6 February 2014: www.gov.uk/government/news/73-million-to-improve-access-to-data-and-drive-innovation.

148 Department for Business, Innovation and Skills, E. Vaizet, 'ICT:Written question – 214448', 17 November 2014: www.parliament.uk/written-questions-answers-statements/written-question/commons/2014-11-17/214448.

149 The National Archives, 'Big Data for Law': www.legislation.gov.uk/projects/big-data-for-law.

150 Information Commissioner's Office, 'Big Data': https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/.

151 Information Commissioner's Office, 'Big Data and data protection', 28 July 2014, p. 2.

152 Parliamentary Office of Science & Technology, 'Big Data': www.parliament.uk/mps-lords-and-offices/offices/bicameral/post/work-programme/big-data/.

153 Parliamentary Office of Science & Technology, POSTnote, 'Big Data, Crime and Security', July 2014, p. 2.

154 Parliamentary Office of Science & Technology, POSTnote, 'Big Data, Crime and Security', July 2014, p. 3.

155 Parliamentary Office of Science & Technology, POSTnote, 'Big and Open Data in Transport', July 2014, p. 3.

156 Biobank, 'About UK Biobank': www.ukbiobank.ac.uk/about-biobank-uk/.

157 Parliamentary Office of Science & Technology, POSTnote, 'Biobanks', July 2014, p. 2.

158 Parliamentary Office of Science & Technology, POSTnote, 'Big Data, Crime and Security', July 2014, p. 4.

159 Parliamentary Office of Science & Technology, POSTnote, 'Big Data, Crime and Security', July 2014, p. 4.

160 Intellectual Property Office and Viscount Younger of Leckie, 'New exceptions to copyright reflect digital age', 1 June 2014: www.gov.uk/government/news/new-exceptions-to-copyright-reflect-digital-age.

161 The Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations 2014.

162 Intellectual Property Office and Viscount Younger of Leckie, 'New exceptions to copyright reflect digital age', 1 June 2014: www.gov.uk/government/news/new-exceptions-to-copyright-reflect-digital-age.

163 Law Commission 'Data Sharing between Public Bodies': www.lawcom.gov.uk/project/data-sharing-between-public-bodies/.

164 England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening).

165 England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening).

166 England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening), *The Incorporated Council of Law Reporting for England & Wales*.

167 England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening), *The Incorporated Council of Law Reporting for England & Wales*; England and Wales Court of Appeal (Civil Division) 27 March 2015, Google Inc v Vidal-Hall & Ors (Information Commissioner intervening).

168 High Court of Justice Queen's Bench Division Divisional Court 17 July 2015, Davis & Ors v SSHD.

169 *Whitehouse blog*, 'Big Data is a Big Deal', 29 March 2012.

170 *Executive Office of the President*, 'Big Data Across the Federal Government', 29 March 2012: www.whitehouse.gov/blog/2012/03/29/big-data-big-deal.

171 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014.

172 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014, p. 61 – 63.

173 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014, p. 63 & 64.

174 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014, p. 64 & 65.

175 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014, p. 66 & 67.

176 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014, p. 67 & 68.

177 Executive Office of the President & President's Council of Advisors on Science and Technology, 'Report to the President Big Data and Privacy: a Technological Perspective', May 2014, p. xiii & xiv.

178 *Whitehouse blog*, 'Big Data is a Big Deal', 29 March 2012: www.whitehouse.gov/blog/2012/03/29/big-data-big-deal.

179 J. Podesta, *Whitehouse blog*, 'Findings of the Big Data and Privacy Working Group Review', 1 May 2014: www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

180 J. Podesta, *Whitehouse blog*, 'Findings of the Big Data and Privacy Working Group Review', 1 May 2014: www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

181 J. Podesta, *Whitehouse blog*, 'Findings of the Big Data and Privacy Working Group Review', 1 May 2014: www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

182 J. Podesta, *Whitehouse blog*, 'Findings of the Big Data and Privacy Working Group Review', 1 May 2014: www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

183 The President, *Whitehouse*, 'Remarks by the President on Review of Signals Intelligence', 17 January 2014: www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

184 The President, *Whitehouse*, 'Remarks by the President on Review of Signals Intelligence', 17 January 2014: www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

185 Parliamentary Office of Science & Technology, POSTnote, 'Big Data, Crime and Security', July 2014.

186 National Insitute of Justice, 'Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise', *NIJ Journal*, *271*, February 2013: www.ncjrs.gov/pdffiles1/nij/240696.pdf; Geoffrey C. Barnes, Jordan M. Hyatt, 'Classifying Adult Probationers by Forecasting Future Offending. Final Technical Report', March 2012: www.ncjrs.gov/pdffiles1/nij/grants/238082.pdf.

187 Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values', May 2014, p. 17 & 18.

188 Privacy Act 1974 (2015 edition).

189 Consumer Privacy Bill of Rights Act of 2015 (draft).

190 Supreme court 8 November 2011, United States vs Jones.

191 Supreme court 23 June 2011, Sorrell v IMS Health inc.

192 Supreme court 23 June 2011, Sorrell v IMS Health inc.

193 United States Court of Appeals for the Second Circuit 7 May 2015, ACLU v. Clapper.

194 Patriot Sunset Extension Act of 2011.

195 U.S.A. Freedom Act 2015.

196 Foreign Intelligence Surveillance Court 2 juni 2015, Memorandum of Law, nr. 15 -75.

197 Edith Ramirez , 'Protecting Privacy in the Era of Big Data', *International Conference on Big Data from a Privacy Perspective, Hong Kong,* 10 June 2015, p. 9.

198 Edith Ramirez , 'Protecting Privacy in the Era of Big Data', *International Conference on Big Data from a Privacy Perspective, Hong Kong,* 10 June 2015, p. 10.

199 Edith Ramirez , 'Protecting Privacy in the Era of Big Data', *International Conference on Big Data from a Privacy Perspective, Hong Kong,* 10 June 2015, p. 10.

200 See *The dynamic identity of neXus*, February 2015, available at www.pwcaccelerator.com/pwcsaccelerator/media-press-article-dynamic-identity-nexus.html.

201 Opinion 03/2013 on purpose limitation.

202 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.

203 www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf.

204 www.privacyconference2014.org/media/16427/Resolution-Big-Data.pdf.