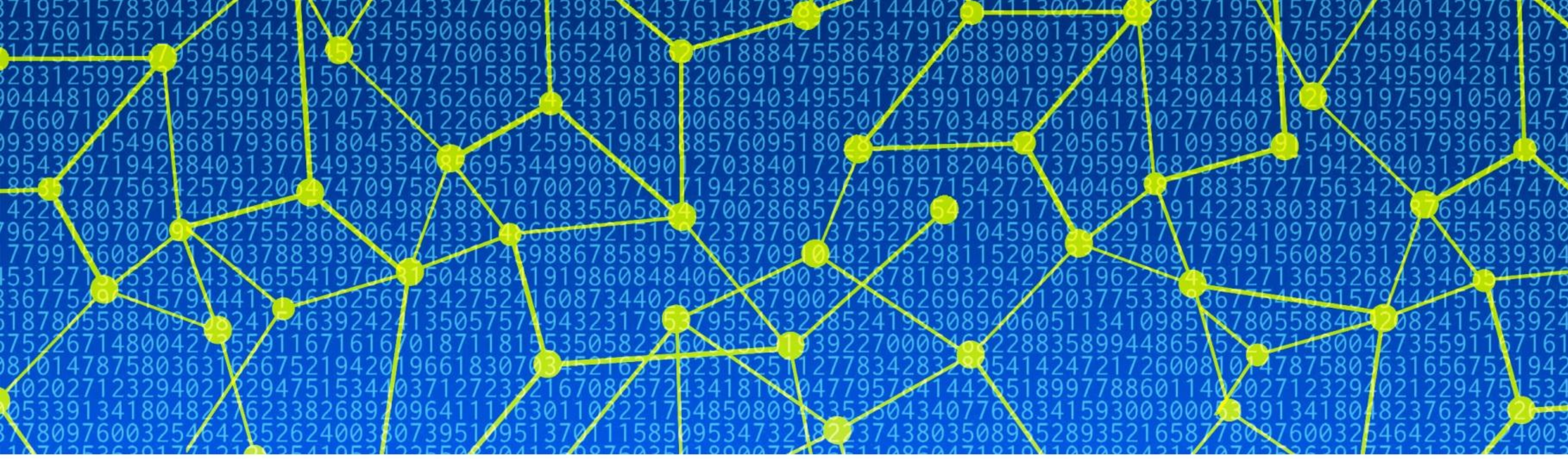


EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2015

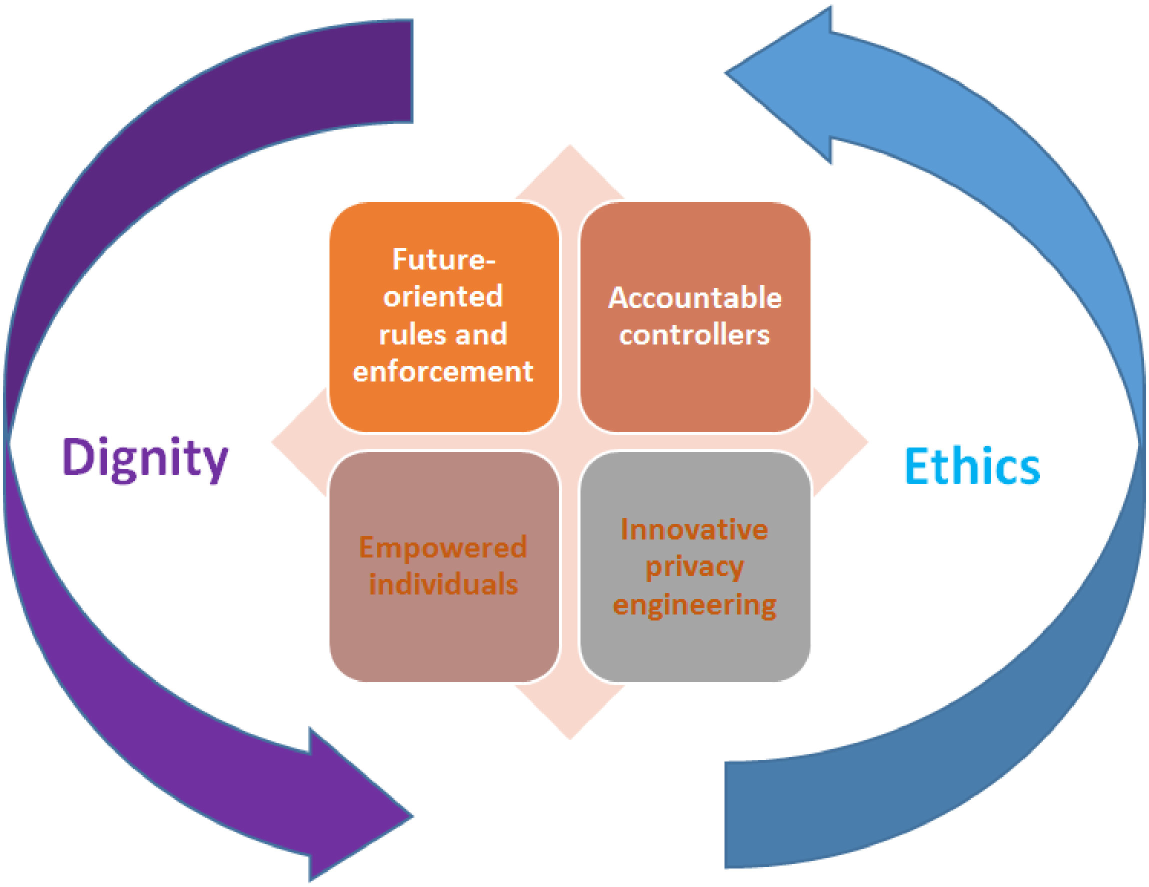
Towards a new digital ethics

Data, dignity and technology

11 September 2015

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41.2 of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. He was appointed in December 2014 together with Assistant Supervisor with the specific remit of being more constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion follows on from the EDPS's previous Opinion on the General Data Protection Regulation which aimed to assist the main institutions of the EU in reaching the right consensus on workable, future-oriented set of rules which bolsters the rights and freedoms of the individual. Like the Opinion on Mobile Health in early 2015, it addresses the challenge of data protection to 'go digital' - the third objective of the EDPS Strategy – 'customising existing data protection principles to fit the global digital arena', also in the light of the EU's plans for the Digital Single Market. It is consistent with the approach of the Article 29 Working Party on data protection aspects of the use of new technologies, such as the ´Internet of Things´, to which the EDPS contributed as a full member of the group.


Future-oriented rules and enforcement
Accountable controllers
Dignity
Ethics
Empowered individuals
Innovative privacy engineering

‘Human dignity is inviolable. It must be respected and protected.’

Article 1, EU Charter of Fundamental Rights

The fundamental rights to privacy and to the protection of personal data have become more important for the protection of human dignity than ever before. They are enshrined in the EU Treaties and in the EU Charter of Fundamental Rights. They enable individuals to develop their own personalities, to lead independent lives, to innovate and to exercise other rights and freedoms. The data protection principles defined in the EU Charter -necessity, proportionality, fairness, data minimisation, purpose limitation, consent and transparency- apply to data processing in its entirety, to collection as well as to use.

Technology should not dictate values and rights, but neither should their relationship be reduced to a false dichotomy. The digital revolution promises benefits for health, the environment, international development and economic efficiency. Under the EU's plans for a digital single market, cloud computing, the ‘Internet of Things’, big data and other technologies are considered key to competitiveness and growth. Business models are exploiting new capabilities for the massive collection, instantaneous transmission, combination and reuse of personal information for unforeseen purposes, and justified by long and impenetrable privacy policies. This has placed the principles of data protection under new strains, which calls for fresh thinking on how they are applied.

In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing. The EU's regulatory framework already allows room for flexible, case-by-case, decisions and safeguards when handling personal information. The reform of the regulatory framework will be a good step forward. But there are deeper questions as to the impact of trends in data driven society on dignity, individual freedom and the functioning of democracy.

These issues have engineering, philosophical, legal and moral implications. This Opinion highlights some major technology trends which may involve unacceptable processing of personal information or may interfere with the right to privacy. It outlines a four-tier ‘big data protection ecosystem’ to respond to the digital challenge: a collective effort, underpinned by ethical considerations.

(1) Future-oriented regulation of data processing and respect for the rights to privacy and to data protection.

(2) Accountable controllers who determine personal information processing.

(3) Privacy conscious engineering and design of data processing products and services.

(4) Empowered individuals.

The European Data Protection Supervisor wants to stimulate an open and informed discussion in and outside the EU, involving civil society, designers, companies, academics, public authorities and regulators. The new EU data protection ethics board we will establish at the EDPS will help define a new digital ethics, allowing to realise better the benefits of technology for society and the economy in ways which reinforce the rights and freedoms of individuals.

TABLE OF CONTENTS

1. Data everywhere: Trends, opportunities and challenges........ 6

1.1 BIG DATA........ 6

1.2 ‘INTERNET OF THINGS’........ 7

1.3 AMBIENT COMPUTING........ 7

1.4 CLOUD COMPUTING........ 7

1.5 PERSONAL DATA-DEPENDENT BUSINESS MODELS........ 8

1.6 DRONES AND AUTONOMOUS VEHICLES........ 8

1.7 TRENDS WITH A POTENTIALLY LARGER, LONGER-TERM IMPACT........ 9

2. A big data protection ecosystem........ 9

2.1 FUTURE-ORIENTED REGULATION........ 9

2.2 ACCOUNTABLE CONTROLLERS........ 10

2.3 PRIVACY-CONSCIOUS ENGINEERING........ 10

2.4 EMPOWERED INDIVIDUALS........ 11

A ‘prosumer’ environment........ 11

Consent........ 11

Control and data ‘ownership’........ 11

3. Dignity at the heart of a new digital ethics........ 12

3.1 DIGNITY AND DATA........ 12

3.2 A EUROPEAN ETHICS ADVISORY BOARD........ 14

4. Conclusion: Time to deepen the discussion........ 14

Notes........ 16

1. Data everywhere: Trends, opportunities and challenges

Ever-increasing amounts of personal information are being collected and processed in increasingly opaque and complex ways. With the progressive deployment of computers in businesses and public administrations in the 1980s, there was a widespread perception that the practices of powerful governments and corporations in processing personal data was reducing individuals to the status of mere data subjects, threatening fundamental rights and freedoms. What distinguishes the current wave of integrated information and communication technology is its ubiquity and power.

Last year it was reported that there were more connected devices on the planet than people[1]. Increases in processor capacity[2], storage and transmission bandwidth mean that there are progressively fewer technical constraints on processing of personal information. The 'Internet of Things' and big data analytics are expected to converge with artificial intelligence, natural language processing and biometric systems to empower applications with machine-learning ability for advanced intelligence. Governments and companies are able to move beyond 'data mining' to 'reality mining', which penetrates everyday experience, communication and even thought[3]. As society adjusts to the demands of the digital marketplace, there are now renewed efforts to teach programming to young children[4]. Harnessing these trends in a sector where the EU is a leading consumer but laggard in service provision, is a recurring theme in the Commission's Digital Single Market strategy[5].

These trends and many of the concepts used today, despite their currency, are vague and overlapping. To help stimulate a debate, we wish to highlight specific trends which -though obviously not exhaustive in our view raise the most important ethical and practical questions for the application of data protection principles.

1.1 Big data

'Big data'[6] refers to the practice of combining huge volumes of diversely sourced information and analysing them, often using self-learning algorithms to inform decisions. This information is not always personal: data generated by sensors for monitoring natural or atmospheric phenomena like the weather or pollution, or for monitoring technical aspects of manufacturing processes, do not relate to 'an identified or identifiable natural person'[7]. But one of the greatest values of big data for businesses and governments is derived from the monitoring of *human* behaviour, collectively and individually, and resides in its predictive potential[8].

One result is the emergence of a revenue model for Internet companies relying on tracking online activity to optimise the economic value of transactions to service providers, not only in targeted advertising but also in the conditions and rates of insurance policies, loans and other contractual relationships. In the competitive market for users' attention, most people are unaware of the broad extent of this tracking[9]. Such 'big data' should be considered personal even where anonymisation techniques have been applied: it is becoming ever easier to infer a person's identity by combining allegedly 'anonymous' data with other datasets including publicly available information for example on social media[10]. Where that data is traded especially across borders and jurisdictions, accountability for processing the information becomes nebulous and difficult to ascertain or enforce under data protection law, particularly in the absence of any international standards.

1.2 ‘Internet of Things’

Many Internet-connected devices are already commonplace, like smartphones, tablets and machines for dispensing cash and for flight check-ins. By 2020 connectivity is predicted to become a standard feature, with 25 billion connected objects (compared to 4.8 billion in 2015) ranging from telemedicine to vehicles, from smart meters to a whole range of new stationary and mobile devices for enabling smart cities[11].

These sensors will provide immediate and granular information which statistical offices and surveys cannot reach today, but which is not necessarily more accurate and may even be potentially misleading[12]. The estimated 1.8 bn automotive machine-to-machine connections by 2022 could reduce accidents and pollution, increase productivity and the autonomy of the elderly and the disabled[13]. ‘Wearables’, like clothes and watches will process personal information like other connected devices. They will be able to detect blood clots and to monitor fitness and wound healing; connected fabrics could protect against extreme environments, in firefighting for example. These devices will upload personal data directly into cloud storage, linked to social networks and potentially broadcast publicly, enabling identification of users and tracking of the behaviour and movements of individuals and crowds[14].

How this information is handled could affect the privacy not only of the users of the devices, including where used in the workplace, but also the rights of others who are observed and recorded by the device. While there is little evidence of actual discrimination, it is clear that the huge volume of personal information collected by the ‘Internet of Things’ is of great interest as a means for maximising revenue through more personalised pricing according to tracked behaviour, particularly in the health insurance sector[15]. Other domain-specific rules will also be challenged, for example where devices involving processing of health data are not be technically categorised as medical devices and fall outside the scope of regulation[16].

1.3 Ambient computing

Ambient or invisible computing refers to a key technology underlying the ‘Internet of Things’. One of its most obvious applications is ‘smart homes’ and ‘smart offices’ composed of devices with built-in sophisticated information processing capacity, which promise greater energy efficiency and more informed individuals able to influence their consumption remotely (though it would depend on the independence of the resident from the landlord or building manager). It will need to be clear who is responsible for the purpose and means of processing of the personal data involved in ambient computing applications, not only for protecting individuals' fundamental rights but also for appropriate allocation of liability for ensuring respect for overall system security requirements.

1.4 Cloud computing

Cloud computing is known as a central enabling technology both for the advanced analytics and mining capabilities, big data collection and analytics, and the flood of data from the ‘Internet of Things’, currently used by about a fifth of individuals and businesses in the EU[17]. It enables the concentration of data from the myriad ‘Internet of Things’ devices and relies on the availability and connectivity of enormous volumes of data in large-scale storage and processing facilities around the world[18]. Wider adoption of cloud computing[19] by private and public sectors is estimated potentially to add a total of €449 bn to the EU28 GDP (0.71% of total EU GDP).

Control over personal information is often shared between the customer and the cloud service provider and the responsibility for data protection obligations is not always clear. This might mean that insufficient protection is provided in practice. These obligations are irrespective of the **physical location of the data storage. Moreover,** even though only a background technology supporting the business applications, cloud computing infrastructure itself may become a critical infrastructure and increase the imbalances in market power, with 30% of businesses recently claiming difficulty in unsubscribing or changing providers[20].

1.5 Personal data-dependent business models

These technologies have enabled new business models which rely on information not only generated from service provision but also from other sources like social media presence to assess risk and creditworthiness and maximise revenue. A prominent business model today is represented by platforms which link sellers and buyers, enabling the sharing and redistribution of products, services, skills and assets. Often referred to as the 'sharing economy', 'collaborative consumption' or online and mobile peer-to-peer business platforms,[21] these platforms may offer classic economic efficiencies, inject competitiveness into markets and reduce waste. Their global value is estimated to quadruple in value from $26 to $110 billion in coming years[22]. Such data-driven business models are already generating enormous revenues in car sharing and home rentals and in financial technology and social lending. Surveys indicate that consumers appreciate their apparent greater affordability and convenience[23].

The currency of such platforms is typically user reputation, peer reviews and identity verification. This potentially may be seen as enhancing transparency and accountability, but not necessarily in relation to the platform provider itself. Large players in these markets have been criticised for allegedly withholding reputational data from the very individual users to whom the information relates. There is a huge risk that individuals could be excluded from services on the basis of reputations based on inaccurate data which they cannot challenge or request to be deleted. The reliance on data from multiple sources also calls into question the principle in EU law of data minimisation. The extent of the future impact on individuals and society of these and future technology-enabled business models merits careful reflection[24].

1.6 Drones and autonomous vehicles

Drones**,** or semi-autonomous aircraft, currently serve mainly military purposes, but are increasingly used for purposes of surveillance, mapping, transportation, logistics and public security, such as containing wildfires[25]. Photographs, videos and other personal data collected by drones can be exchanged over telecommunications networks. Their use risks serious interference with privacy and a chilling effect on freedom of expression. The question arises how their design and use can be effectively regulated so that data subjects can exercise their rights to access data captured by these machines.

On the ground, autonomous vehicles or driverless cars will change the way individual travel is used and organised, and may blur the difference between private and public transport. It is estimated that there will be 12 million fully autonomous and 18 million partly autonomous vehicles by 2035, with Europe among the early adopters[26]. The algorithms steering the cars will govern decisions which may directly concern the physical integrity and even life or death of individuals, for example in the choice programmed in the event of an unavoidable impact. As well as the obvious need for clarity on who is responsible and liable for data control and data security, these applications raise a number of ethical questions.

1.7 Trends with a potentially larger, longer-term impact

3D bioprinting of organic items, which uses copies of patients cells and collagen ‘bio bandages’ (that is, sensitive data under EU law) to lay down successive rows of living cells, is estimated to become soon readily available[27]. It would ease supply of customised human anatomical parts and be particularly valuable in poorer and post-conflict areas of the world. Bioprinting raises obvious questions for medical ethics, safeguarding of intellectual property and consumer protection but also, as it relies on the processing of intimate and sensitive data concerning individuals health, for the application of the data protection rules.

Artificial intelligence, like robotics, refers to a technological requirement for autonomous machines both stationary and mobile. Their advancement will offer immense potential beyond their current application. Deep learning computers teach themselves tasks by crunching large data sets using (among other things) neural networks that appear to emulate the brain. Researchers and companies are aiming to improve unsupervised learning. Already algorithms can understand and translate languages, recognise images, write news articles and analyse medical data[28]. Social media supply vast amounts of personal information effectively pre-labelled by individuals themselves. This may be the latest in a line of cognitive enhancements to augment ability of the human brain, like paper or the abacus or integrated into autonomous machines, robots, but now is the moment to consider the wider ramifications for individuals and society[29].

2. A big data protection ecosystem

The EU now has the opportunity to lead the way in demonstrating how governments, regulators, controllers, designers, developers and individuals can better act together to reinforce rights and to steer, not to block, technological innovation. The trends described in section two have, according to one commentator, ‘widened the gap between what is possible and what is legally allowed’[30]. Contrary to some claims, privacy and data protection are a platform for a sustainable and dynamic digital environment, not an obstacle. Independent data protection authorities like the EDPS have a key role in dispelling such myths and responding to individuals’ genuine concerns of loss of control over their personal information[31].

The next generation of personal data is likely to be even less accessible to the individuals to whom it relates. Responsibility for shaping a sustainable digital single market is necessarily dispersed, but it is also interdependent, like an ecosystem, requiring effective interaction between developers, businesses and regulators in the interests of the individual. In this section we outline the contribution that these four essential players can bring.

2.1 Future-oriented regulation

We recently urged the EU to seize its historic opportunity to put in place simpler rules for handling personal information which will stay relevant for a generation[32]. Negotiations on the General Data Protection Regulation and the directive for data protection in the police and judicial sectors are in the final stages, and attention will soon turn to the future of the e-Privacy Directive on electronic communications and the new Regulation governing how EU institutions and bodies themselves process personal data. With the economic cost of collecting and storing data close to negligible, it will fall to data protection authorities to enforce these rules consistently to avoid the ‘moral hazard’ of excessive data processing[33].

The Digital Single Market strategy recognises the link between the control of large volumes of data and market power. It shares the conviction, expressed in our 2014 preliminary

Opinion on ‘Privacy and Competitiveness in the Age of Big Data’, of the need for more coherence among regulators. The EU already has the tools for redressing the power imbalances in the digital market: for example the European Commission's ongoing antitrust proceedings are an acknowledgement of the predominance of mobile devices for accessing the Internet. More holistic enforcement is possible within the existing legal framework, such as through an EU clearing house for supervisory authorities to consider whether individual cases may raise questions of compliance with competition, consumer and data protection rules. For example:

- Requiring greater transparency of the price - cash or otherwise - for a service, can inform and facilitate the analysis of competition cases[34], and

- Detecting unfair price discrimination on the basis of poor data quality and unfair profiling and correlations[35].

Closer dialogue between regulators from different sectors could lead to a response to growing calls for global partnerships which can create a ‘commons’ of open data where data and ideas, such as statistics and maps, can flow and be available and exchanged in the public interest, with less risk of surveillance, to give individuals more influence over decisions which affect them[36].

2.2 Accountable controllers

Accountability requires putting in place internal policies and control systems that ensure compliance and provide relevant evidence in particular to independent supervisory authorities.

We have argued for eliminating bureaucracy in data protection law, by minimising the requirements for unnecessary documentation to maximise room for more responsible initiative by businesses, supported by guidance from data protection authorities. The principle that personal data should be processed only in ways compatible with the specific purpose(s) for which they were collected is essential to respecting individuals’ legitimate expectations. For example, codes of conduct, audits, certification, audits and a new generation of contractual clauses and binding corporate rules can help build a robust trust in the digital market. Those responsible for handing personal information should be much more dynamic and proactive and move away from the so-called ‘Black Box’ tendency of secrecy and opacity of business practices while demanding ever more transparency of customers[37].

2.3 Privacy-conscious engineering

Human innovation has always been the product of activities by specific social groups and specific contexts, usually reflecting the societal norms of the time[38]. However technological design decisions should not dictate our societal interactions and the structure of our communities, but rather should support our values and fundamental rights.

The EU should develop and promote engineering techniques and methodologies that permit implementing data processing technologies to fully respect the dignity and rights of the individual. Systems and software engineers need to understand and better apply the principles of privacy-by-design in new products and services across design phases and technologies. Accountability needs to be supported by greater research and development into methods and tools for ensuring accurate audits and for determining the compliance of controllers and processors with the rules, such as by 'tagging' every unit of personal data with 'metadata' that describing data protection requirements.

Engineering solutions should empower individuals who wish to preserve their privacy and freedom through anonymity. The EU should promote the design and implementation of algorithms that conceal identities and aggregate data in order to protect the individual at the same time as harnessing the predictive power of the data[39].

We must today lay the foundation for addressing these tasks by bringing together developers and data protection experts from different areas in broad networks, such as the Internet Privacy Engineering Network (IPEN), which contribute to a fruitful inter-disciplinary exchange of ideas and approaches.

2.4 Empowered individuals

A 'prosumer' environment

Individuals are not merely passive objects who require protection of the law against exploitation. The digital trends described above present positive opportunities for strengthening the role of the individual. For example, people now produce as well as consume content and services, and increasingly may be considered jointly responsible with service providers for processing personal data, unless it is for purely 'household' purposes[40] (the concept of 'prosumers' has emerged to describe this development[41]). Meanwhile, virtual currencies offer users anonymity and the bypassing of third party verification of transactions, and so lower transaction costs in paying for goods and services across borders. On the other hand, the anonymity and cross-jurisdictional (or, it might be argued, *a-jurisdictional*) nature of these virtual currencies leave individuals vulnerable to fraud and criminal markets which are hard to detect and investigate. Aside from the duties of regulators, businesses and engineers, citizens too have a responsibility to be aware, alert, critical and informed when making choices on- as well as offline[42].

Consent

Moreover, contrary to traditional thinking, not all human behaviour can be explained by economic principles which assume that human beings are entirely rational and sensitive to economic incentives[43]. This is relevant to the future role of consent by the individual to the processing of personal information about him or him. Under EU law, consent is not the only legitimate basis for most processing. Even where consent plays an important role, it does not absolve controllers from their accountability for what they do with the data, especially where a generalised consent to processing for a broad range of purposes has been obtained.

Control and data 'ownership'

Individuals must be able to challenge mistakes and unfair biases arising from the logic used by algorithms to determine assumptions and predictions. By way of illustration, in the US a study of almost 3,000 credit reports belonging to 1,000 consumers and found that 26 percent had 'material' errors problems serious enough to affect the consumers' credit scores and the therefore the cost of obtaining credit[44].

Data is often considered a resource, like oil, to be traded, ideally by equally well informed parties to the transaction[45]. Customers are not fairly compensated for their personal information which is traded, and some have argued in favour of a data ownership model.

Absolute control over personal data is however difficult to guarantee - there will be other concerns such as public interest and the rights and freedoms of others. Control is necessary but not sufficient[46]. However human dignity is always a constant, and under EU law, the analogy of ownership cannot be applied as such to personal information, which has an intrinsic link to individual personalities. There is no provision in EU data protection law for an individual to waive this fundamental right.

One alternative method for giving individuals better control over their data, who can access and for what purpose, could be the use of personal data stores or 'data vaults'[47]. The concept of such a 'personal store' requires security mechanisms that ensure that only those entities authorised by the data subject can access the data and only those parts for which they are authorised. Personal data stores would be most effective where they concern current and constantly updated information, such as geospatial data or signs of life. Beyond the technical safeguards, data users would be obliged to respect the rules about data sharing and use. Competition and the possibility to change the service one is using is the single most effective power of a consumer to influence the market of services available to them. Ensuring the portability of connections, including identifiers and contact information, has proven to be a powerful enabler for competition and has effectively reduced consumer prices when the telecoms market was liberalised. Data portability, that is the factual and practical possibility to transfer most of one's own data from one service provider to another, is an effective starting point for creating the conditions for true consumer choice.

3. Dignity at the heart of a new digital ethics

An ethical framework needs to underpin the building blocks of this digital ecosystem. The EDPS considers that better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics.

3.1 Dignity and data

In the wake of the industrial revolution of the 18th and 19th centuries, the human rights movement sought to secure the wider social good by reducing obstacles to respect for the individual. The EU has now, with the Charter of Fundamental Rights, and following the Universal Declaration of Human Rights and the European Convention of Human Rights, taken as its starting point the inviolability of human dignity. The dignity of the human person is not only a fundamental right in itself but also is a foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data[48]. Violations of dignity may include objectification, where a person is treated as a tool serving someone else's purposes[49]. Privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing. In Germany the right to 'informational self-determination' was based on the rights to personal dignity and to free development of the personality laid down in Articles 1 and 2 of the German Constitution[50].

However in the early 21st century, individuals are increasingly required to disclose much more personal information over the Internet in order to participate in social, administrative and commercial affairs, with ever more limited scope for opting out. With all activity potentially always online, the notion of free and informed consent is placed under enormous strain. 'Digital breadcrumbs' are dropped every minute and combined to classify individuals in real time to create multiple and at times contradictory profiles. These profiles can be circulated in microseconds without individuals' knowledge, and used as the basis for important decisions affecting them.

Profiles used to predict people's behaviour risk stigmatisation, reinforcing existing stereotypes, social and cultural segregation and exclusion[51], with such ‘collective intelligence’ subverting individual choice and equal opportunities. Such ‘filter bubbles’ or ‘personal echo-chambers’ could end up stifling the very creativity, innovation and freedoms of expression and association which have enabled digital technologies to flourish.

Meanwhile a continued state of exception on grounds of ‘security’ is used to justify the multiple layering of intrusive techniques for monitoring individuals' activity[52]. Understanding this ‘surveillance ratchet’ requires a longer term perspective on the overall effects on society and behaviour.

Along with third countries, the EU needs to look hard at how to ensure these values not merely respected on paper while in effect being neutralised in cyberspace. The EU in particular now has a ‘critical window’ before mass adoption of these technologies to build the values into digital structures which will define our society[53]. This requires a new assessment of whether the potential benefits of the new technologies really depend on the collection and analysis of the personally-identifiable information of billions of individuals. Such an assessment could challenge developers to design products which depersonalise in real time huge volumes of unorganised information making it harder or impossible to single out an individual.

We already recognise that certain data processing, genetic data for example, must not only be regulated but also subject to evaluation of wider societal concerns by for instance ethics committees. By their very nature, genetic data relate not only to one individual, but also to their ancestry and offspring. Genetic data not only serve to identify family relationships, but elements found in the genes of one individual can also provide information about their parents and children, and lead to decisions by controllers which influence their chances in life even before their birth. The potential concentration of genetic personal data in the hands of a few giant market players has implications for market economies as well as data subjects. A growing dependence on a global system of collection and analysis of a constant flow of data could make society and economy more vulnerable to unprecedented security flaws and malicious attacks.

The existing framework could fail if we do not approach the future with innovative thinking. There is an increasing demand and need to consider the data subject as an individual not simply as a consumer or user. Truly independent data protection authorities have a crucial role in preventing a future where individuals are determined by algorithms and their continuous variations. They need to be equipped to exercise a ‘duty of care’ towards individuals and their dignity online. Traditional privacy and data protection concepts and principles already contained ethical nuances for the protection of dignity, such as employment and health. But today's trends have opened an entirely new chapter, and there is a need to explore whether the principles are robust enough for the digital age[54]. The notion of personal data itself is likely to change radically as technology increasingly allows individuals to be re-identified from supposedly anonymous data. In addition, machine learning and the merging of human and artificial intelligence will undermine concepts of the individual's rights and responsibility.

3.2 A European Ethics Advisory Board

This is not to paint an alarmist picture of dystopia. Discussions are already ongoing in the legal, political, economic, social, scientific and even religious spheres[55]. Simplistic approaches that give unilateral advantage to economic profit or surveillance for security are probably no more useful than overly restrictive application of existing laws that stifle innovation and progress. The EDPS therefore proposes a thorough, broad and multidisciplinary analysis to provide recommendations and inform societal debate on how a free, democratic society should meet the technological challenge.

The EDPS Strategy [56] committed to developing an ethical approach to data protection which recognised that 'feasible, useful or profitable does not equal sustainable' and which stressed 'accountability over mechanical compliance with the letter of the law'. We intend to reach out beyond the community of EU officials, lawyers and IT specialists towards eminent persons who are equipped to judge the medium to long-term implications of technological change and regulatory responses. In the coming months, we will establish at our independent institution an external advisory group on the ethical dimension of data protection to explore the relationships between human rights, technology, markets and business models in the 21st century.

Our Ethics Advisory Board will be composed of a select group of distinguished persons from the fields of ethics and philosophy, sociology, psychology, technology and economics, supported as required by additional experts with knowledge and expertise in areas like health, transport and energy, social interaction and media, economy and finance, governance and democracy and security and policing. They will be invited to consider the wider ethical implications of how personal data is conceived and used, with maximum transparency given to their deliberations.

4. Conclusion: Time to deepen the discussion

Privacy and data protection are part of the solution, not the problem. For the time being, technology is controlled by humans. It is not easy to classify neatly these potential developments as good or bad, desirable or harmful, advantageous or detrimental, even less so when a number of potential trends have to be seen in context. Policy makers, technology developers, business developers and all of us must seriously consider if and how we want to influence the development of technology and its application. But equally important is that the EU consider urgently the ethics and the place for human dignity in the technologies of the future.

Data protection principles have proven capable of safeguarding individuals and their privacy from the risks of irresponsible data processing. But today's trends may require a completely fresh approach. So we are opening a new debate to what extent the application of the principles such as fairness and legitimacy is sufficient. The data protection community can play a new role using existing tools like prior checks and authorisations - because no other bodies are equipped to scrutinise such data processing. With technology, global innovation and human connectedness developing at breakneck speed, we have an opportunity to attract attention, to trigger interest and to build a consensus.

With this Opinion we hope to provide a framework for a wider and deeper discussion on how the EU can ensure the integrity of its values at the same time as it embraces the benefits of the new technologies.

Done in Brussels, 11 September 2015

(**signed**)

Giovanni BUTTARELLI
European Data Protection Supervisor

Notes

[1] Source: GSMA Intelligence.

[2] 'Moore's Law' that the number of transistors that can be put on a microchip doubles about every 18 months has proven generally accurate; Moore, Gordon E. (1965-04-19). 'Cramming more components onto integrated circuits', Electronics. 2011-08-22.

[3] Nathan Eagle, Alex (Sandy) Pentland, 'Reality mining: sensing complex social systems', Journal Personal and Ubiquitous Computing Volume 10 Issue 4, March 2006, pp. 255–268. Shoshana Zuboff in 'Big Other: surveillance capitalism and the prospects of an information civilization', Journal of Information Technology (2015) 30, pp. 75-89, writes 'As a result of pervasive computer mediation, nearly every aspect of the world is rendered in a new symbolic dimension as events, objects, processes, and people become visible, knowable, and shareable in a new way'. Zuboff envisages a 'the rise of a new universal architecture' which she calls 'Big Other', 'a ubiquitous networked institutions regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit'; pp. 77, 81.

[4] 'BBC Micro Bit computer's final design revealed' 7.7.2015, http://www.bbc.com/news/technology-33409311(accessed 10.09.2015); 'No assembler required: How to teach computer science in nursery school', The Economist, 1.8.2015.

[5] None of the top ten companies in the technology sector by market capitalisation is based in the EU (eight are US companies, one each in China and Taiwan) according to the PWC Global Top Ten Companies by Market Capitalisation, 31 March 2015 Update.

[6] '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: analytics) using computer algorithms'; WP29 Opinion 3/2013 on purpose limitation. A White House report in 2014 described Big Data as 'The growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data', see Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President ('Podesta-report'), May 2014.

[7] Under EU law, 'personal data' are defined as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'; Article 2 (a) Directive 95/46/EC. This definition is broadly comparable to those adopted by the Council of Europe in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108) and by OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. For an in-depth analysis see Article 29 Working Party 'Opinion 4/2007 on the concept of personal data', WP136.

[8] See for example speech from United States Federal Trade Commission Chairwoman in 2014: 'The proliferation of connected devices, the plummeting cost of collecting, storing, and processing information, and the ability of data brokers and others to combine offline and online data means that companies can accumulate virtually unlimited amounts of consumer information and store it indefinitely. Using predictive analytics, they can learn a surprising amount about each of us from this;' Opening Remarks FTC Chairwoman Edith Ramirez, 'Big Data: A Tool for Inclusion or Exclusion?', Washington, DC September 15, 2014. According to Sandy Pentland, 'Social physics is a quantitative social science that describes reliable, mathematical connections between information and idea flow on the one hand and people's behaviour on the other… it enables us to predict the productivity of small groups, of departments within companies and even of entire cities'. This 'is what is required to build better social systems' (pp. 4, 7) and to 'allow (government officials, industry

managers, and citizens) to use the tools of social network incentives to *establish new norms of behavio'* (p. 189) (our italics); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Special Eurobarometer 431 on Data Protection, June 2015 and Pew Research Panel Survey January 2014 on Public Perceptions of Privacy and Security in the Post-Snowden Era. An average visit to a single website according to one study results in 56 instances of data collection, according to Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). The 2014 White House report on big data argues that 'unprecedented computational power and sophistication… create an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it'; 'some of the most profound challenges revealed during this review concern how big data analytics may ... create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms'.

[10] Using 1990 census public anonymous data, 87% of the US population could be likely identified by their five digit zip code combined with gender and date of birth; see Paul Ohm 'Broken promises of privacy: responding to the surprising failure of anonymisation', UCLA Law Review 2010 and 'Record linkage and privacy: issues in creating new federal research and statistical info', April 2011. DNA is unique (except for identical twins) and stable throughout a lifetime. It contains information on ethnicity, predispositions to disease and can identify other family members. In January 2013 researchers were able to identify individuals and families from anonymous DNA data from publicly accessible genealogy databases; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). See also 'Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts', 23.06.2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (accessed 10.09.2015). See also WP29 Opinion 04/2007 on the concept of personal data; WP29 Opinion 03/2013 on purpose limitation; WP29 Opinion 06/2013 on open data and 'PSI' reuse; and WP29 Opinion 05/2014 on anonymisation.

[11] Source: Gartner.

[12] See for example panel discussion 'What is the future of official statistics in the Big Data era?' the Royal Statistical Society, London 19 January 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (accessed 10.09.2015).

[13] Ten technologies which could change our lives: potential impacts and policy implications, Scientific Foresight Unit, European Parliamentary Research Service, January 2015.

[14] The EU's Horizon 2020 Work Programme 2016–2017 is supporting these developments including large scale pilots which will look at privacy and ethical concerns.

[15] Insurance has been described as 'the native business model for the Internet of Things'; 'From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance industry', Business Insider 11.6.2015. The notion of price discrimination in competition law, derived from Article 102 TFEU, which prohibits a dominant undertaking in a market from 'directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions', is highly contentious, see for example Damien Gerardin and Nicolas Petit Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles (July 2005), Global Competition Law Centre Working Paper Series No. 07/05. On big data and its (according to the authors not yet realised) potential to accelerate personalised pricing, see Executive Office of the President of the United States, Big Data and Differential Pricing, February 2015, and a recent analysis which concludes that personalised pricing generally entails the processing of personal data, and therefore must respect data protection law's transparency principle which requires companies to inform people about the purpose of processing their personal data: companies must say so if they personalise prices. And if a company uses a cookie to recognise somebody, the e-Privacy Directive requires the company to inform the person about the cookie's purpose'; working draft by Frederik Borgesius 'Online Price Discrimination and Data Protection Law'. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (accessed 10.09.2015).

[16] Medical devices are defined in EU law under Council Directive 93/42/EEC concerning medical devices amended by Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007. On the data protection implications of 'mobile health', see EDPS Opinion 1/2015.

[17] According to Eurostat, 21% individuals and 19% businesses in the EU use cloud storage services.

[18] 'If the worldwide Internet were a country, it would be the 12th-largest consumer of electricity in the world, somewhere between Spain and Italy. This represents roughly 1.1 to 1.5 percent of global electricity use (as of 2010) and the greenhouse gases generated annually by 70 to 90 large (500-megawatt) coal-fired power plants'. Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

[19] Report of the study 'SMART 2013/0043 - Uptake of Cloud in Europe'.

[20] Source: Eurostat.

[21] The term 'sharing economy' has been criticised as misleading: 'The Sharing Economy Isn't About Sharing at All', Giana M. Eckhardt and Fleura Bardhi, Harvard Business Review, 28.01.2015.

[22] Rachel Botsman and Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

[23] Future of Privacy Forum, 'User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy', June 2015.

[24] See 9 June 2015 workshop by US Federal Trade Commission on 'Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy', https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (accessed 10.09.2015).

[25] On the data protection implications of drones or remotely piloted aircraft systems, see EDPS opinion on the Communication from the Commission to the European Parliament and the Council on 'A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner', November 2014.

[26] Source: Boston Consulting Group.

[27] Gartner.

[28] Facebook DeepFace facial recognition algorithm has reported 97% success - outperforming people; DeepFace: Closing the Gap to Human-Level Performance in Face Verification, published in report on IEEE Conference on Computer Vision and Pattern recognition June 2014.

[29] Robo has been defined as a 'machine situated in the world that senses, thinks, and acts'; Bekey, G, Current trends in robotics: technology and ethics, in Robot Ethics - The ethical and social implications of robotics, The MIT Press2, 2012, p. 18. It is estimated that 22m service robots will have been sold between 2013 and 2016; IRF World Robotics Report, 2013. On AI see Rise of the Machines, Economist, 09.5.15 and Pew Research Centre Internet Project 2014. An artificial intelligence company made its acquisition by a leading tech company in 2014 conditional on the establishment of an ethics and safety board and a prohibition on use of AI work military or intelligence purposes; Forbes, Inside Google's Mysterious Ethics Board, 03.02.2014.

[30] Pentland, *Social physics*, p. 147

[31] See note 9 above. Pentland *Social Physics* p.153: 'Great leaps in health care, transportation, energy and safety are all possible… the main barriers to achieving these goals are privacy concerns and the fact that we don't yet have any consensus around the trade-offs between personal and social values'. The debate surrounding the 2014 Ebola pandemic in West Africa is illustrative of how this false dichotomy between individual privacy and societal needs is drawn. Diseases have tended to be tracked and their lifespan measured via surveys and censuses which easily get out of date and which

are hard to extrapolate to anticipate where will strike next. There are some examples of use of 'big data' to track malaria outbreaks in Namibia and Kenya, and in 2009 to track effectiveness of government health warnings during the Mexican swine flu crisis. One source of data is mobile call records which show the base station that handled the call and can give in real time a rough approximation of location of people and where they are going. Gathering all these records is not targeted - it cannot distinguish between those with or without Ebola. A Swedish non-profit mapped population mobility in West Africa but the data were not used because mobile phone operators would not release it to approved outside researchers, claiming that they required instructions from governments, who in turn cited privacy concerns which could not be warranted under EU law; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (accessed 10.09.2015)

[32] EDPS Opinion 3/2015.

[33] A big data assumption that 'N=all' refers to looking at all data points not just a sample, Viktor Mayer-Schönberger, and Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013 .The Lisbon Council and the Progressive Policy Institute have argued that prosperity will increase by maximising 'digital density'- 'the amount of data used per capita in an economy' http://www.lisboncouncil.net/component/downloads/?id=1178 (accessed 10.09.2015). The International Working Group on Data Protection in Telecommunications (know as 'the Berlin Group') have proposed derogations for big data from data protection principles; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (accessed 10.09.2015). The World Economic Forum has called for focusing on use and not collection and to move away from the requirement of consent for collection of personal data; Unlocking the Value of Personal Data: From Collection to Usage, 2013.

[34] See EDPS Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data.

[35] Article 21 of the Charter of Fundamental Rights prohibits 'Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'. Many of these categories of data ('revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life') are given enhanced protection under Article 8 of Directive 95/46/EC.

[36] On the idea of a digital commons see Ambition numérique: Pour une politique française et européenne de la transition numérique, French Digital Council, June 2015 p. 276; Bruce Schneier advocates creation of 'unowned public spaces' on the Internet, like public parks, *Data and Goliath*, pp. 188-189; Sandy Pentland argues for a 'public data commons', *Social Physics*, p. 179. On assessment of safety of publishing aggregated datasets as open data, see WP29 Opinion 06/2013 on open data and public sector information reuse.

[37] 'Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent' http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. On qualified transparency, see, e.g. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] 'Behind the technology that affects social relations lie the very same social relations', David Noble, 'Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools', in *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979. See also Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 pp. 89-90; and Zuboff, 'Big Other' (cited in note 3 above).

[39] Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014 (WP 216.)

[40] On narrowly construed exemption from data protection rules for purely personal or household purposes, see CJEU judgment Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů.*

[41] The term prosumer was coined by Alvin Toffler in *The Third Wave*, 1980. For a discussion of the 'prosumer environment' and how it should be regulated see Ian Brown and Chris Marsden, *Regulating Code*, 2013.

[42] Opinion of the European Group on Ethics in Science and New Technologies to the European Commission: Ethics of Security and Surveillance Technologies, Opinion No 28, 20.05.2015, p. 74.

[43]See for example, Homer Economicus: The Simpsons and Economics, ed. Joshua Hall, 2014.

[44] Under the most conservative definition of error, this means that 23 million Americans have material errors on a consumer report. Five percent of the study participants had errors that once corrected, improved their credit score such that they could obtain credit at a lower price; Federal Trade Commission, Report To Congress Under Section 319 Of The Fair And Accurate Credit Transactions Act Of 2003, December 2012; Chris Jay Hoofnagle, How the Fair Credit Reporting Act Regulates Big Data (September 10, 2013). Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet, 2013. Available at SSRN: http://ssrn.com/abstract=2432955.

[45] The WEF posits data as a valuable asset of the individual whose rights of possession, use and disposal may be given to companies and governments in exchange for services. See recent speeches also by Commission Vice-President Ansip speech, for example on 7.9.2015 at Bruegel annual meeting entitled 'Productivity, innovation and digitalisation - which global policy challenges?': 'Ownership and management of data flows, use and re-use of data. Management and storage of data. These underpin important emerging sectors like cloud computing, the Internet of Things and big data'.

[46] 'So who possesses the right to use the information and data that truly do not belong to one's self? This is an issue that transcends borders of commerce, ethics, and morals, leading to privacy issues and the protection of privacy'; Al-Khouri Nov 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. See also Margaret Jane Radin, Incomplete Commodification in the Computerized World, in The Commodification of Information 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: 'It makes a big difference whether privacy is thought of as a human right, attaching to persons by virtue of their personhood, or as a property right, something that can be owned and controlled by persons. Human rights are presumptively market-inalienable, whereas property rights are presumptively market-alienable'.

[47] The MIT Computer Science and Artificial Intelligence Lab's Crosscloud project supported by several EU-based companies aims to '1) make it easy to develop multi-user ('social') software using only front-end development and respecting the rights and privacy of users. And 2) allow users the freedom to move easily among applications, hardware platforms, and social networks, keeping their data and social connections'; http://openpds.media.mit.edu/#architecture (accessed 10.09.2015).

[48] See Explanation to Article 1 of the Charter of Fundamental Rights.

[49] Martha Nussbaum, Objectification, in Philopsophy and Public Affairs 24, 4, 1995.

[50] Judgment of 15 December 1983, BVerfGE 65, 1-71, Volkszählung.

[51] See European Group on Ethics in Science and New Technologies, Opinion on Ethics and Surveillance, p. 75. A study has suggested that an ad-targeting algorithm was discriminatory, with searches on average returning ads for higher paid jobs for men compared with women visiting job sites; Carnegie Mellon University and the International Computer Science Institute. On the tendency of digital assistants to be given by default a female voice, se for example Judy Wajcman, Feminist theories of technology. Cambridge Journal of Economics, 34 (1). pp. 143-152, 2010.

[52] Giorgio Agamben, *State of Exeption, 2005.*

[53] Neil Richards, Neil and Jonathan King, Big Data Ethics (May 19, 2014), Wake Forest Law Review, 2014.

[54] BBC, Information watchdog investigates 'charity data sales', 1.9.2015.

[55] See letter from Future of Life Institute. The Papal encyclical *Laudato Si:* 'when media and the digital world become omnipresent, their influence can stop people from learning how to live wisely, to think deeply and to love generously. In this context, the great sages of the past run the risk of going unheard amid the noise and distractions of an information overload. Efforts need to be made to help these media become sources of new cultural progress for humanity and not a threat to our deepest riches. True wisdom, as the fruit of self-examination, dialogue and generous encounter between persons, is not acquired by a mere accumulation of data which eventually leads to overload and confusion, a sort of mental pollution. Real relationships with others, with all the challenges they entail, now tend to be replaced by a type of Internet communication which enables us to choose or eliminate relationships at whim, thus giving rise to a new type of contrived emotion which has more to do with devices and displays than with other people and with nature. Today's media do enable us to communicate and to share our knowledge and affections. Yet at times they also shield us from direct contact with the pain, the fears and the joys of others and the complexity of their personal experiences. For this reason, we should be concerned that, alongside the exciting possibilities offered by these media, a deep and melancholic dissatisfaction with interpersonal relations, or a harmful sense of isolation, can also arise'.

[56] See Action 4 of the EDPS Strategy 2015-2020, developing an ethical dimension to data protection.