IDC
ANALYZE THE FUTURE

eLAW
LEIDEN

Fraunhofer

e-SIDES

Ethical and Societal Implications of Data Sciences

White Paper

Overview of emerging issues of big data technologies, and real-life cases

"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."

About the e-SIDES project

Data-driven innovation is deeply transforming society and the economy. Although there are potentially enormous economic and social benefits this innovation also brings new challenges for individual and collective privacy, security, as well as democracy and participation. The main objective of the CSA e-SIDES is to complement the research on privacy-preserving big data technologies, by analyzing, mapping and clearly identifying the main societal and ethical challenges emerging from the adoption of big data technologies, conforming to the principles of responsible research and innovation; setting up and organizing a sustainable dialogue between industry, research and social actors, as well as networking with the main Research and Innovation Actions and Large Scale Pilots and other framework program projects interested in these issues. It will investigate stakeholders' concerns, and collect their input, framing these results in a clear conceptual framework showing the potential trade-offs between conflicting needs and providing a basis to validate privacy-preserving technologies. It will prepare and widely disseminate community shared conclusions and recommendations highlighting the best way to ultimately build confidence of citizens and businesses towards big data and the data economy.

Deliverable D2.2 Lists of ethical, legal, societal and economic issues of big data technologies

Find more at: http://e-sides.eu/media/deliverable-22-lists-of-ethical-legal-societal-and-economic-issues-of-big-data-technologies

About this white paper

This document is an extract of the Deliverable D2.2 Lists of ethical, legal, societal and economic issues of big data technologies, released and published on 31 August 2017.

D2.2. Main contributors:

Bart Custers (Leiden University)

Karolina La Fors (Leiden University)

Magdalena Jozwiak (Leiden University)

Esther Keymolen (Leiden University)

Daniel Bachlechner (Fraunhofer ISI)

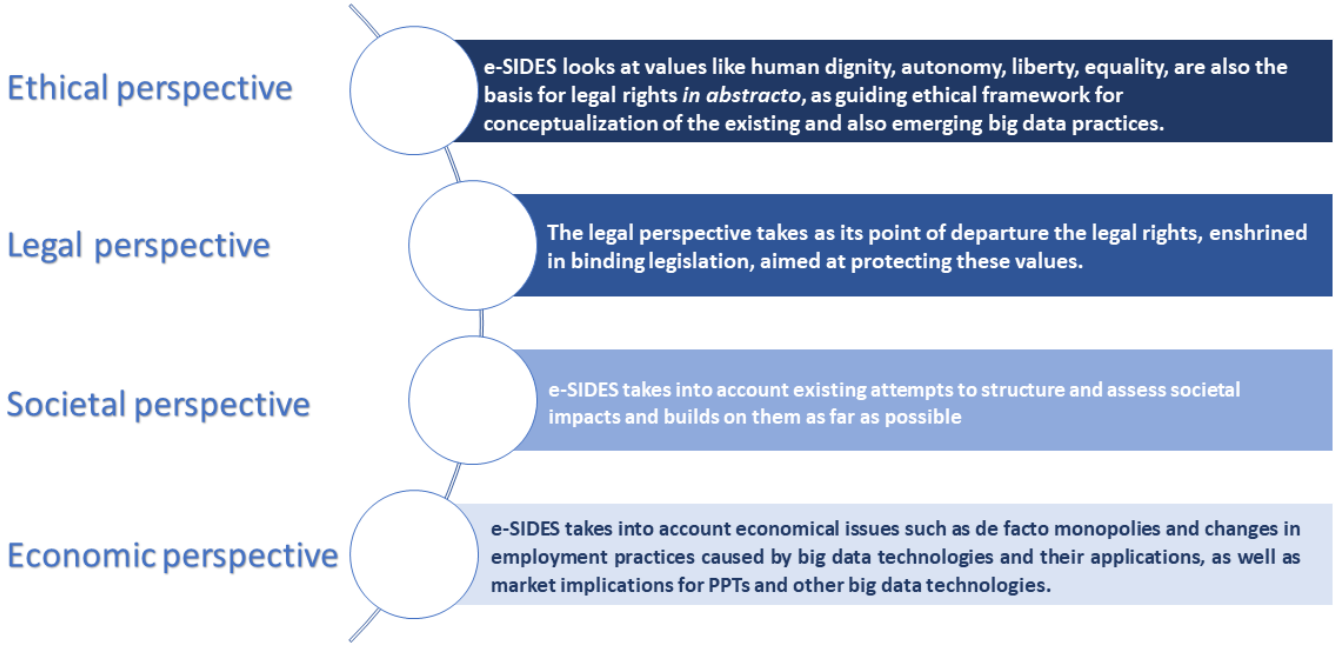
Michael Friedewald (Fraunhofer ISI)

Stefania Aguzzi (IDC)

Duncan Brown (IDC)

1. About this document

e-SIDES examines the implications of big data technologies from different perspectives to complement the research on privacy-preserving big data technologies. This white paper sets forth our main findings at this stage of the project and maps issues related to big data from four different perspectives.



The four perspectives taken on big data technologies

The selection of issues discussed, while not exhaustive, represents some of the most urgent challenges of the big data technologies approached from the various angles.

The lists of such issues were determined on the basis of research and through interaction with some of the stakeholders at the two project workshops.

This selection is aimed to form a useful stepping stone for the assessment of privacy-preserving big data technologies (both existing and under development) and also for the development of design requirements for these technologies in the next stages of e-SIDES.

2. Ethical perspective: main issues

In e-SIDES our ethical insights are gathered from moral philosophy, philosophy of technology and biomedical ethics, taking into account the ethical values that seem being most under pressure in contexts of big data technologies. For our analysis we have chosen the theoretical structure of virtue ethics.

We considered that virtue ethics may better accommodate the exploration of what ethical life in the big data era may look like. Virtue ethics does not conceive human beings as merely rational agents, but pays attention to their emotional disposition, their relations and the social context in which they operate. Moreover, because of its focus on practical wisdom, a virtue ethics approach fits well to theorize how to implement such values in design and practice.

We have chosen three lists of ethical values from philosophy of technology and one from biomedical ethics to draw our own selection. We used Shannon Vallor's technomoral virtues, Batya Friedman's values from value-sensitive design (VSD) and Philip Brey's list of values from anticipatory technology ethics. Given that the consequences of big data technologies are often unforeseeable for citizens we have chosen Beauchamp's and Childress's list of values from biomedical ethics as this discipline has a human- and care-centred attitude as prime guideline for practice.

Relevant ethical values	*Issues putting pressure upon values*	*Real-life examples*
Human welfare	When "emerging technologies are used as supplements for human caring" this endangers human welfare. This can thus be under pressure when, e.g. big data technologies take over (health)care tasks from humans or when they project discriminative images about humans to others. Detrimental implications can also occur in contexts of work, schooling, travelling, etc.	***The dangers of trusting robots.*** *"In February, a South Korean woman was sleeping on the floor when her robot vacuum ate her hair, forcing her to call for emergency help. It may not be the dystopian future that Stephen Hawking warned us about – where intelligent devices "spell the end of the human race" – but it does highlight one of the unexpected dangers of inviting robots into our home."* This article suggests that beyond tremendous positive potential, robots can indeed go bad and endanger human welfare. Evidence shows that sharing the deepest secrets of our lives to robots, for instance in forms of children toys (also called as anthropomorphic robots) can indeed be used against us as exploitative code. The article raises the question: "How do we protect ourselves from double-crossing decepticons?". Source: http://www.bbc.com/future/story/20150812-how-to-tell-a-good-robot-from-the-bad
Autonomy	Autonomy is at risk when big data technologies and data transfer processes are not transparent for citizens: when decision-making takes place without explanation about how a decision occurred, when big data-driven profiling practices limit free will, free choice, when they manipulate instead of support knowledge production as to news, culture or politics.	***Amazon Is Suggesting "Frequently Bought Together" Items That Can Make a Bomb****. A team from Channel 4 News found that Amazon has been prompting customers looking to buy "a common chemical used in food production" to also purchase other ingredients that, together, could be used to produce black powder. (The report did not specify exactly which ingredients, for obvious reasons.) Further down the page, according to the report, Amazon also nudged the customer to buy ball bearings, which can be used as shrapnel in homemade explosives.* Source: http://www.slate.com/
Non-maleficence	Non-maleficence could limit detrimental effects of big data-based calculations. For many new bid data systems no defined legal framework exists (yet). Although, for instance, data reuse in these systems would be possible for such purposes as earning profit this might violate one's privacy. During such dilemmas non-maleficence could be a vital compass.	***"OKCupid. A very large public dataset of dating site users. Open Differential Psychology****. In 2016 70,000 profiles from OkCupid (owned by Tinder's parent company Match Group) were made public by a Danish researcher, Emil Kirkegaard, who explored the correlations between cognitive ability, religious beliefs and even Zodiac signs (no correlation for this last one). Kirkegaard, E. O. W., & Bjerrekær, J. D. (2016)."* Source: http://www.pnas.org/c

Justice	In big data contexts systematic injustice emerges when, for instance, false positives occur during big data-led profiling practices within law enforcement or false negatives during biometric identification processes. As a direct consequence of big data-led correlations instances of false accusation, stigmatization and other forms of injustice also grow.	***Facial recognition tech perpetuates injustice***. *Australia's Prime Minister Malcolm Turnbull has pushed state premiers to hand over their drivers' licence database in order to enhance facial recognition systems, particularly at airports. COAG has agreed, with the ACT insisting that only perfect matches be used for non-counterterrorism purposes. It is hard to find this reassuring.* Source: https://www.eurekastreet.com.au
Accountability (incl. transparency)	Due to their rapid evolution accountability checks in big data-led processes are vital in democracies. Raising transparency as a pre-requisite assists to gain more of it. When, for instance, patients or consumers are unaware of how their data is shared for secondary purposes puts accountability at risk.	***The limits of transparency without accountability.*** *A Tinder user asked for her personal data (based on GDPR right of access) and was horrified by the amount and detail of the information. She got back 800 pages of online activities and preferences including Facebook likes, Instagram photos (even if the account had been cancelled), education, dating preferences, email chats with all the men she dated through Tinder. Her main worry is that this personal data may be hacked and sold. Tinder's privacy policy in fact denies accountability by stating "you should not expect that your personal information, chats, or other communications will always remain secure" and that the Tinder Scraper tool can "collect information on users in order to draw insights that may serve the public".* Source: https://www.theguardian.com
Trustworthiness	Being unable to refute their big data-based profile undermines citizens' trust, at the same time technology operators' trust often lies too much in big data-based decisions. When employed as a moral, mutual requirement for designers, data brokers, scientists and others, trustworthiness could improve effectivity, transparency as well as citizens' legal position.	***"British courts may unlock secrets of how Trump campaign profiled US voters.*** *A US professor is trying to reclaim his personal data from the controversial analytics firm that helped Donald Trump to power. In what legal experts say may be a "watershed" case, a US citizen is using British laws to try to discover how he was profiled and potentially targeted by the Trump campaign. British data protection laws may provide some transparency on the company at the heart of Trump's data operation – Cambridge Analytica – and how it created profiles of 240 million Americans."* Source: https://www.theguardian.com
Privacy	Persons can be identified through big datasets with ease even if technical measures of encryption and/or anonymization are in place. The myriad of algorithmic correlations in big data schemes allows for easy identifiability and increasing chances	***Taser wants to build an army of smartphone informants***. *Axon, the world's largest vendor of police-worn body cameras, is moving into the business of capturing video taken by the public. In a survey emailed to law enforcement officials last month, the company formerly known as Taser International solicited naming ideas for its provisionally titled Public Evidence Product.*

	for privacy intrusion which brings this value at risk.	*According to the survey, the product will allow citizens to submit photos or video evidence of "a crime, suspicious activity, or event" to Evidence.com, the company's cloud-based storage platform, to help agencies "in solving a crime or gathering a fuller point of view from the public."* Source: https://theintercept.com/
Dignity	When revealing too much about a user, principles of data minimization in big data appear not to work. Adverse consequences of algorithmic profiling, such as discrimination or stigmatization, also demonstrate that dignity is fragile in big data contexts. Implementing dignity into design and socio-technical practice could minimize detrimental effects of big data.	*The outrage surrounding United Airlines' brutal treatment of a customer has made one thing crystal clear: The story isn't really about airline travel, overbooking policies or even consumer rights. It's about the nature of dignity itself, and it doesn't reflect well on the society it has so preoccupied. The algorithm that decided to bump Dr. David Dao from an overbooked flight was trained to find the "lowest value customer" to inconvenience -- a coach passenger, naturally, not a business traveler, but also a passenger who had paid less than others and wasn't a rewards member.*
Solidarity	Expressing solidarity in daily life, for instance, by taking the courage to come up for others, allows for "the co-flourishing of diverse human societies"[1]. Solidarity, hence, should be kept in discussions on big data. When, for instance, big data-based commercial calculations rank citizens based on their wealth and dominate non-profit interests, solidarity is under pressure.	***The Facebook/Admiral Scandal Shows The Limits And Dangers Of Big Data Capitalism*** *"Insurance company Admiral planned to offer to first time car owners setting their premium based on the analysis of their Facebook data. The basic idea was to observe users' online behaviour in order to assess whether they are conscientious drivers or not. Data to be analysed should have included users' writing style, their likes, or the way they plan meetings. Facebook pulled out of the deal with the insurance company in the last second before the launch." Still the example shows that big data generated in social networking contexts and reused in the insurance context can undermine the value of solidarity and trust.* Source: http://www.huffingtonpost.co.uk/christian-fuchs1/the-facebookadmiral-scand_b_12785994.html
Environmental welfare	Big data has rather indirect effects on the environment; lithium mining for batteries is such. We do not argue for abandoning batteries, but for using batteries with a longer life expectancy. By this, big data technologies would assist in preserving the	***Drones and wildlife – working to co-exist*** *"The drone market is booming and it is changing the way we use airspace, with some unforeseen consequences. The uptake of remotely piloted aircraft (RPAs) has been swift. But despite their obvious benefits, concerns are growing about impacts on wildlife. In our research we investigate whether regulation is keeping pace*

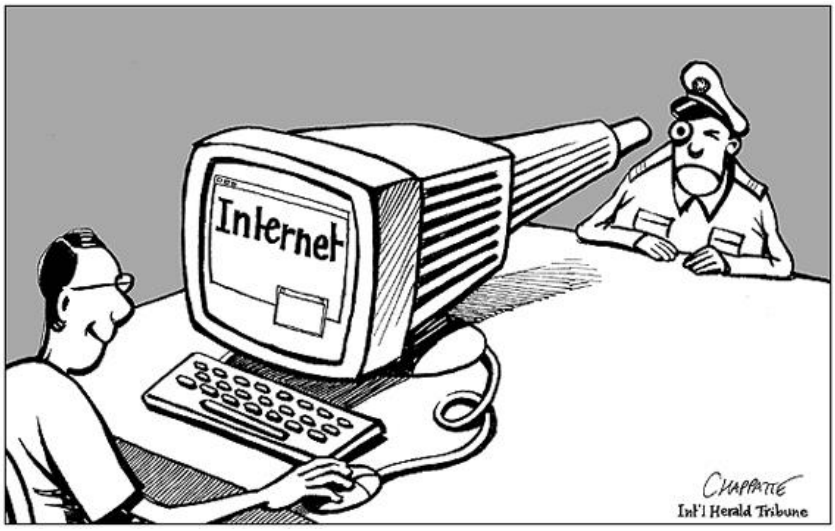
[1] Vallor, S. (2017)

	environment or at least in slowing down its erosion.	*with the speed of technological change. We argue that it doesn't, and we suggest that threatened species might need extra protection to ensure they aren't harmed by drones."* This article suggests that the implications of drones on disturbing the ecosystem and wildlife, including birds and their habitat, are largely underestimated and urgently require legal amendments in order to protect the environment. Source: http://theconversation.com/drones-and-wildlife-working-to-co-exist-83488

3. Legal issues

Big data technologies challenge the human rights architecture from many angles. The fundamental rights singled out as particularly challenged in the context of big data technologies are following:

- Privacy
- Data protection
- Freedom of expression
- Freedom of assembly
- Non-discrimination
- Fair trial and effective remedy
- Consumer protection



These selected fundamental rights, as set forth in the EU Charter of Fundamental Rights and the European Convention on Human Rights, the EU secondary legislation and further specified in the relevant case law, were analyzed in the context of challenges brought about by the big data technologies. As a result, certain common issues emerged. In particular, the legal issues which arise at the nexus between human rights set forth in the EU legal framework and big data technologies could be seen from the perspective of 'within' the legal framework and from 'outside' the legal framework. The former concerns the issues related to the application of different human rights in the context of big data and the latter concerns the issues of the more general character, related to application of the legal framework of human rights as a whole.

List of legal issues	*Analysis of the issues in contexts of big data technologies*	*Real-life examples*
Lack of transparency	Big data technologies are inherently non-transparent as to the specific actors involved, data gathered, and their processing. Transparency, i.e. insight into purposes of data collection, the identity of controller and the kind of personal data processed, not only is intrinsically connected to the right of personal data protection, but also preconditions effective recourse to some other fundamental rights. The lack of transparency in big data technologies is at the core of the challenges involving the chilling effects referred to with respect to the right to privacy and the right to freedom of expression, as it creates the sense of constant fear of surveillance and has an inhibitive impact on individual well-being and autonomy.	*In case of algorithms used for determining the probability of repeated offence which are used in establishing the length of prison sentences or in parole proceedings, the criteria used for such determination are not transparent. The decisions influenced by such algorithmic process have been proved in journalistic investigations to lead to systemic biases; however, it is difficult to establish in an individual case that discrimination has indeed taken place and thus to take recourse of legal measures provided for in the antidiscrimination law.* Source: propublica.com
Vagueness of the concept of harm Lack of individually attributable harm	Due to the fact that big data technology is not a single linear process, but consists of different stages, with different actors involved and with large amounts of data, the harms connected to these processes can have an incremental character difficult to articulate and difficult to attribute to any given stage or actor. In this context, it is very often the case that not specific individuals but rather different groups bearing certain common characteristics are targeted.	*Search results upon a name which might suggest that a person is black show ads which imply criminal a criminal record. While it is difficult to specifically attribute harm of such result to an individual, this exemplifies the situation where racist attitudes are perpetuated in society as a result of data analytics by search engine. Such situation, although clearly harmful to certain segment of society, does not allow for specific legal recourse since such harm is not easy to grasp and pinpoint according to legal criteria.* Source: www.technologyreview.com
Proportionality	The application of this principle and balancing of conflicting rights might be problematic in the case of big data. Application of such technologies might have an immediate appeal and the harm might be postponed, vague and dispersed. Consequently, it would be necessary to coin a list of criteria that may be applicable in cases of such conflicts which would take into account the particularities of big data technologies.	*The algorithms used for preventive policing might be very advantageous for crime preventions; however, such systems might yield biased results, reflecting systemic biases in existing police data bases. Such biases might be difficult to ascertain at the outset while the potential for crime prevention is very promising. Thus, it might be difficult to make sure that the system does not lose its functionality and at the same time takes into account possible adverse outcomes.*

Accountability	The issue of accountability shifts the attention from a rights holder to the duty bearer. The examination of all the selected human rights revealed that big data technologies challenge to a large extent the possibility of holding accountable any single actor taking part in the different stages of big data gathering, processing and decision making. It should be recognized that big data technologies bring about challenges connected with artificial intelligence and self-learning machines and thus ensuring accountability in the context of such automated systems might require entirely novel approaches.	*The example of algorithm which connects searches for names commonly connected to black people, and subsequently suggests the ads implying the criminal record demonstrates how difficult it is to hold any specific actor accountable. Although such algorithm leads to clearly racist outcomes, it is difficult to establish who bears responsibility. As AI might simply reflect the biases in society and concrete outcomes of applying such technology are difficult to foresee at the stage of its design, there is not one single actor that could be held accountable.*
Establishing the adequate regulatory framework	The current legal framework for protection of human rights displays a number of vulnerabilities in the context of big data applications, thus, finding the proper tools for safeguarding values inherent in these human rights becomes a separate issue. Different alternative approaches are suggested in literature for remedying the loopholes in the current system of human rights protection in relation to big data technologies. For example, rather than focussing on the stages of data gathering and decision-making, the central stage of data analytics could become the focal point for ensuring the protection of human rights at risk by introducing an additional duty of care for those processing personal data.	*Facebook provided a possibility for advertisers to identify with its algorithms the teenagers that feel unsecure and worthless. While such solution would not be illegal as such, it can lead to serious abuses of power against the most vulnerable group. Thus, a regulatory framework that would prevent such situation would need to be established. At the same time, it is debatable whether such situation would be tackled best by laws, self-regulation, technical solutions or the combination of those.* Source: www.guardian.com
The role of private actors in the context of human rights framework	The secondary legislation on the right to data protection provides for several provisions which shift the obligation of balancing different fundamental rights and interests on the private actors. With little guidance provided, the question is about the legitimacy of such decisions, especially where obligations of private actors are coupled with the lack of transparency.	*Online platforms are encouraged to take steps to remove certain harmful content and this is done via automated or semi-automated means. Thus, private actors, using algorithms, make decisions on which content is allowed in public sphere and which is not, with possible harmful impact on the right of freedom of expression and access to information, as in case of YouTube making their algorithms for not user-friendly content stricter, with ramifications for independent media outlets.* Source: www.nytimes.com

4. Societal and economic issues

e-SIDES identified a series of issues that emerge with the increasing use of big data technologies. The seven issues that are relevant from a societal and an economic perspective are the following:

1. Unequal access
2. Normalization
3. Discrimination

This group focuses on how actors differ or do not differ and how distinctions are made or not made between actors. While the first issue focuses on different starting positions with respect to big data, the second one addresses the neglecting of individual properties and the third one puts the consideration of individual properties in the centre.

4. Dependency
5. Intrusiveness
6. Non-transparency

They focus on the relationship between data subjects and data processors. The first issue looks at various forms of dependency. The second and the third issue focus on the discrepancy between excessive intrusion into the data subjects' affairs on one side, and limited insight into the data processing on

7. Abusiveness

Given all the other issues relevant in the context of big data technologies, it is not only likely that data is abused in one form or the other but also that, if abuse happens, its impact may be substantial.

The issues are relevant for individuals, groups of individuals and the society as a whole. All issues include societal as well as economic aspects. This underlines the close connection of the societal and the economic perspective. Consequently, no distinction was drawn between societal and economic issues.

	Societal/economic issue	*Description*	*Real-life examples*
How distinctions are made or not made between actors	**Unequal access to data and big data technologies**	Not everybody or every organisation is in the same starting position with respect to big data. Certain skills are needed to find one's way in the data era. Inequalities exist also between companies of different industries, sizes and regional contexts. The ability to exploit the potential of big data is a key competitive advantage. Unequal access results in unequal chances.	***Privacy policies, for instance, are usually long and difficult to understand.*** *The Michigan State University and the University of Connecticut wanted to see how many internet users actually read the notoriously lengthy policies before clicking "agree.", through an experiment with students: researchers found that 74% of participants didn't read the fake website's privacy policy or terms of service. Only 9 of the 543 students noticed that the terms of services include the slightly controversial "child assignment clause".* Source: https://people.howstuffworks.com/the-real-reason-website-app-terms-service-are-confusing.htm
	Normalisation - classification of people and organisations based on data	Deals with the products and services offered to consumers are selected on the basis of comparisons of their preferences and the preferences of others considered similar. As a result, people are put into categories whose characteristics are determined by what is most common. Pressure toward conformity is often the result of normalisation. The breadth of choices is restricted, and pluralism and individuality are pushed back.	***"You Might Also Like:" Privacy Risks of Collaborative Filtering.*** *To help users find items of interest, sites routinely recommend items similar to a given item. For example, product pages on Amazon contain a "Customers Who Bought This Item Also Bought" list. These recommendations are typically public, and they are the product of patterns learned from all users of the system. If customers often purchase both item A and item B, a collaborative filtering system will judge them to be highly similar.* Source: https://freedom-to-tinker.com/2011/05/24/you-might-also-privacy-risks-collaborative-filtering/
	Discrimination	Understood as the unfair treatment of people and organisations based on individual characteristics or belonging to certain larger group. Information about customers and predictions about their behaviour have considerable potential in many sectors. However, the data as well as the algorithms may be incorrect or unreliable. There is a thin line between legitimate customisation of	***When Algorithms Discriminate.*** *Google's online advertising system, for instance, showed an ad for high-income jobs to men much more often than it showed the ad to women, a new study by Carnegie Mellon University researchers found.* Source: https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

		services and illegitimate and unfair discrimination. Discrimination leads to immediate disadvantages and unequal chances.	
relationship between data subjects and data processors	**Dependency**	Focuses on reliance on organisations and technology. It is considered a misconception that people can be self-governing in a digital universe defined by big data. People choosing not to disclose personal information may be denied critical information, social support, convenience or selection. Moreover, people depend on the availability of services provided by companies. Organisations are strongly dependent on the data and the big data technologies they use. Dependency leads to a limitation of flexibility.	***As Dependency on the Digital Universe Grows, It's Also Becoming More Unequal.*** *Human dependency on technology is increasing. At an individual level, devices tell users if they are walking enough, eating too much or sleeping soundly. Many people would be lost without Google Maps, even in cities they call home. Earlier this year, WannaCry and Petya affected hundreds of thousands of people and organisations around the world. WannaCry crippled over 230,000 computers across 150 countries, with the UK's National Health Service, Spain's phone giant Telefónica and Germany's state railways among those hardest hits.* Source: https://thewire.in/197573/internet-big-data-inequality-digital/
	Intrusiveness	Big data has integrated itself into nearly every part of people's online life and to some extent also in their offline experience. People's behaviour is affected by intrusive big data applications. Moreover, protecting privacy is often counterproductive to both companies and customers, as big data is a key to better quality services. Companies and customers need to strike a balance between the use of personal data and privacy concerns.	***As mass data collection becomes the norm, concerns about surveillance are growing.*** *For example, for every case of a smart city bringing enhanced efficiency, there is an equally worrying instance of privacy invasion. Even at this early stage, there have been numerous cases of smart sensors harvesting data without consent. In 2013, retail outlet Nordstrom used smartphone data to monitor customers in 17 stores throughout the US. By tracking Wi-Fi signals, the store was able to measure how long consumers stayed within a particular department.* Source: https://www.theneweconomy.com/business/as-mass-data-collection-becomes-the-norm-concerns-about-surveillance-are-growing
	Non-transparency	Algorithms are often like black boxes: not only opaque but also mostly unregulated and thus perceived as incontestable. People usually cannot be sure who is collecting, processing or sharing	*According to Reuters Institute Digital News Report 2016, 36% of survey respondents were happy with the news automatically selected for them based on what they have read before, 30% were happy for news to be selected for them based on the*

		which data. Moreover, there are limited means to check if a company has taken suitable measures to protect sensitive data. Companies know a lot about their customers but customers are often not aware that this is the case. Additionally, there is a lack of experience with respect to audits including data protection or privacy impact assessments.	*judgement of editors or journalists. In addition, 22% were happy with the news selected based on what their friends had consumed.* *Some big stakeholders are stepping forward and opening up about the use of the algorithms, for instance, Facebook revealed its experiments, where it monitored the effect of the change in the number of negative and positive posts shown to the user. In spite of the criticism received this revelation raised awareness about the role of algorithms and brought to light the need for higher transparency and greater accountability from big internet stakeholders on the use of the algorithms.*
	Abusiveness	Deals with the potential for abuse of data and big data technologies. Even with privacy regulations in place, large-scale collection and storage of personal data is vulnerable to abuses by criminals. Simply anonymised data sets can be easily attacked. The risk of abuse is not limited to unauthorised actors alone but also to an overexpansion of the purposes of data use by authorised actors. Data as well as technologies may be used for illegal purposes or for purposes that fall into a legal grey zone. Abusiveness leads to control loss and mistrust.	***Customer Experience in the Age of Data Breaches.*** *Hacking has become elaborate and the numbers of both ransom and non-ransom attacks are increasing each year: "more than 4,000 ransomware attacks have occurred every day since the beginning of 2016". So, it might as well happen to your company at some point.* Source: http://customerthink.com/customer-experience-in-the-age-of-data-breaches/

5. Conclusive remarks

Conclusion 1:

Although there is some overlap in issues from the different perspectives, this does not mean that the overlapping issues are the same from each perspective – each perspective simply shows different aspects of each issue. Thus, the same challenge brought about the big data can gain different meaning when approached from the different perspective. Thus, when approached from different angles, it is visible that big data technologies trigger changes or pose challenges on many different levels. Hence such comprehensive analysis allows going beyond one narrow domain and rather having a holistic overview of implications of big data technologies. It is also worth noticing that certain issues might transcendent different perspectives with time.

Conclusion 2:

The list of issues identified is very extensive, but not exhaustive. The rapid changes in big data technologies call for periodic updates of identification of issues. Because big data technologies and applications are rapidly changing all the time, no approach can be truly exhaustive. This implies that on the one hand the comprehensive approach taken makes it very likely that the most important issues are actually identified, but on the other hand, this inventory may require periodic updates after some time.

Conclusion 3:

The issues identified are hard to prioritize, as they may be context-dependent and many issues are interconnected. Such prioritization is further complicated by the fact that many issues are interconnected. For instance, when profiling takes place and results in price discrimination, some may consider this a privacy issue regarding data collection (the data should not be collected in the first place), others may consider it an accountability issue (the data processing was not transparent), and yet others may consider it a justice issue (the decision-making is discriminating and, hence, not just or justifiable).

Conclusion 4:

The identified issues should not only or merely be regarded as problems to be solved, but rather as providing the goals to strive for. An attitude of continuous attention is required for these issues. Most or perhaps all of the issues identified are rather complex. Also, they pose challenges that may be hard to solve and it may be hard to determine when they are addressed or solved sufficiently. The issues should, therefore, not be regarded as problems to be solved at once and forever, but rather as goals to keep striving for. An attitude of checking-the-box, whether on legal compliance, data ethics or risk mitigation, is not what is required, as this is perhaps never finished. Rather, an attitude of continuous attention for these issues is called for, including regular updates on the issues themselves.

To know more about e-SIDES:

www.e-sides.eu

To contact us:

info@e-sides.eu

@eSIDES_eu