Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

ACTION GRANTS TO SUPPORT TRAINING ACTIVITIES ON THE DATA PROTECTION REFORM

REC-DATA-2016-01

TAtoDPR – Training Activities to Implement the Data Protection Reform

Project Number 769191

Grant Agreement number 769191 — TAtoDPR — REC-DATA-2016/REC-DATA-2016-01

RELAB Paper

Deliverable No. (use the number indicated on technical annex)	**D1.10**		
Workpackage No.	**WP1**	Workpackage Title	**Management and Coordination of the Project**
Activity No.	**1.3**	Activity Title	**Dissemination and communication management**
Authors (per company, if more than one company provide it together)	**Roberto Montanari, Sara Saleri (RE:Lab)**		
Status (F: final; D: draft; RD: revised draft):	**F**		
File Name:	**TAtoDPR_D1.10_REL_Paper**		
Project start date and duration	**1st November 2017, 24 Months**		
Category	**Technical Area**		

Version History table

DATE	COMMENT
20/10/2019	First draft
29/10/2019	Final version

Table of Content

List of abbreviations

ACRONYM	DESCRIPTION
GDPR	General Data Protection Regulation
DPO	Data Protection Authority
EIoT	Enterprise Internet of Things
IoT	Internet of Things

Executive Summary

As in the short story written by Jorge Louis Borges “The Garden of Forking Paths", the multifaceted combinations between privacy and technological evolution display in front of us a multifaceted landscape, and uncountable set of links among data, technologies and privacy are echoing continuously several alternatives. Moving from this emblematic metaphor of current scenario, this paper intends to overview the strongest implications in terms of privacy induced by raising of big data related technologies, internet of things and blockchain.

Introduction

The present deliverable reports the scientific paper that has been produced by RE:Lab in the context of the TAtoDPR project. This article, together with the others that were produced in the project's framework, is published in the online journal European Journal of Privacy Law & Technologies (EJPLT): http://www.ejplt.tatodpr.eu/

Paper: A garden of forking paths: the several and multifaceted perspectives in the relationship between privacy and technical enablers

Summary: Introduction - 1. Big data huge volume in data spread - 2. Internet of Things: every little thing they do is magic - 3. Blockchain: an in-course disruptive innovation since the Internet itself - Conclusions: challenging regulatory framework and role of DPO

Introduction

In the wide debate on privacy, even wider after the recent introduction of GDPR, the role of the technological enablers is among the “hottest” points. It is of course largely acknowledged how technologies are growing fast since the beginning of the digital age. What is actually and recently impressive is how the technological roadmaps, as well as the improvement in their functional capabilities, are stimulated and fed by the raising of the big data (Mayer-Schönberger, Kenneth Cukier 2013). In brief, the amount of data availability, every given year after 2014, seems to be larger than the amount of data managed by the entire world from the previous year till the beginning of the human history. And this is only one, and may be not the most relevant, of the data revolutionary related aspects.

Therefore, data and technologies are deeply entitled, and it goes without saying how this chain would influences and modify privacy, and of course its regulatory framework. Same happen for others relevant technological players which are changing the game field in privacy. For instance, Internet of Things, i.e. the possibility to address a telematic identity to all things around us, is multiplying possibilities to control everything from everything, to assess what happen in every remote filed of our life, even in space, even among concrete staffs. Blockchain, a revolutionary new way to handle payments and many other financial behaviours, is another big step toward a deeper digitalisation in every part of humans’ life.

The intent of this paper is trying to start in outlining and retracing the wide set of paths in which data, privacy, and technologies are entitled. As in the short story written by the Argentine writer Jorge Louis Borges and titled “The Garden of Forking Paths" ("El jardín de senderos que se bifurcan"), the landscape in front of the multiple combinations among data, technologies and privacy are echoing continuously several alternatives, that are appearing in front of us as soon as we set out among one of the identified path.

The shape in which we have tried to propose such scenario is a literature review to which we have approached following three main criteria. First of all, we have tried to consider trending and emerging topics, with a special focus on new technologies (such as blockchain or user-tracking technologies) which are likely to continue to impact Data Protection in the future; secondly, given the nature of Data protection and the speed of change and evolution, we have given preference to

recent research; thirdly, to maximize the possibility to deepen and disseminate knowledge on the mentioned topics, our research focused mainly on Open Access content[1].

This paper was drafted within the framework of the EU-Funded project "Training Activities to Implement the Data Protection Reform" (TAtoDPR)[2], which was aimed at preparing and training professionals to effectively perform the duties of Data Protection Officers (DPO) as outlined in the General Data Protection Regulation (Regulation 2016/679, known as GDPR).
More specifically, this review is part of the work that RE:Lab has undertaken to structure the Technical, Organizational and Impact Assessment (TOIA) Module of the training courses, which was focused on the technical aspects of data creation, management and storing.

We have identified a series of topics that are central in the current literature and that could also be important for the DPO – the major protagonist of the project to which this paper take the move - and we have decided to focus our review on the three technological domains (briefly introduced above) which are predominant in our hyper-connected society and that have strong implications in terms of data protection, namely Big data, Internet of Things and Blockchain.

1. Big Data: huge volume in data spread

If it is broadly recognized that Volume, Variety and Velocity (the so-called *Three Vs*) are the three main dimensions characterizing Big Data[3] (Laney 2001, Chen, Chiang, Storey 2012), they also represent a challenge in terms of data protection. In a technical perspective, large data sets are particularly problematic in terms of data capturing, storage, analysis (Gandomi, Haier, 2015), transfer, visualization, and of course privacy.
The challenges – together with the opportunities – implied by Big Data are approached by many authors from the company's perspective: Raguseo (2018) investigates the adoption levels of big data technologies in companies, and the big data sources they use; Chluski & Ziora (2015) and Sivarajah et al. (2017) focus on application of big data solutions in the process of organizations' management; Elgendy & Elragal (2016) and Kościelniak & Puto (2015) have a more focused perspective on the role of Big Data in decision-making processes.
Starting from the company's perspective doesn't mean that the individual's side is neglected: the sheer number and dimension of data available also exposes individuals to unprecedented privacy vulnerability, where organizations managing them are unprepared to do so correctly and

[1] The authors would like to sincere thank Andrea Castellano, Francesco Giacomello and Francesco Maria Riccio for their competent contribution to the paper's contents, and Doina Tiganu for her support in the editing.
[2] More precisely the TAtoDPR project has been co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020) under Grant Agreement n. 769191. For more information on the TAtoDPR project see: https://www.tatodpr.eu.
[3] This definition has also been formalized in different kind of glossaries or official documents, such as the Tech America Foundation's Federal Big Data Commission, which states "Big data is a term that describes large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information".

effectively (Yu 2016). In particular, the issue of *profiling* activities is crucial: Big Data also means that companies have the chance to use automated data analysis and filter the amount of gathered data to understand customers and users, research and record their preferences, and gain a vantage point in addressing them commercially. Such practices require special attention, as they might threat privacy when incorrectly performed.

Some studies focus on concrete case studies in contexts where the impact of Big Data on privacy issues cannot be underestimated. Logica and Magdalena (2015) for example, point their attention on the academic realm, in particular on the application of Big Data to e-Learning. The medical, biomedical and healthcare fields, instead, are the main focus of the study by Abouelmehdi et al. (2017): as they point out, while Big Data is being hailed as the key to improving health outcomes, gain valuable insights and lowering costs, the security and privacy issues are so overwhelming that healthcare industry is unable to take full advantage of it with its current resources.

More analytically, a number of investigations focus on how to reduce the risk of breaching the privacy of individuals. Katal et al. (2013) examine the circumstances under which the individuals' privacy might be breached, while Matturdi et al. (2014) introduce the concept of privacy protection in big data.

To better understand the implications of big data in terms of privacy, it can be useful to focus on the different stages of a big data life cycle, as suggested by Mehmood et al. (2016): data generation, data storage, and data processing.

During the first stage – *data generation* –, as underlined also by Xu et al. (2014), the risk of privacy violation can by minimized either restricting access or by falsifying data, for example through tools such as *Socketpuppet*, which conceals individual's activities online by creating a false identity, or *MaskMe*, which alows users to create aliases of their personal information, such as email address or credit card number.

As it concerns the *data storage phase*, the main approaches to preserve the user's privacy in this phase are: Attribute based encryption (Goyal et al. 2006; Bethencourt et al. 2007); Identity based encryption (Boyenand, Waters 2006); Homomorphic encryption (Gentry 2009); Storage path encryption (Hongbing et al. 2015); usage of hybrid clouds (Huang and Du 2014).

The last phase of big data cycle, *privacy protection in data processing*, according to Mehmood et al. (2016), should be analytically divided into two sub-phases.

In the first one, the goal is to safeguard information from unsolicited disclosure because the collected data may contain sensitive information about the data owner. In this case, the main strategy consists in anonymization techniques: generalization, suppression, anotomization, permutation, perturbation (Fung et al. 2010). However, due to the availability of huge volumes of data and powerful data analytic tools, the existing anonymization techniques are becoming increasingly ineffective. Some researches for example indicate that simply anonymized data sets can be easily attacked in terms of privacy. De Montjoye et al. (2013) collected a 15-months mobility dataset of 1.5 million people. After a simple anonymization operation (removing the obvious identifiers, such as name, home address, phone number, and staff ID), they obtained a data set where the location of an individual was specified hourly with a spatial resolution equal to that given by the carrier's antennas. From the processed data set, they were able to identify a

person with 95% accuracy by only four spatial-temporal points. The weakness of simple anonymization was later further confirmed by a similar test (De Montjoye et al. 2015).
Even if the level of anonymization is higher (for example combining different techniques, as suggested by Mehta 2016), another criticism arises in the second moment of data processing, which goal is to extract *meaningful information* from the data without violating the privacy. First of all, how can we extract useful information the overwhelming abundance of data characterizing our era? How can we obtain valuable inputs from anonymized data, without losing information? In order to distinguish relevant data from irrelevant data, analytics comes into play to help organizations select the amount and type of information they require. There are several techniques proposed to analyze large-scale and complex data, which can be broadly grouped into: clustering (Feldman et al. 2013, Shirkhorshidi et al. 2014), classification (Agrawal 2005; Weiping 2006) and association rule-based techniques (Leung et al. 2014).
But selecting the right information does not, on its own, suffice to truly unleash the potential benefits it might produce: visualization is sometimes just as important for the exploitation of data as the analysis behind it.
Information visualization, the art of representing data in a way that is easy to understand and to manipulate, can help us make sense of information and thus make it useful. From business decision-making to simple route navigation, there's a huge (and growing) need for data to be presented so that it delivers value (Kahn 2011). Information visualization plays an important role in making data digestible and turning raw information into actionable insights. It draws from the fields of human-computer interaction, visual design, computer science, and cognitive science, among others. Examples include world map-style representations, line graphs, and 3-D virtual building or town plan designs.
Visualization methods are considered to be very important for the users' because they provide mental models of the information (North 2017). Visualization techniques make huge and complex information intelligible and serve as a visual user interface to provides insight of information to the user (Spence 2001). According to Ware (2004), the basic purpose of visualization is to create interactive visual representations of the information that exploit human's perceptual and cognitive capabilities of problem solving. In order to meet the requirement of maintaining a low workload for the user and increase the information effectiveness, generic guidelines (Carr 1999) on info-view suggest to: work on Hierarchical representation of information; minimize the use of 3-dimensional representations; coordinate multiple views; allow an interactive navigation of the data; use them to support the user task.
Visualization techniques, thus, can enhance informed decision-making and data-driven strategies within public and private organizations. In this perspective, Data is not only seen as an individual's resource in need of protection, but also as a collective good, whose conscious exploitation can lead to better decision and policy-making, thus reverberating positive effects on end-users as well.

2. Internet of Things: every little thing they do is magic

One of the greatest present and future challenges to Data Protection is posed by the so-called Internet of Things (IoT). Expanding digitalization of objects and places, accompanied by the transfer of an enormous volume of data, put into question the effectiveness of existing measures for the protection of personal data, while demanding organizations involved to pay greater attention to Data Protection than ever before.

According to the review undertaken by Perera et al. (2015), this challenge is clearly perceived by the users, who are becoming increasingly aware and concerned of possible threats to privacy implied by the pervasive IoT. TRUSTe (2015) even highlighted the fact that privacy concerns could be a significant barrier to the growth of IoT. According to a survey they conducted, about 60% of internet users have basic privacy awareness of IoT and they know that smart devices, such as smart TVs, fitness devices, and in-car navigation systems could collect personal activities data. The survey also revealed that 87% of internet users were concerned about the type of personal information collected.

Thus, in this scenario, the satisfaction of security and privacy requirements plays a fundamental role. According to Sicari et al. (2015), such requirements include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arises scalability issues; therefore, a flexible infrastructure is needed able to deal with security threats in such a dynamic environment.

To tackle this issue, researchers have been focusing on various approaches enforcing security and privacy. Sahmim et al. (2017), in their review, present several techniques, such as encryption, obfuscation, anonymization, the so-called “Sticky policy” (which allows to attach privacy policies to data owners and drive access control decisions and policy enforcement), data segmentation.

Malina et al. (2016) go more in depth, presenting a detailed assessment of the performance of the most used cryptographic algorithms on constrained devices that often appear in IoT networks. In particular, they evaluate the performance of symmetric primitives, such as block ciphers, hash functions, random number generators, asymmetric primitives, such as digital signature schemes, and privacy-enhancing schemes on various microcontrollers, smart-cards and mobile devices. Furthermore, they provide the analysis of the usability of upcoming schemes, such as the homomorphic encryption schemes, group signatures and attribute-based schemes.

On the other hand, other researchers, such as Thierer (2013), advocate for a regulation that do not jeopardize the innovation potential of this technology, while Weinberg et al. (2015) explore one of the central tensions of the IoT, i.e. convenience vs. privacy and secrecy.

The IoT environment is likely to exponentially grow in the future, thus widening the scope of Data Protection concerns related to it. In particular, clearer measures for user’s consent to data treatment and data management policies must adapt to such an evolving context. Furthermore, cybersecurity issues connected with IoT in sensitive domains, such as smart grids, healthcare (Zang et al. 2013), transportation or domotics pose urgent challenges in terms of governance.

Also, EIoT (Enterprise Internet of Things) demands for increased awareness from managers as to the level of protection assigned to data. As highlighted by Dzung et al. (2005), in the past, systematic integration of countermeasures against cyberattacks often followed integration of IT components with some delay. As a result, current Industrial IoT systems are vulnerable to a variety of cyberattacks. To counter these security and privacy risks, affirm Sadeghi et al. (2015), holistic cybersecurity concept for Industrial IoT systems is required, that addresses the various security and privacy risks at all abstraction levels. This includes different aspects, such as platform security, secure engineering, security management, identity management, industrial rights management.

3. Blockchain: an in-course disruptive innovation since the Internet itself

Since its emergence in 2008, Blockchain technology has seen a sharp increase in popularity and use. Its innovative nature has led many observers to consider it as the most disruptive invention since the Internet itself. Its potential is undoubtedly enormous, whether already exploited or not, and likely to have great implications for Data Management and Protection. Moreover, even though its most popular example, the Bitcoin currency, might be regarded as highly controversial, the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world, as pointed out by Crosby et al. (2016). In practice, this technology consists in creating a continuously growing list of ordered records, which are called blocks, to form a digital ledger. Its peculiarity is the fact that this list is widely distributed within a peer-to-peer network, which automatically validates each new record.

Authors such as Huckle et al. (2016) and Banerjee et al. (2017) posit the potential for blockchain technology in facilitating secure sharing of IoT datasets (e.g. using blockchain to ensure the integrity of shared datasets) and securing either civilian or military IoT systems. Starting from similar considerations, Ouaddah et al. (2017) propose FairAccess as a new decentralized pseudonymous and privacy preserving authorization management framework that leverages the consistency of blockchain technology to manage access control on behalf of constrained devices. Indeed, access control is currently facing big challenges in the IoT world, since it is quite hard to implement current access control standards on smart objects due to their constrained nature. Here the blockchain technology might come to rescue, allowing for a reliable third party access handling.

Similarly, Angraal et al. (2017) describe the possible use of the blockchain in the health-care sector, precisely because, offering a secure, distributed database that can operate without a central authority or administrator, it can provide a platform to improve the authenticity and transparency of healthcare data through many use cases, from maintaining permissions in electronic health records (EHR) to streamlining claims processing.

It is very important to notice how in all of the previous examples a fundamental role is played by the decentralization of the processes. This is because entitling a single institution to control a data flow corresponds inevitably to a security issue. On the other hand, blockchain allows for an egalitarian networking system which relies on the users' community itself, since it becomes harder and harder to violate its mechanism the more copies of blockchain are distributed. Hence one

could say that the power of this technology actually comes from the fact that it evades any possibility of a centralized management.
On this matter, we are due to notice the perspective of Scott (2016), who rises potential points of concerns such as the tech-from-above "solutionism" and conservative libertarian political dynamics of some of the technology start-up community that surrounds Bitcoin. The author considers "blockchain 2.0" technologies with more overtly communitarian ideals and their potential for creating "cooperation at scale". Again, this might provide us some remarkable insights, since this principle of cooperation is not just about ideals but could be crucial in order to manage security hazards.
Moreover, authors such as S. Raval and O'Reilly (2016) state that decentralized applications (dapps) will become even more widely used than today's most popular web apps. Dapps are just applications that are executed on a peer-to-peer network, and thus existed well before the blockchain. However, it is argued how, implementing them with a blockchain mechanism, they will provide a more flexible, better-incentivized structure than current software models. As an example of a dapp exosystem, the authors describe the OpenBazaar decentralized market, and examine two case studies of dapps currently in use. Indeed, Huckle et al. (2016) discuss how the IoT and blockchain technology can benefit shared economy applications, overtaking current shared economy applications such as Airbnb and Uber by creating a myriad of sharing applications, e.g. peer-to-peer automatic payment mechanisms, foreign exchange platforms, digital rights management and cultural heritage.
In the future, Data Protection Officers will be called to assess their compliance with existing national and international regulations: in this sense, they will have to consider the rising of new technologies such as that of blockchain-based Smart Contracts, which allow to enforce contracts remotely in a more trustable way. In conclusion, it should be kept in mind that, as with any new technology, the blockchain has to be considered with a critical attitude, even though it should be by construction a mechanism which guarantees a high level of dependability.

Conclusions: challenging regulatory framework and role of DPO

In the end, it appears clear how the metaphor chosen in the beginning of this paper looks relevant in understanding the current landscape where big data, IoT and Blockchain are not only influencing each other, and together are depicting a new frame for privacy, but as in the garden of forking paths, they are shaping every alternative, every possibility, in a kind of uncountable alternative producing mechanism.
These continuous transformations put in front of the DPOs and the regulators new challenges. The first have to cope in their daily work with these transformations, especially in trying to quickly understand which is the expect impact in organizations, data management and foreseeable risk for privacy and rules. The latter have to quickly understand what is happening around, which technologies are emerging and what of these technologies is concretely impacting on people and originations life. Of course, these challenges are enormous and require a wide view and quick capabilities to understand. In this paper, we have briefly outlined some technological players which are mature and relevant, but many other urgently require attention. Just one among the

others: the role of Artificial Intelligent (AI), which is becoming to appear as a quite mature enabler. AI is hugely relevant in our scenario, another path full of forking paths, and it goes without saying that it could affect all the above-mentioned enablers, introducing a deeper level of autonomy and behavioral independence. DPO and regulators – from their different perspective – have to be tuned, even changing their interpretation framework in understanding transformations which are not only influencing privacy and data management but even more transforming intimately the nature of privacy and data management.

References

K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, M. Saadi, *Big data security and privacy in healthcare: A Review* (EUSPN 2017)

S. Angraal, H. M. Krumholz, Wade L. Schulz, *Blockchain Technology Applications in Health Care,* (Circulation: Cardiovascular Quality and Outcomes, 2017)

S. Agrawal and J. R. Haritsa, *A framework for high-accuracy privacy- preserving mining* (Proc. 21st Int. Conf. Data Eng., Apr. 2005, pp. 193–204)

M. Banerjee, J. Lee, Kim-Kwang R. Choo, *A blockchain future to Internet of Things security: A position paper,* (Digital Communications and Networks, 2017)

J. Bethencourt, A. Sahai, and B. Waters, *Ciphertext-policy attribute- based encryption*, (Proc. IEEE Int. Conf. Secur. Privacy, May 2007, pp. 321–33)

X. Boyenand B. Waters*, Anonymous hierarchical identity-based encryption -without random oracles* (Proc. Adv. Cryptol. (ASIACRYPT), vol. 4117. Aug. 2006, pp. 290–307)

D. A., Carr, *Guidelines for Designing Information Visualization Applications*, 1999.

H. Chen, R. H. L. Chiang and V. C. Storey, *Business Intelligence and Analytics: From Big Data to Big Impact* (MIS Quarterly, Vol. 36, No. 4 (December 2012), pp. 1165-1188)

A. Chluski, L. Ziora, *The role of big data solutions in the Management of organizations. Review of selected practical examples* (*Procedia Computer Science, Vol. 65*, 2015)

M. Crosby, Nachiappan, P. Pattanayak, S. Verma, V. Kalyanaraman, *BlockChain Technology: Beyond Bitcoin* (Applied Innovation Review, Issue 2, June 2016)

A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, *Unique in the crowd: The privacy bounds of human mobility* (Sci. Rep., vol. 3, Mar. 2013, Art. no. 1376)

A. de Montjoye, L. Radaelli, V. K. Singh, and A. Pentland, *Unique in the shopping mall: On the reidentiability of credit card metadata* (Science, vol. 347, no. 6221, pp. 536-539, 2015)

D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin, *Security for industrial communication systems* (Proceedings of the IEEE, 93(6), 2005)

D. Feldman, M. Schmidt, and C. Sohler*, Turning big data into tiny data: Constant-size core sets for k-means, PCA and projective clustering* (Proc. ACM-SIAM Symp. Discrete Algorithms, 2013, pp. 1434–145)

B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, *Privacy-preserving data publishing: A survey of recent developments* (ACM Comput. Surv., vol. 42, no. 4, Jun. 2010, Art. no. 14)

A. Gandomi, M. Haier, *Beyond the hype: Big data concepts, methods, and analytics* (International Journal of Information Management, Vol. 35, Issue 2, April 2015)

C. Gentry, *A fully homomorphic encryption scheme* (Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009)

V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute-based encryption for fine-grained access control of encrypted data* (Proc. ACM Conf. Comput. Commun. Secur., Oct. 2006, pp. 89–98)

C. Hongbing, R. Chunming, H. Kai, W. Weihong, and L. Yanyan, *Secure big data storage and sharing scheme for cloud tenants* (China Commun., vol. 12, no. 6, pp. 106–115, Jun. 2015)

X. Huang and X. Du, *Achieving big data privacy via hybrid cloud* (Proc. Int. Conf. INFOCOM, Apr. 2014, pp. 512–517)

S. Huckle, R. Bhattacharya, M. White, N. Beloff, *Internet of Things, Blockchain and Shared Economy Applications*, (Proceedings of the International Workshop on Data Mining in IoT Systems (DAMIS), 2016)

M. Kahn, *Data and Information Visualization Methods, and Interactive Mechanisms: A Survey* (International Journal of Computer Applications, 2011)

K. Kang Z. Pang, C. Wang, *Security and privacy mechanism for health internet of things* (The Journal of China Universities of Posts and Telecommunications, Volume 20, Supplement 2, December 2013, Pages 64-68)

Katal, M. Wazid, and R. H. Goudar, *Big data: Issues, challenges, tools and good practices* (Proc. IEEE Int. Conf. Contemp. Comput., Aug. 2013, pp. 404-409)

D. Laney, *3-D data management: Controlling data volume, velocity and variety. Application Delivery Strategies by META Group Inc.* Retrieved from https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (2001, February 6)

B. Logica, R. Magdalena, *Using Big Data in the Academic Environment* (Procedia Economics and Finance, Vol. 33, 2015)

C. K.-S. Leung, R. K. MacKinnon, and F. Jiang, *Reducing the search space for big data mining for interesting patterns from uncertain data* (Proc. Int. Conf. Big Data, Jun./Jul. 2014, pp. 315–322)

L. Malina, J. Hajny, R. Fujdiak, J. Hosek, *On perspective of security and privacy-preserving solutions in the internet of things* (Computer Networks, Volume 102, June 2016)

B. Matturdi, X. Zhou, S. Li, and F. Lin, *Big data security and privacy: A review* (China Commun., vol. 11, no. 14, pp. 135145, Apr. 2014)

A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, S. Guo, *Protection of Big Data Privacy* (Special Section: Theoretical Foundations for Big Data Applications: Challenges and Opportunities, IEEE Access, Vol. 4, 2016)

B. B. Mehta, U. P. Rao, *Privacy Preserving Unstructured Big Data Analytics: Issues and Challenges* (Procedia Computer Science, Vol. 78, 2016)

C. North, *Information Visualization* (Center for Human-Computer Interaction, Department of Computer Science Virginia Polytechnic Institute and State University Blacksburg, VA 24061 USA, 2017)

A. Ouaddah, Anas A. Elkalam, A. Ait Ouahman, *Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT,* (Europe and MENA Cooperation Advances in Information and Communication Technologies, 2017)

C. Perera, R. Ranjan, L. Wang, S. U. Khan, A. Y. Zomaya, *Privacy of Big Data in the Internet of Things Era* (IT Professional, Vol. 17, Issue 3, May-June 2015)

E. Raguseo, *Big data technologies: An empirical investigation on their adoption, benefits and risks for companies* (International Journal of Information Management, Vol. 38, Issue 1, 2018)

S. Raval, O'Reilly, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology,* **(**Media, 2016)

A. R. Sadeghi, C. Wachsmann, M. Waidner, *Security and Privacy Challenges in Industrial Internet of Things* (DAC '15 Proceedings of the 52nd Annual Design Automation Conference, Article No. 54, June 2015)

S. Sahmim, H. Gharsellaouib, *Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review* (Proceedings of the International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017, 6-8 September 2017)

B. Scott, *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?,* (prepared for the UNRISD Workshop Social and Solidarity Finance: Tensions, Opportunities and Transformative Potential" in collaboration with the Friedrich-Ebert Stiftung and the International Labour Office, Feb 2016)

A. S. Shirkhorshidi, S. R. Aghabozorgi, Y. W. Teh, and T. Herawan, *Big data clustering: A review* (Proc. Int. Conf. Comput. Sci. Appl., 2014, pp. 707–720)

S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, *Security, privacy and trust in Internet of Things: The road ahead* (Computer Networks, Vol 76, January 2015)

R. Spence, R, *Information Visualization* (Addison-Wesley 2001)

TechAmerica Foundation's Federal Big Data Commission*, Demystifying big data: A practical guide to transforming the business of Government*. Retrieved from www.techamerica.org/Docs/fileManager.cfm?f=techamerica-bigdatareport-final.pdf (2012)

A. D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation* (Richmond Journal of Law and Technology, Vol. 21, Issue 2, 2013)

TRUSTe, *Internet of Things Industry Brings Data Explosion, but Growth Could be Impacted by Consumer Privacy Concerns* (TRUSTe Research, 29 05 2014. [Online]). Available: http://www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion- but-growth-could-be-impacted-by-consumer-privacy-concerns/

C. Ware, *Information Visualization: Perception for Design* (Morgan Kaufmann C 2004)

B. D. Weinberg, G. R. Milne, Y. G. Andonova, F. M. Hajjat, *Internet of Things: Convenience vs. privacy and secrecy* (Business Horizons, Vol. 58, Issue 6, November–December 2015)

G. Weiping, W. Wei, and Z. Haofeng, *Privacy preserving classification mining* (J. Comput. Res. Develop., vol. 43, no. 1, pp. 39–45, 2006)

S. Yu, *Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data* (IEEE Access, Vol. 4, 2016)

C. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, *Information security in bigdata: Privacy and data mining* (IEEE Access, vol. 2, pp. 1149-1176, Oct. 2014)