Legal Information Management, 22 (2022), pp. 166–174
© The Author(s), 2022. Published by British and Irish Association of Law Librarians doi:10.1017/S1472669622000317

An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies

Abstract: New emergent technologies, like cloud computing, blockchain, the 'internet of things', and artificial intelligence (AI), have received significant attention from research and industry. Public and private organisations benefit from these technologies, but the privacy of individuals is threatened. This research paper, by Varda Mone and CLV Sivakumar, analyses the existing data protection laws with respect to new emerging technologies like AI, big data, and algorithms. The purpose is first, to discuss and analyse the impact and emergence of modern concepts like big data, algorithms and artificial intelligence (AI), Cloud computing, and the 'internet of things', etc mainly in light of GDPR (General Data Protection Regulation) provisions. The article examines the challenges of GDPR compliance posed by the features of these technologies, both individually and collectively. Due to the unique features of these technologies, we are able to identify areas of compliance that needed attention. With regard to the compliance issues identified, we discuss possible solutions as well as raise new questions for further investigation. It is not an exhaustive assessment of these fields but an attempt is made to shed light on a few of them from a data protection perspective.

Keywords: data protection; privacy; GDPR; technology; big data; artificial intelligence; AI

1. INTRODUCTION

The new and contemporary technological advancements and breakthroughs of computers and the Internet have increased the chances of privacy invasion and created an environment in which it is inexpensive and simple to access an ever-expanding pool of personal information about identifiable individuals anywhere in the cyber universe. Not only is it possible to target market products and services with the data collected, but web businesses can also sell advertising space on their websites based on this information.[1] This personal data recorded by government agencies, credit card companies, and telephone service providers can be misappropriated, leaving individuals vulnerable to the whims of predators. Several important trends contribute to breaches of privacy like globalization and the development of the Internet, which has removed geographical limitations to the flow of data. Modern-day social and commercial transactions necessarily require sharing of information. All social networking, mobile applications, and e-commerce platforms run on the sole minimum procedure of sharing some personal or sensitive information.

Researchers have long agreed that technological advances are accelerating at a rate that legal frameworks cannot keep up with.[2] Emerging technology such as cloud computing (CC), blockchain (BC), the Internet of Things (IoT), and artificial intelligence (AI) all have one thing in common: an openness that allows them to be incredibly innovative.[3] Organizations and societies see this openness as a driver of innovation in our interconnected world. Each new technology offers appealing advantages. CC provides scalable distributed Information Technology (IT) resources and skills while lowering capital expenditures.[4] The world is witnessing a phase where data transfer and sharing of information is rampant in all forms of communications and transactions. These modern-day systems of transactions and communications are not only restricted to sharing information which is general and has no legal ramifications or individual's privacy at stake. Changing contours of data transfers and transactions have many legal and related implications. Since the nature of information being shared and transferred may be very sensitive, such as medical information, banking information, biometric information, defence-related information, etc. between the transferor and transferee, the transfer/sharing of such information may warrant big legal implications. The implications of such sharing in modern applications and communications are unknown for multifarious reasons.[5]

This article analyses the issues pertaining to data protection in the onset of new emerging technologies. For this purpose, a precise case study of modern concepts like big data, algorithms and artificial intelligence (AI), Cloud computing, and the Internet of Things has been made to understand how they can be used to reap profit causing breaches of data privacy and to find out the inadequacy of existing legal framework to protect such cases. Therefore, the article explores the following research questions: What impact will GDPR (the General Data Protection Regulation) have on new emerging technologies? Also, do GDPR criteria aid in the prevention of data misuse? If not, what should be done to eliminate the ill use of accumulated data by data companies?

2. METHOD

The method used to do research on this paper is entirely based on secondary sources of data analysis. Various law books, articles, and other primary and secondary sources have been used to get the data. These include legislation, treaties, conventions, and reports from different groups. It is only a study of interpretation and analysis.

3. IMPACT OF GDPR ON EMERGING TECHNOLOGIES

In today's digital economy, there has been a complete change in how businesses connect their operations. Businesses can gain an advantage over their competitors by predicting what people will need to make decisions about what goods and services they want to buy. GDPR applies to all organisations, whether based inside or outside the EU, that offer goods and services to EU citizens.[6] GDPR also applies to all organisations that process the personal data of EU data subjects, regardless of where they offer products or services to them or whether the processing is manual or automated.[7]

Data analytics processes have had a significant impact on the operational activities of a business, such as integrated supply chain management mechanisms that connect multiple departments and business domains, including warehouses, transportation and suppliers and retailers. Protecting data that is collected from different sources using digital technologies is proven to be safe under the EU GDPR, which was put into place a reasonable amount of time ago. A company's opportunities can only be fully realized if it has accurate and timely information from new emerging technologies like big data analytics, artificial intelligence applications as well as cloud computing software and virtual/augmented reality devices. 'Data analytics' also helps in business operational tasks such as supply chain management systems which also include warehouses, transportation, suppliers, retailers, and other organizations.

Commercial and government organizations around the world are confronted with a variety of opportunities and challenges when it comes to safeguarding and preserving personal data as it may have a destructive impact if fallen into wrong hands.

'Data is the new oil[8]' and with oil comes catastrophe and convenience[9]. New emerging technologies (such as big data, AI, social media etc.) can be lethal and non-lethal at the same time depending on their usage. The rise of big data, the Internet of Things, and algorithmic decision-making, artificial intelligence[10], social media advertisements has a big impact on the notice and consent model.[11] Furthermore, state authorities undertaking mass surveillance activities, such as project Aadhaar, may make use of these technologies and cause a significant impact on the rights of individuals.

In the modern era, privacy is threatened by the power of private actors, and the need to ensure that every personal information handling recognises fundamental rights requirements has become extremely relevant. Furthermore, we have seen encouraging rates of websites (e.g., social media platforms) publishing privacy policies, and that's where the story of success ends.[12] All of the internet's free sites and services are funded by the collection of personal information, the mining of that data and targeted advertising. It is also increasingly easy to follow people online, cookies and other electronic identifiers, as well as the traceability of IP addresses, make it difficult to conduct activities online anonymously.

From a broader perspective, the GDPR framework aims to safeguard user information collected by internet technologies and protect legal rights for consumers and individual personnel. The following are some of the key areas of new emerging technologies where the General Data Protection Regulation will have a significant impression in the near future. The key to advancement by a lot of businesses will be to use data that has been gathered over time to deal with rising financial markets. The European Union's GDPR is about how to get, analyse, and store a huge chunk of information in the form of data from people. It also protects the people, ensuring them the right to be explained on the personal information used by digital gadgets.

3.1 BIG DATA

The term big data commonly encompasses *'the growing technological ability to collect, process and extract new and predictive knowledge from the great volume, velocity, and variety of data.'*[13] One of the most effective approaches for obtaining and analysing actual-time data through different AI technology and sensors is big data analytics. Organizations spend a lot of money to integrate big data analytics into their day-to-day operations.

The concept encompasses both the data and the data analytics. They collect personal data of the public, sensors and machines that collect data like weather and satellite images, digital pictures and videos, GPS signals or

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press

IP addresses, and so on. The collected data can be used for many other purposes other than the primary purpose, such as to provide consumers with customised services. These technological innovations make it possible to structure, process and evaluate masses of data[14] giving outcomes that would be unobtainable on a lower scale. Europe's economic growth, innovation, and digitization could be sparked by it.[15] Though it may offer new opportunities for new social, economic or scientific insights, the chances of testing and handling big data in a specific way has opened up new avenues for consumer-centric advertising and profiling.[16]

Moreover, the machine learning algorithm systems that convert data into information are not perfect; they rely on imperfect input variables, reasoning, plausibility, and the people who design them.[17] Big data has also changed the way political audiences are viewed. A common belief is that big data facilitates new ways of securing political affiliation through algorithmic clustering.[18] Further, many arguments about big data tend to focus on government surveillance and the Orwellian world of surveillance either through the internet or via mobile phone tapping.[19]

Analysis

- AI algorithms and big data don't go together. Article 5 (1) b. ML algorithms may use personal data for unclear or illegal reasons and create new data, which makes it hard for data subjects to know what will be done with all of this information.
- ML algorithms and big data don't follow Article 5 (1)c. ML algorithms tend to collect and repurpose a lot of personal data, which makes it hard for data subjects to know if all of these data are adequate and relevant for the purpose they are processed for.
- Article 4 (11) isn't followed by ML algorithms and big data. Processing and reusing large amounts of personal data makes it hard to get informed consent based on a statement or a clear affirmative action.

3.2 ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence applications are used by many businesses and organisations to increase the quality of and even outperform human abilities, such as understanding, learning, and interacting with people and machines, among other things.[20] Technology and software use algorithms to automate choice by emulating the process of human decision-making. As a method of calculation, data processing, evaluation, and automated reasoning and decision-making, an algorithm fits the bill nicely.

The GDPR emphasizes allowing individuals to access personal data, own and control it, and make changes to it as they see fit. Data such as a person's age and gender are among the sensitive information that is collected by a large number of organisations. Apps on digital devices used by individuals can track personal data, according to a number of studies.

AI requires the collection and processing of a lot of data for things like targeting and profiling, for example. This is a process that may be automated and make decisions based on predefined patterns or factors. Asked by the Commerce and Judiciary Committees of the US Senate, Mark Zuckerberg said that "AI tools" are important to any plan to fight hate speech, fake news, and manipulations that use data ecosystems to target people.[21]

As a result, many people are reluctant to share personal information, fearing that misused data could negatively impact both society and the organisation. GDPR regulations ensure that necessary precautionary measures are to prevent the adverse consequences and the effective continuance of AI applications and their actions targeting consumer data collection in order to improve consumer experience and provide satisfying performance.

Analysis

- Article 5 (2) of GDPR does not allow AI systems to be autonomous. It makes it hard to hold AI systems accountable for the harm they may cause to the data subject.
- Automation and machine learning algorithms do not follow Articles 13(2)f, 14(2)g, 15(1)h, or 22. (1). It makes it hard to explain the complicated ML algorithm logic that is used to process personal data, which hurts fairness and transparency. So, the people whose information is being used can't opt-out of automated decisions and profiling because they don't know what will happen to them if they do.

3.3 INTERNET OF THINGS (IoT)

The Internet of Things (IoT) is a term used in the information technology industry to describe devices that communicate with each other via the internet. Personal data such as name, online data, gender, physical location, IP addresses, age, and so on are accessed by IoT devices. IoT also known as the Internet of Everything, is a rapidly increasing supply of electronics and devices from which information can be accumulated.[22] It has two categories, namely 'Information and Analysis' and 'Automation and Control.'[23] The 'Fitbit', a device that tracks behaviour, is the most well-known example of an IoT. It is best known for its wristband fitness trackers, which allow users to track foot-steps, various categories of workouts, total calories, and other health information.[24] IoT can help organisations and countries in many ways, such as by increasing productivity, improving quality of life, automating processes, personalising services, creating apps that work best in certain situations, and generating rich data in real-time.[25] But there are big problems that make it hard to

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press

live up to these values, such as privacy, security attacks, lack of interoperability because devices are different, immature technology for storing and processing huge amounts of data, and weak regulatory frameworks.[26]

The biggest problems between IoT and GDPR are transparency, consent, privacy, discrimination, and complicated contracts (see Analysis). IoT is characterised by the use of identification technologies to constantly link data from people's devices to their unique identities and to link data between devices and services to give them personalised services.[27]

Analysis:

- Constant identification, data linkage, IoT devices, and multiple stakeholders breach Articles 12 (1), 13, 14 (1–4), 4 (11), and 6(1) a. Data subjects may not be aware of IoT devices' constant identification, data linkage, data collection and sharing, and data processing by IoT devices and many stakeholders. This makes it difficult for controllers to inform data subjects of their collection and processing. Thus, data subjects may not give informed consent for data processing.
- Article 5 (1)c and Article 5 (1)b are not followed when third parties collect too much information or change the reason for processing. They may collect more than is necessary personal information about people and how they act. Controllers and third parties can use the huge amounts of personal data they've collected for reasons other than what they were collected for, and the data subjects may not even know it.
- IoT devices that are connected to the internet, big data analytics and algorithms, and complicated, multilayered contracts between IoT stakeholders don't abide by GDPR's Article 28(3) and Article 5(2). In reality, the processors are the ones who write up the terms of the contract and the instructions for processing. This makes the controller responsible for giving the processor the instructions for processing instead of the other way around. This could also make it hard for the controller to show accountability, since the standard contracts of the processors and their sub processors may not be as detailed as GDPR requires. It also gets harder to show who is responsible for the harm done to the people whose data is being used by IoT devices or big data analytics and algorithms.

3.4 CLOUD COMPUTING & DATA MINING

Internet-connected devices' ability to show stored data on web servers instead of on the device itself is known as cloud computing.[28] It allows for tremendous storage and processing capabilities at a relatively low cost. Importantly, because the bulk of the processing is done by remote servers, it increases the capabilities of less powerful devices such as mobile phones. The protection of data collected in the cloud is generally governed by the privacy policies and terms of service agreements of cloud service providers. From a privacy perspective, however, several challenges remain.[29] Many companies offering cloud computing services have failed to build in security features such as encryption technologies. It can also be challenging to maintain control of data in the cloud.

With a revolution in information technology, datamining is a growing field that is used for everything from consumer research, fraud identification, and client retention to manufacturing control and scientific exploration, there's something for everyone.[30]

GDPR can not ask for permission for every single thing that the devices do. If there were a lot of people doing a lot of networking, it would be very hard to keep track of everything they did. It is a requirement under the General Data Protection Regulation for all organisations to track the individual's personal data they collects at all times, as well as keep an eye on who has access to the data and what permissions they have to use it. This way, no one can use personal data without permission. There has been more emphasis on protecting and maintaining a privacy channel to make sure that personal data is safe and not at risk. GDPR's rules about protecting people's personal information are quickly growing as more and more devices and technology are being used by people. However, there are a lot of problems when it comes to protecting and getting permission for people to get their personal information.

Analysis:

- The virtual cloud environment doesn't meet the requirements of Article 33 (1), (2), and (3) Article 5(1)f because attackers can use flaws in the hypervisor to gain access to the cloud environment and delete or change personal data or settings of virtual computing resources. They can also delete all traces of their intrusion, which creates a problem for cloud forensics. This means that when the processor (i.e., CSP) finds out about a personal data breach, it can't tell the controller right away. So, the controller (i.e., the customer organisation) might not be able to tell the supervisory authority about the personal data breach and give details about it within 72 hours of finding out about it and without too much delay. So, it's possible that the controller can't follow the "integrity and confidentiality" principle.
- Article 28 (1), (3)a, and (4), as well as Article 5(1)a, Recital 39, are not met by simple and standard CSP contracts. Due to the large number of tenants, the

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press

SLAs are not the same as the actual levels. As a result, CSPs and their subcontractors tend to offer simple, standard agreements that are less clear about the complexity of the hardware in the cloud infrastructure and about where and how personal data is stored and processed. This is not in line with GDPR because it doesn't give enough guarantees to put in place the right technical and organisational measures to protect the rights of data subjects. It makes it hard to meet the contractual requirements of GDPR, which say that the CSP and its subcontractors must process personal data based on what the controller tells them to do in writing. So, the controller might not be able to show that the personal data was processed in a transparent way, as required by GDPR's "lawfulness, fairness, and transparency" principle.

- Articles 7(2) and 17(1) do not allow for CC backups that are spread out in different places. It is not clear where the backup copies of personal data that have been shared are, which makes it hard to get the data subject's clear consent. It also makes it hard to guarantee the right to be forgotten and make sure that all backup copies are deleted.

4. DATA PROTECTION-RELATED ISSUES UNDER GDPR

The use of big data and artificial intelligence raises a number of questions regarding the identification of controllers and processors, as well as their liability. The General Data Protection Regulation (GDPR) establishes a legal regime for the liability of data controllers and processors. When artificial intelligence and algorithms are considered products, it raises questions about the distinction between individual liability, which is governed by the General Data Protection Regulation, and product liability, which is not governed by the GDPR.[31]

The essence, evaluation, and application of big data call into question the application of some of the most fundamental principles of the GDPR, such as the principles of lawfulness, data minimization, purpose limitation, accuracy, and transparency. The business model of big data may be the polar opposite of data minimization, as it necessitates the collection of ever-increasing amounts of data for unspecified purposes.

The complexity of big data analytics, as well as the lack of transparency surrounding it, may necessitate a rethinking of ideas about individual control over personal data. Profiling and targeted advertising may not necessarily be a problem if people are aware that they are being targeted with advertisements that are tailored to them. Personality profiling becomes a problem when it is used to manipulate individuals, such as when it is used to look for specific personalities or groups of people for political campaigning purposes.

5. HOW EFFECTIVE ARE GDPR PARAMETERS IN REDUCING THE ABUSE OF ACCUMULATED DATA?

GDPR is founded on a body of rules that organisations must adhere to as they conduct business operations. They are distinct from the company's fundamental rules and regulations, which over time tend to become obsolete and inconsistent. These principles, which were established by GDPR, give persons certain legal rights over their accumulated data, including the ability to access, modify, and delete pertinent data that is tracked and collected by machines, and if they are violated, 'a fine of up to 4% of total accumulated revenue will be assessed.' Companies, from the other side, bear a greater obligation to safeguard individual information recorded from individuals in order to comply with the rules and standards that guide GDPR policies and frameworks. [32]

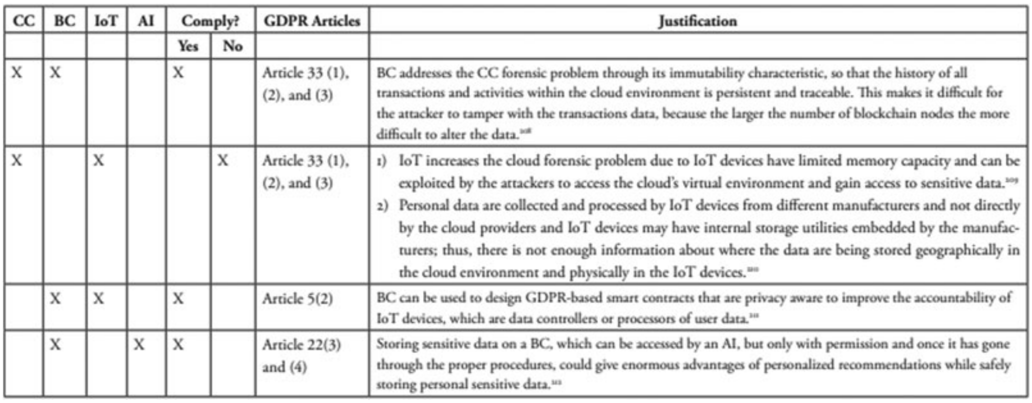
Numerous legal matters have required identifying inappropriate use of individual information collected in order to apply protective regulations to avoid massive losses incurred by the institutions, compelling the regulatory body to enact a law specifically addressing personal data protection and assuming responsibility for identifying and investigating two organizations that violate the law. Because so many businesses are reliant on digital technologies and customer data, there is a high potential for data theft that could be harmful to a large number of businesses if the information is made available to competitors. People and organizations are becoming increasingly concerned about how their personal information is being used to benefit production industries and massive international organizations.

There is very little recognition given to small businesses that rely on data accumulated through the use of artificial intelligence technologies and devices in comparison to large organizations. Many safeguards must be put in place by organizations that rely on technology and Big Data Analytics to safeguard the privacy of the information they collect from individuals. The guidelines and framework for obtaining personal data must be followed by organizations on a proactive basis as well. The source of data collection from individuals has all the rights of ownership and control over personal information, so data protection must be given the highest priority. Any business that uses digital technology or artificial intelligence methodologies must be held responsible for the data it uses.[33]

6. CONCLUSION

The new emerging technologies used by various organisations to achieve and embark on a sustainable journey will be significantly impacted by GDPR. Businesses must comply with GDPR and see it as an opportunity to improve their data-driven outcomes. Personal data analysis and strategy development should be facilitated by

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press



CC	BC	IoT	AI	Comply?		GDPR Articles	Justification
				Yes	No		
X	X			X		Article 33 (1), (2), and (3)	BC addresses the CC forensic problem through its immutability characteristic, so that the history of all transactions and activities within the cloud environment is persistent and traceable. This makes it difficult for the attacker to tamper with the transactions data, because the larger the number of blockchain nodes the more difficult to alter the data.[108]
X		X			X	Article 33 (1), (2), and (3)	1) IoT increases the cloud forensic problem due to IoT devices have limited memory capacity and can be exploited by the attackers to access the cloud's virtual environment and gain access to sensitive data.[109] 2) Personal data are collected and processed by IoT devices from different manufacturers and not directly by the cloud providers and IoT devices may have internal storage utilities embedded by the manufacturers; thus, there is not enough information about where the data are being stored geographically in the cloud environment and physically in the IoT devices.[110]
	X	X		X		Article 5(2)	BC can be used to design GDPR-based smart contracts that are privacy aware to improve the accountability of IoT devices, which are data controllers or processors of user data.[111]
	X		X	X		Article 22(3) and (4)	Storing sensitive data on a BC, which can be accessed by an AI, but only with permission and once it has gone through the proper procedures, could give enormous advantages of personalized recommendations while safely storing personal sensitive data.[112]

Figure 1: Source: Combinations of technologies versus GDPR.[34]

organisations that operate globally and have a need to comply with GDPR.

Different approaches can be used to recognise the GDPR compliance problems created by the physical properties of emerging technologies. The strategy in this paper is to combine the four technologies so that the characteristics of one address the compliance challenges of the other. Comparing the engineering for GDPR compliance by design is concerned with software design, development, and operations.

Personal data used in technology applications must be safeguarded in order in order to gain the confidence of both customers and staff. An increasing number of organizations have come to appreciate the important connection between information and technology collection in recent years, resulting in positive results. Global privacy regulation (GDPR), as well as recent technological advancements, will help organisations improve their efficiency and gain a competitive edge in today's and tomorrow's global economic environments by better collecting and analysing personal data and using that data.

Effectively, GDPR compliance by design is a short-term solution to the four emerging technologies' compliance challenges. In the long run, the EU data protection law may be modified to accelerate the adoption of emerging technologies. We have seen the revision of EU data protection law from Directive 95/46/EC to GDPR in order to accommodate the use of new technologies and facilitate cross-border data exchange.[35] While GDPR may be seen as a burden by many organisations, it has helped raise awareness of data use and abuse in our digitally connected world. It remains to be seen whether new technologies will potentially impact data protection regulations.

7. RECOMMENDATIONS

As a result of GDPR, many organisations face challenges in maintaining the confidentiality of individual data collected through a slew of computer programmes. Because of this, organisations should take proactive measures that could benefit the wider populace and the way businesses and organisations make decisions about what products and services to make and how to make them in the present economy. Following are a few suggestions to help organisations implement and comply with the GDPR:

1. **Data Security:** Organizations should focus on adapting to methods and practises that could involve the use of technology in gathering relevant information and analysing legitimate information in a secure environment in order to improve the judicial process of companies through the use of personal information concentration. The implementation of new methods and practices should not be the primary focus of institutions. Additionally, institutions should examine how they can be more open and honest with the public about the reasons for finding private information.
2. **Developing Trust:** Customer service and commercial activities require organizations that deal with customers to maintain positive public relations. The majority of decisions are based on the preferences and requirements of the customer. The collection of personal data in order to better understand and predict consumer behaviour is critical in order to deliver products and services that consumers expect. When it comes to gaining consumer trust, there are a variety of factors that influence organizations to be transparent and honest in their duties and practices. When customers have faith in a company, they are more willing to share personal information as well as pertinent information that could help the company improve its operations.
3. **Data Localisation:** Data is essential to our economy's future and unlike any other resource. Data is now considered an asset, with implicit value derived from insights, patterns, and distribution of data, as well as its amalgamation with other data. Data localisation has two strategic aspects: geographically located storage and sharing with optimum control over its usage.

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press

Footnotes

[1] Masoud Barati, Ioan Petri, and Omer F Rana, 'Developing GDPR Compliant User Data Policies for Internet of Things' in *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing* Auckland, NZ (IEEE, 2019).

[2] Nir Kshetri, 'Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution' (2013) 37(4-5) *Telecommunications Policy* 372–86.

[3] Michel Avital et al, 'Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future' in *Proceedings of the 37th International Conference on Information Systems*, Dublin, Ireland (Association for Information Systems, 2016).

[4] Will Venters and Edgar A Whitley, 'A Critical Review of Cloud Computing: Researching Desires and Realities' (2012) 27(3) *Journal of Information Technology* 179–97.

[5] A Gobeo, C. Fowler and W. J. Buchanan, 'GDPR and Cyber Security for Business Information Systems' (Gistrup, Denmark: River Publishers, 2018).

[6] Article 3 of GDPR. Available at: https://gdpr-info.eu/art-3-gdpr/

[7] Article 3, Recital 15, GDPR. Available at: https://gdpr-info.eu/recitals/no-15/

[8] Department for the Promotion of Industry and Internal Trade, *Draft E-Commerce Policy* (23 February 2019). Available at: https://dipp.gov.in/sites/ default/files/DraftNational_e-commerce_ Policy_ 23February2019.pdf

[9] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (Harper Collins Publishers India 2018).

[10] Amba Uttara Kak, *Cambridge Analytica and the Political Economy of Persuasion* (Engage Economic Political Weekly 2018). <Cambridge Analytica and the Political Economy of Persuasion | Economic and Political Weekly (epw.in)>

[11] Daniel Solove, 'Privacy Self-management and Consent Dilemma' (2013) *Harvard Law Review* 1880-1903. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf.

[12] Aleecia M McDonald and Tom Lowenthal, 'Nano-Notice: Privacy Disclosure at a Mobile Scale' (2013) *Journal of Information Policy* 331–354 https://www.jstor.org/stable/10.5325/jinfopoli.3.2013.0331 accessed 28-10-2019.

[13] Council of Europe, Consultative Committee of Convention, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (23 January 2017) p 2. Available at https://rm.coe.int/16806ebe7a

[14] 'The European Economic and Social Committee and the Committee of the Regions towards a thriving data economy European Commission' Communication from the Commission to the European Parliament, the Council (July 2014) https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-442-EN-F1-1.Pdf.

[15] 'Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement', Parliament resolution (14 March 2017) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0076.

[16] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work and Think* (John Murray, 2013) 153.

[17] 'Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights' (White House Report May 2016). https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[18] Payal Arora, 'Politics of Algorithms, Indian Citizenship, and the Colonial Legacy' in Aswin Punathambekar and Sriram Mohan, *Global Digital Cultures Book Subtitle: Perspectives from South Asia* (University of Michigan Press 2019). https://www.jstor.org/stable/j.ctvndv9rb.5

[19] Ralph Schroeder, *Big data: Shaping Knowledge, Shaping Everyday Life* (UCL Press 2018). https://www.jstor.org/stable/j.ctt20krxdr.9

[20] Stuart Russel and Peter Norvig, *Artificial Intelligence: a Modern Approach* (3rd ed, Alan Apt, 2009, Upper Saddle River, New Jersey: Prentice Hall) p 2. https://www.cin.ufpe.br/~tfl2/artificial-intelligence-modern-approach.9780131038059.25368.pdf

[21] 'Transcript of Mark Zuckerberg's Senate Hearing' *Washington Post* (10 April 2018) https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

[22] Thomas M. Lenard and Paul H. Rubin, 'Big Data, Privacy and the Familiar Solutions' (2015) 11 *J.L. Econ. & Poly* 1 available at Hein online.

[23] Branden Ly, 'Never Home Alone: Data Privacy Regulations for the Internet of Things' (2017) *U. Ill. J.L. Tech. & Poly* 539 available at Hein online.

[24] William Weir, 'Fitbit Founder, and Upcoming Tech Summit Speaker Eric Friedman is an 'Eternally Optimistic' Entrepreneur' *Yale News* (25 October 2016) available at https://news.yale.edu/2016/10/25/fitbit-founder-and-upcoming-tech-summit-speaker-eric-friedman-eternally-optimistic-entrep.

[25] Papadopoulou, Panagiota, et al, 'Investigating The Business Potential Of Internet Of Things' *MCIS 2017 Proceedings*, Genoa, Italy (Association for Information Systems 2017).

[26] Ibid.

[27] Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR' (2018) 34(3) *Computer Law and Security Review* 436–49

[28] Riley v California 573 U.S. 373 (2014)

[29] Paul M Schwartz, 'Information Privacy in the Cloud' (2013) 161 *University of Pennsylvania Law Review* 1623-1662 https://www.jstor.org/stable/23527814 accessed 28-10-2019.

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press

[30] Jiawei Han and Micheline Kamber, *Data Mining: Concepts and Techniques* (3rd ed. Morgan Kaufmann, 2011) http://myweb.sabanciuniv.edu/rdehkharghani/files/2016/02/The-Morgan-Kaufmann-Series-in-Data-Management-Systems-Jiawei-Han-Micheline-Kamber-Jian-Pei-Data-Mining.-Concepts-and-Techniques-3rd-Edition-Morgan-Kaufmann-2011.pdf.

[31] European Parliament, *European Civil Law Rules in Robotics*, (Directorate-General for Internal Policies, 2016), no. 14, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf.

[32] Andreas Kaplan and Michael Haenlein, 'Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence' (2019) 62(1) *Business Horizons* (Elsevier Ltd) 15–25.

[33] J Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) 26(1) *International Journal of Law and Information Technology* 45–63.

[34] Rania El-Gazzar and Karen Stendal, 'Examining How GDPR Challenges Emerging Technologies' (2020) 10 *Journal of Information Policy* 237–275.

[35] Mira Burri, and Rahel Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 479–511.

Bibliography

Aleecia M McDonald and Tom Lowenthal, 'Nano-Notice: Privacy Disclosure at a Mobile Scale' (2013) 3 *Journal of Information Policy* 331–354. https://www.jstor.org/stable/10.5325/jinfopoli.3.2013.0331 accessed on 28-10-2019.

Amba Uttara Kak, 'Cambridge Analytica and the Political Economy of Persuasion' (*Engage Economic Political Weekly*, 18 May 2018). Available at: Cambridge Analytica and the Political Economy of Persuasion | Economic and Political Weekly (epw.in)

Masoud Barati, Ioan Petri, and Omer F Rana, 'Developing GDPR Compliant User Data Policies for Internet of Things' in *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*, Auckland, NZ (IEEE, 2019).

Branden Ly, 'Never Home Alone: Data Privacy Regulations for the Internet of Things' (2017) *U. Ill. J.L. Tech. & Poly* 539. Available on Hein online.

Mira Burri, and Rahel Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 *Journal of Information Policy* 6, no. 2016, 479–511.

Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 2, available at https://rm.coe.int/16806ebe7a.

Draft E-Commerce Policy, Department for the Promotion of Industry and Internal Trade, 23 February 2019. Available at: https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy* (July 2014) https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-442-EN-F1-1.Pdf.

'European Parliament resolution of 14 March 2017 on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law-enforcement' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0076.

European Parliament, *European Civil Law Rules in Robotics*, (Directorate-General for Internal Policies, 2016), no. 14

A Gobeo, C. Fowler and W. J. Buchanan, *GDPR and Cyber Security for Business Information Systems* (Gistrup Denmark: River Publishers, 2018). https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

Jiawei Han and Micheline Kamber, *Data Mining, Concepts and Techniques* (3rd ed. Morgan Kaufmann, 2011) http://myweb.sabanciuniv.edu/rdehkharghani/files/2016/02/The-Morgan-Kaufmann-Series-in-Data-Management-Systems-Jiawei-Han-Micheline-Kamber-Jian-Pei-Data-Mining.-Concepts-and-Techniques-3rd-Edition-Morgan-Kaufmann-2011.pdf.

Andreas Kaplan and Michael Haenlein, 'Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence' (2019) 62(1) *Business Horizons* (Elsevier Ltd) 15–25.

J Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) 26(1) *International Journal of Law and Information Technology* 45–63.

Paul M Schwartz, 'Information Privacy in the Cloud' (2013) 161 *University of Pennsylvania Law Review* 1623–1662 https://www.jstor.org/stable/23527814 accessed: 28-10-2019.

Payal Arora, 'Politics of Algorithms, Indian Citizenship, and the Colonial Legacy' in Aswin Punathambekar and Sriram Mohan, *Global Digital Cultures Book Subtitle: Perspectives from South Asia* (University of Michigan Press 2019). https://www.jstor.org/stable/j.ctvndv9rb.5

Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (Harper Collins Publishers India 2018).

Ralph Schroeder, *Big data: shaping knowledge, shaping everyday life* (UCL Press 2018). https://www.jstor.org/stable/j.ctt20krxdr.9

Daniel Solove, 'Privacy Self-management and Consent Dilemma' (2013) *Harvard Law Review* 1880–1903. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf.

Stuart Russel and Peter Norvig, *Artificial Intelligence: a Modern Approach* (3rd ed, Alan Apt, 2009, Upper Saddle River, New Jersey: Prentice Hall) p 2. https://www.cin.ufpe.br/~tfl2/artificial-intelligence-modern-approach.9780131038059.25368.pdf.

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press

Nir Kshetri, 'Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution' (2013) 37(4-5) *Telecommunications Policy* 372–86

Thomas M. Lenard and Paul H. Rubin, 'Big Data, Privacy and the Familiar Solutions' (2015) 11 *J.L. Econ. & Poly* 1. Available on Hein online.

Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work and Think* (John Murray, 2013) 153.

'Transcript of Mark Zuckerberg's Senate Hearing' *Washington Post*, (10 April 2018).https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/

'Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights' (White House Report May 2016)

William Weir, 'Fitbit Founder and Upcoming Tech Summit Speaker Eric Friedman is an 'Eternally Optimistic' Entrepreneur' *Yale News* (25 Oct 2016). https://news.yale.edu/2016/10/25/fitbit-founder-and-upcoming-tech-summit-speaker-eric-friedman-eternally-optimistic-entrep

Michel Avital et al, 'Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future' in *Proceedings of the 37th International Conference on Information Systems*, Dublin, Ireland (Association for Information Systems, 2016).

Will Venters and Edgar A Whitley, 'A Critical Review of Cloud Computing: Researching Desires and Realities' (2012) 27(3) *Journal of Information Technology* 179–97.

Biographies

Ms Varda Mone graduated (B.A. LLB) from Nagpur University and Post-graduation (LLM in Constitution and Administrative Law) from Dr Ram Manohar Lohia National Law University Lucknow. She has worked as Assistant Professor at the Indore Institute of Law, Indore, M.P. She was also a full-time research intern at the Office of Mr. Vijay Sai Reddy, Member of Rajya Sabha, Indian Parliament. Presently She is a Research Scholar at VIT-AP School of Law pursuing a PhD in data Protection Laws.

Dr CLV Sivakumar did his B.Com. From Nagarjuna University, A.P.in the year 1989; M.A. from Alagappa university T.N. in the year 2004; B.L. from Nagarjuna University, A.P. in the year 1994 and M.L. from Nagarjuna University, A.P. in the year 1996. He completed PhD (Law) from Nagarjuna University in 2012. He has worked as Lecturer in Law during the period 1996–1998 in SBRTM Law College, Cuddapah (A.P). and as Assistant Professor of Law in Jaya Group of Educational Institutions, Chennai, (TN) during the period 1998–2008; Later to which he worked as Associate Professor of Law in VIT Business School, VIT University, Vellore, Tamil Nadu. He served in the position of Registrar VIT-AP University from 2016 till 15 June 2022. Presently, he is a Professor of Law at VIT University, Vellore, Tamil Nadu. His email address is: sivakumar.clv@vit.ac.in

https://doi.org/10.1017/S1472669622000317 Published online by Cambridge University Press