GDPR Impact on Computational Intelligence Research

Keeley Crockett[1], Sean Goltz[2], Matt Garratt[3]
[1]School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University, Manchester, M1 5GD, UK, K.Crockett@mmu.ac.uk
[2]Business & Law School, Edith Cowan University, Perth, Australia, n.goltz@gmail.com
[3]School of Engineering and IT. University of New South Wales, PO Box 7916, Canberra BC 2610, ACT 2902, Australia, m.garratt@adfa.edu.au

***Abstract*— The General Data Protection Regulation (GDPR) will become a legal requirement for all organizations in Europe from 25th May 2018 which collect and process data. One of the major changes detailed in Article 22 of the GDPR includes the rights of an individual not to be subject to automated decision-making, which includes profiling, unless explicit consent is given. Individuals who are subject to such decision-making have the right to ask for an explanation on how the decision is reached and organizations must utilize appropriate mathematics and statistical procedures. All data collected, including research projects require a privacy by design approach as well as the data controller to complete a Data Protection Impact Assessment in addition to gaining ethical approval. This paper discusses the impact of the GDPR on research projects which contain elements of computational intelligence undertaken within a University or with an Academic Partner.**

Keywords- GDPR, Profiling, automated-decision making, computational Intelligence

I. INTRODUCTION

In a society governed by rules attempting to protect person's privacy, people are generally unaware as to how much of their personal information is collected and the ways in which this data will be manipulated and used. Historically, when consent was requested in order to collect a subject's data, this request was often lengthy and shrouded in legal terminology. This usually results in the consent form not being read in detail and questioned by the data subject, or not being understood. For example, a person may give consent whilst not really knowing to what use their data will be put or how their data will be manipulated.

Concerns about privacy are of particular importance to those in the computational intelligence (CI) field. CI encapsulates "*the theory, design, application, and development of biologically and linguistically motivated computational paradigms emphasizing neural networks, connectionist systems, genetic algorithms, evolutionary programming, fuzzy systems, and hybrid intelligent systems in which these paradigms are contained*."[1]. In conducting research within the field, Dunis et. al [2] highlights some of the known scientific difficulties such as overfitting, feature selection, interoperability and parameter tuning. More recently, further data related challenges (velocity, variety, volume, veracity, and value) associated with applying CI algorithms to Big Data have added further complexities to the development of new and existing applications of CI algorithms. Such challenges can cause CI systems either to be difficult to set up, run the risk of skewing the results or can mean that the results that emerge are difficult to interpret. Sandvig et al. [3] asks, 'Can an Algorithm be Unethical?'. Models generated from CI algorithms are derived from an underlying set of data upon which decisions are formulated. It would therefore be correct to assume that CI systems might be prone to pick up the biases inherent in the data despite the fact that they are supposed to be totally unbiased. Examples of bias learnt from human behaviour includes the photo recognition software that classifies those of a certain heritage as a gorilla [4] and Microsoft's sexist and racist Chabot, Tay [5]. It is debatable whether as CI becomes more complex, our ability to understand and therefore guide how it makes decisions - decreases. In order to comply with international legal requirements such as the GDPR, we also need to understand not only the societal and ethical challenges but also the legalities of conducting CI research.

A requirement of the GDPR is to make the consent of data subjects to be in an, "*intelligible and easily accessible form*" [6]. The GDPR also gives individuals the right to receive an explanation on how an automated decision was made in their case. Individuals will now have the right, "*not to be subject to a decision…which is based solely on automated processing and which provides legal effects (on the subject).*"[6]. If, for example, a mortgage application uses machine learning algorithms based on decision trees then it is straightforward to extract a set of rules that led to the decision whether to approve a mortgage in a specific case or not. However, the justification of the statistics that have been used based on the training sample might be trickier (i.e., biased). If, however, traditional artificial neural networks were to be used to construct the mortgage data model, explanation of how a decision was reached will be complex. In both cases the language used to provide explanations will have to be public friendly. The GDPR does state what types of decisions the legislation will cover and it may be left to the discretion of the European Union individual countries. For example, within the UK, the Information Commissioner's Office (ICO)

has stated that individuals are "*very likely*" to ask for explanations of decisions when applying for credit, insurance and possibly in recruitment decisions [7]. Given that the definition of explainable decisions and where they might apply is still vague, Dinsmore [8] argues that the requirement may force data scientists to stop using techniques such as deep learning where decisions are more difficult to explain and interpret. Organizations that violate the GDPR can be fined up to 4% of their annual global turnover or €20 Million [6]. In light of this new legislation, current and future CI focused research conducted in Universities will need close examination and scrutiny of the appropriate legislation.

The concept of Responsible Research and Innovation (RRI) [9], a growing area, particularly within the EU, offers potential solutions to workplace bias and is being adopted by several research funders such as the EPSRC (The UKs Engineering and Physical Sciences Research Council) [10], who include RRI core principles in their mission statement. RRI is an umbrella concept that draws on classical ethics theory to provide tools to address ethical concerns from the outset of a project (design stage and onwards). Quoting Von Schomberg, "*Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society).*" [11]. Through recent consultations, individual countries are putting the ethics of artificial intelligence at the core of technological developments, for example at the World Economic Forum in Davos (January 2018), the current British Prime Minister (PM), outlined plans for a national center for ethics in artificial intelligence [12].

The IEEE is leading the global initiative in establishing a set of societal, and policy driven guidelines for the use and impact of autonomous and intelligent systems. Version 2 of the IEEE Ethically Aligned Design document [13] was released in December 2017 and contains a chapter on personal data and individual access control. Working groups for four IEEE standards on data privacy have been setup. The initiative suggests using a "personalized privacy AI" agent to act as a broker between each individual and all other entities wishing to access their private data. The idea of a broker is to help deal with the fragmentation of data across numerous organizations that might use that data and to help individuals make informed decisions on how to share their data whilst navigating the complexities of the consequence of such sharing with so many potential organizations wanting to use that data. The agent could provide advice on options regarding which type of data can be shared, track what permissions have been granted and check compliance of the receiving organizations. Development of such an agent and policies on how it might be used could be a very useful area of research. Principle 4 of the IEEE Ethically aligned design document [13] also highlights the fact that transparency in decision making is important because it builds human trust into the system. In the case where the system makes the wrong decision, the internal processes that the autonomous system took will need to be explainable. It is designed to protect vital interests of the data subject. As the IEEE global initiative gains providence, the Ethically Aligned Design Document will become an essential resource for CI practitioners. Privacy by design is a legal requirement under the GDPR.

For researchers conducting projects with a CI focus undertaken within or with a University or Academic Partner, the challenge is in understanding the impact of the GDPR on their research. Clearly in an international context, it is not only those in the European Union and/or countries, which adopt regulation that will need to be GDPR ready. This paper discusses the impact of the GDPR on CI as elements of research projects undertaken within or with a University or Academic Partner. Whereas academics may be pioneers in their specific fields, they may have less knowledge of privacy by design approaches, data protection impact assessments and what the GDPR actually means for their research. The paper ends with a set of brief recommendations that CI researchers should consider at the start of every research project.

This paper is organized as follows; Section II provides an overview of the legislation regarding the GDPR and Profiling. Section III reviews some example profiling systems based on computational intelligence approaches. Section IV examines the role of privacy by design from the perspective of undertaking research projects within a university, and finally Section V makes recommendations for researchers working in the field of computational intelligence.

II. GDPR: PROFILING AND AUTOMATED DECISION MAKING

Article 4(4) of the GDPR defines what forms of data processing could be considered as "*profiling*". This includes any form of automated processing of personal data; and utilizing this personal data to evaluate certain personal aspects relating to a natural person. For example, analyzing or predicting "*aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*" [6]. Recital 71 provides a lengthy definition of what is meant by the term profiling [6] especially in relation to any personal aspect "*concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.*". Article 22 of the GDPR concerns the rights of an individual when interacting with systems that may automatically make a decision or profile them in any way that they have not given consent to [6]. The main principle of article 22 is *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or*

similarly significantly affects him or her" [6]. In any aspect of automated decision making, the individual has the right to ask for human intervention and provide an explanation of how the machine based decision has been reached through disclosure of "*the logic involved*" (article 13 [6]). Recital 71 states that the data controller should use appropriate mathematical and statistical procedures for profiling and that data should be accurate in order to minimize the risk of errors. On the subject of automated profiling, UK Lawyers, Wright Hassall [14] recommend that companies should avoid automated processing on any sensitive personal data unless explicit informed consent of an individual is first obtained.

The GDPR also now requires organizations to conduct a Data Protection Impact Assessment (DPIA) specifically in the case where profiling and/or automated decision making is utilized - "*A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures"*([6] Recital 91]. More discussion regarding conducting a DPIA in terms of CI research is discussed in section IV.

CI based systems, have historically been used within profiling and automated decision-making. Some examples are the profiling of users within intelligent tutoring systems to provide recommended learning activities using fuzzy trees [15] or the personalization of learning from utilizing neural networks to automatically detect and monitor learner's comprehension from the non-verbal behaviour [16]. Zheng et al [17] utilized a fuzzy deep learning approach to profiling airline passengers for "*classifying normal passengers and potential attackers…*" [17]. Angelos et al. [18] used a fuzzy c-means clustering algorithm to detect abnormalities within customer energy consumption profiles within Power Distribution Systems [18]. The new legislation within the GDPR suggests that CI researchers need to re-examine the legalities of profiling systems especially in a) the ability to communicate effectively that a person is to be profiled and what this profile will be used for and b) the ability for the CI system to provide an explain the logic behind a person be assigned a particular profile.

III. COMPUTATIONAL INTELLIGENCE DECISION BASED SYSTEMS

A. Overview

It has been argued that as CI gets more complex our ability to understand and therefore guide how it makes decisions decreases. Moreover, it may come to pass that these machines will need to be maintained by other specialist machines, further removing humanity from the equation [19]. A list of existing and potential CI application is limitless, yet with each application that involves decision making, researchers must consider the ethical, moral, social and legal implications of the system making a decision and ask: Does a human have the final say? Can the system give a reason why the decision was made? Is the decision itself explainable to a member of the public who will use the system?

Let us consider self-driving cars. On the positive side, while self-driving cars will lack the innate morality of humans, they might also lack the distractions (unless these are programmed into the cars themselves). That is to say an autonomous vehicle won't be thinking about what to cook for dinner or how their upcoming interview will go which could lead to less accidents overall. Conversely, self-driving cars come with the risks inherent in a non-sentient being in control of a dangerous object. On the one hand, no one wants to be in a situation where the car will decide to avoid danger to others at all costs but neither will society allow the manufacture of vehicles that seek only their own protection [20]. The classic tension in this space is exemplified by the oft cited "trolley problem" whereby a decision needs to be made whether to take a positive action and kill something or do nothing and risk killing several people [21]. Some countries, such as the UK's Department of Transport have already issued a set of "Key principles of vehicle cyber security for connected and automated vehicles" which manufacturers must adhere to for such cars to drive in UK roads [22].

Another CI application area which has huge ethical dilemmas is that of autonomous weapons systems (AWS). If (and when) drones are used in combat situations, how are we able to be sure that they correctly recognize the target from innocent parties. This is particularly relevant in the case of using a learning or evolutionary intelligence, which may change the way things are viewed over time. The IEEE Global Initiative has identified eleven issues concerning AWS in a document currently open for public discussion [13], each having a set of detailed candidate recommendations covering areas such as predictability of a weapon systems, the use of learning and adaptive learning algorithms, and the ability for humans to have meaningful control. All require the AWS to be able to clearly explain their reasoning and decisions. Can AWS ever be made safe? The Future of Life Institute created a short film [23] which was shown at the United Nations Convention on Conventional Weapons in November 2017, hosted by the Campaign to Stop Killer Robots. This movie clearly raises the issue of whether these systems cross the moral line of who dies and who lives. Another risk isn't so much with the ethics of the machines but rather of nefarious individuals who seek to exploit them. Just as current machines can be hacked, one cannot rule out the possibility that future ones might be hacked as well, with potentially calamitous results.

B. Case Study: Automated Deception Detection

Automated deception detection systems (ADDS) detect whether an individual is lying or not by conducting some measurement on that individual's behavior. Systems such as the polygraph which intrusively detect lies by measuring

physiological changes related to stress through body during an interview have been around since the 1920s [24]. Ultimately, a trained polygraph examiner makes the decision on whether physiological changes indicate truthful or deceptive behavior and are widely accepted by the public and used in courts of law (although usually requiring the parties consent to be used). In contrast, Silent Talker [25, 26] is an ADDS system which uses computational intelligence, specifically artificial neural networks (ANN), to make judgements of participants' deception based on microgestures (small facial and other movements). Silent Talker utilizes up to 40 channels of facial nonverbal behavior which it extracts from static or live feed video, processes, detects the behaviour of channel objects i.e. the left eye, and feeds all information into a final classifier to give a probability of deception/ truthfulness. This system has been shown in laboratory conditions to achieve an accuracy of up to 87% [25]. So how can the Silent Tracker's decision be explained? Depending on whether the final classifier is ANN based or decision forest based determines whether some explanation is possible – but would it actually be meaningful to a human being? Especially if providing a numerical representation of the behaviour of a facial feature such as an eye. It would also be common that the number of rules generated by decision trees in such a domain can be in excess of 1000's making human comprehension difficult. This raises the question on how do such complex CI systems provide an adequate explanation that satisfy the GDPR requirement? However, in CI systems which operate within the security field, releasing how a decision is made could lead to a higher risk of spoofing the system.

iBorderCtrl [27, 28] is a system currently under development whose prime aim is to enable faster and thorough border control for third country nationals crossing the land borders of EU Member States in line with the current status quo of Schengen Border Management. The system will feature an ADDS system based on a near real-time Silent Talker for traveler pre-arrival border-style crossing interviews. The system, funded as a H2020 grant (2016-2019) [28] by the EU involves a partner institution expert in legal informatics, data protection, data security and ethics who will lead the EU-wide legal review and the tasks associated with legal and ethical compliance. However, institutions such as Universities will also have their own standard operating procedures and processes for conducting ethical research and for data governance, which may have some different legalities dependent on the country's own legislation. In addition, some institutions may put initial effort into ensuring compliance with GDPR principles that align more directly with the Data Protection Act 1998, rather than examine the newer laws regarding profiling, the right to refuse an automated decision and the right to an explanation which may involve R&D protocol and physical systems changes in the ways that they conduct business.

IV. Data Privacy Impact Assessments and Etical Considerations

A) Data Privacy Impact Assessments

Kamarinou et al [29] argues that if personalized data was anonymized and used to target individuals or infer some behavior about them for automated decision-making, then this would be considered as "*incompatible with the purpose for which the data were originally collected*". Data Privacy Impact Assessments (DPIA) are fundamental to undertaking a privacy by design approach which is mandatory under the GDPR. The DPIA is designed to be a tool that allows organizations to "comply with their data protection obligations and meet individuals' expectations of privacy." [30, 31]. The DPIA contains a description of data processing operations and its purpose, an internal assessment of the necessity and proportionality of the processing in relation to the purpose, a risk assessment to individuals along with the associated measures to address the risk such as consideration of all issues in relation to data security.

Consider a research project, which spans academics and industry over several countries. The project lead, will adopt one DPIA format, whilst organizations will have their one in house format. In the UK, the ICO [32], provides suggestion on the content of a DPIA but states that organizations can adopt their own content as long as it is compliant with the requirements. The first stage comprises of a set of screening questions (Figure 1) which determine whether a DPIA is necessary. [32]. If it is deemed that a DPIA is required, then a series of six steps is required to complete the DPIA (Figure 2), followed by a further section where the DPIA is linked to the data protection principles.

The challenge to a CI researcher is in having the depth of knowledge of the GDPR articles to be able to complete an effective DPIA. For example, consider the case study of the ADDS system described in section III. Under Step three: Identify the privacy and related risks - the compliance risk associated with each privacy issue should be recorded in terms of non-compliance with the Data Protection Act and also specific articles of the GDPR. One might consider that as ADDS provides a deception risk score determined from a hierarchy of neural networks, individuals cannot get an explained decision on how the ADDS artificial neural network classifiers obtained this score from their nonverbal behaviour during an automated pre-travel interview. This initially suggests non-compliance with GDPR Article 22 – "*the right not to be subject to a decision based solely on automated processing"* [33] but as ADDS is part of a larger Border Control system, where ultimately a decision on whether to "Go" straight through border control, or "proceed to a second line check" is made by combining of the results of multiple sub-systems [28] – does ADDS alone need to meet this GDPR requirement as ADDS does not make the final decision of the overall system "*which is based solely on automated processing*"?. However, as ADDS does make a decision on the deception risk element through effectively profiling an individual then this individual will have the right,

at the informed consent stage, to choose whether or not to undertake a pre-arrival border-style crossing interview.

1. Will the project involve the collection of new information about individuals?
2. Will the project compel individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5. Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
6. Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
8. Will the project require you to contact individuals in ways that they may find intrusive?

Fig.1. DPIA Screening Questions [23]

Step one: Identify the need for a PIA
Step two: Describe the information flows
Step three: Identify the privacy and related risks
Step four: Identify privacy solutions
Step five: Sign off and record the PIA outcomes
Step six: Integrate the PIA outcomes back into the project plan

Fig.2. Steps for completion of a DPIA [23]

B) Research Ethics

Organizations have long established principles, policies and procedures which guide the researcher on how to conduct ethically aligned research in accordance with the law. Universities will have a set of clear set of guidelines that addresses how researchers and research organizations should conduct themselves when working with participants, their personal data (including personal artifacts) [34]. Recently, there has been an emergence in companies creating specific ethics research units as part of their R&D in the field of computational intelligence i.e. DeepMind, owned by Google, has launched a research unit called DeepMind Ethics & Society in late 2017 [35]. Mustafa Suleyman, co-founder of DeepMind reported "*A tech company that applies its technology without due consideration for ethical and social implications is destined to be a bad tech company*" [35]. Whilst other companies follow suit, this is a clear indicator that ethically aligned design will be considered more as the norm rather than the exception. Indeed, "*Ethics is an essential element of good research governance*" [34].

Traditionally, the process of making an ethical application for a research project, has involved the research lead completing a number of checklists and forms i.e. an ethics checklist, an ethics application, research insurance form, a health and safety risk assessment form and in some projects a security sensitive information form. The application as a whole is then reviewed by an internal ethics panel where it may be approved or further meetings with the research team are required for clarification. Some universities have begun adopting an electronic ethical process using systems such as the Ethics Online System (EthOS) to establish clear workflows and responsibilities. However, the questions asked on an ethics application can overlap with those on the DPIA. For example, in identifying any ethical issues, the researcher would have to detail how the data would be secured to ensure protection of a participant's confidentiality. In addition, a clear description and justification must be given if any sensitive data was to be collected, such as age, colour, race/ethnicity, disablement, religion etc.

The challenge to the CI researcher is the knowledge and the time to carry out the processes effectively within the organization. For example, challenges can occur when a research project conducted within a University is part of a larger international consortium based project where effectively the DPIA and the Ethics application must be undertaken twice to meet the legal requirements of a number of different countries. Secondly, there is the terminology barrier between those who review the ethics application (from a multidisciplinary area) who may be unfamiliar with the terminology and methodologies used in CI research. In situations such as this communication of the ethical considerations required can only be understood by all parties through additional meetings. Hence, it is crucial that specific time be built into all projects to go through the ethical approval process.

V. RECOMMENDATIONS AND CONCLUSIONS

This paper has attempted to discuss impact of the GDPR on research projects, which contain elements of computational intelligence. It has attempted to raise awareness of what this legislation will mean for CI systems that profile and/or produce automated decisions and how it will be expected that decisions made by such systems should be explainable. Although the GDPR is a European Regulation, research and collaboration is often undertaken within an international community which implies that for data sharing, there may will be a need for international compliance. In our limited experience so far, we present the following recommendations:

- CI researchers should gain familiarity in the principles of the IEEE Ethically aligned design document V2 [13].

- Ensure the local research team has had appropriate training in the GDPR [6, 7, 31, 33, 36, 37]
- Adopt a privacy by design approach at the start of the research project and build in privacy and data protection to the research proposal or any knowledge transfer partnerships with industry [32]
- Ensure the legal responsibility between project partners is clear and well defined.
- Conduct an initial ethical review at the project proposal stage. This will naturally lead to the identification of data privacy issues, risks, security including cybersecurity of data).
- Conduct a Data Protection Impact Assessment in phases, if appropriate at the same time as the initial ethical review [30].
- Build in specific time (as a specific task) into any grant application for conducting a DPIA and an ethical review.

Whilst all current and new CI research projects must seek to confirm to the GDPR, draft guidance from European regulators suggests that this "data protection by design" approach should be extended to existing systems within three years [31]. The impact of this in terms of time will be significant and it will need the establishment of specialized teams with extensive knowledge of both the GDPR and the field of computational intelligence.

The GDPR is a warranted step towards the much-needed protection humans require in the midst of the artificial intelligence fourth industrial revolution. In the context of computational intelligence and academic research it is yet to be seen whether the implementation and compliance of the relevant GDPR principles will provide a desirable outcome. The interface between regulation and complex systems, especially autonomous systems, is highly challenging and requires new and innovative approach. Developing new research projects with the GDPR main goal in mind (protecting human subjects) should be the overarching principle to be considered in any related future academic research.

REFERENCES

[1] Scope of Computational Intelligence, IEEE Computational Intelligence society, [online], Available: http://cis.ieee.org/field-of-interest.html. [Accessed 23/12/2017].

[2] Dunis, C, Likothanassis, S, Karathanasopoulos, A, Sermpinis, G, & Theofilatos, K (eds) (2014), Computational Intelligence Techniques for Trading and Investment, Taylor and Francis, Florence. Available from: ProQuest Ebook Central. [Accessed 26/0/2017].

[3] Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2016). When the Algorithm Itself Is a Racist: Diagnosing ethical harm in the basic components of software. International Journal of Communication, 10, pp. 4972–4990.

[4] Larson, J. Angwin, J., & Parris Jr., T. (2016), [online], How Machines Learn to be Racist. ProPublica. Available at: https://www.propublica.org/article/breaking-the-black-box-how-machines-learn-to-be-racist?word=Trump [Accessed 19/10/2017]

[5] Lee, P. Learning from Tay's Introduction (2016), [online], available: https://blogs.microsoft.com/blog/2016/03/25/learning-tays-Introduction/, Date Accessed [2/1/2017]

[6] The GDPR Portal (2017), [online]. Available at: https://www.eugdpr.org/ Accessed [21/12/2017].

[7] Information commissioner's Office (2017), Guide to the General Data Protection Regulation (GDPR) [online]. Available at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf Accessed [21/12/2017]

[8] Dinsmore, T. How GDPR Affects Data Science (2017), [online], , Available at: https://thomaswdinsmore.com/2017/07/17/how-gdpr-affects-data-science/ Accessed [20/12/2017]

[9] Burget, M., E. Bardone, and M. Pedaste. "Definitions and Conceptual Dimensions of Responsible Research and Innovation: A Literature Review." Science and Engineering Ethics 23, no. 1 (2016): pp.1–9.

[10] EPSRC, Engineering and Physical Sciences Research Council. [online], Available at https://www.epsrc.ac.uk/ [Accessed 22/01/2018].

[11] Von Schomberg, R. (2011), Prospects for Technology Assessment in a Framework of Responsible Research and Innovation, in Technikfolgen Abschätzen Lehren: Bildungspotenziale Transdisziplinärer Methode, Wiesbaden, Germany: Springer VS, pp. 39–61.

[12] PM's speech at Davos 2018: 25 January, [online]. Available: https://www.researchprofessional.com/0/rr/news/uk/politics/whitehall/2018/1/May-seeks-consensus-on-AI-s-benefits-and-limitations-.html?utm_medium=email&utm_source=rpMailing&utm_campaign=personalNewsDailyUpdate_2018-01-25#sthash.mvPeuPmd.dpuf [Accessed: 28/1/2018].

[13] Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2, The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (2017) [online], Available: https://ethicsinaction.ieee.org/, [Accessed 23/12/2017].

[14] GDPR – Individuals' Rights, (2017) Wright Hassall, [online], Available at: https://www.wrighthassall.co.uk/knowledge/legal-articles/2017/11/21/gdpr-individuals-rights/ [Accessed: 28/1/2018].

[15] Wu, D. Lu, J. Zhang, G. (2015) A Fuzzy Tree Matching-Based Personalized E-Learning Recommender System, IEEE Transactions on Fuzzy Systems, Vol:23:6, pp. 2412 – 2426.

[16] Holmes, M. Latham, A. Crockett, K, O'Shea, J. (2017) Near real-time comprehension classification with artificial neural networks: decoding e-Learner non-verbal behaviour, IEEE Transactions on Learning Technologies, 2017, Vol:PP: 99, DOI: 10.1109/TLT.2017.2754497.

[17] Zheng, Y. Sheng, W. Sun, X. Chen, S. (2017) Airline Passenger Profiling Based on Fuzzy Deep Machine Learning, IEEE Transactions on Neural Networks and Learning Systems, Vol28:12, pp 2911 – 2923.

[18] Angelos, E. Saavedra, O. Cortés, O. Nunes de Souza, A. (2011), Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems, IEEE Transactions on Power Delivery, Vol:26:4, pp. 2436 – 2442.

[19] Heron, M. & Belford, P., (2015), Fuzzy ethics: or how I learned to stop worrying and love the bot. ACM SIGCAS Computers and Society, 45(4), pp.4–6.

[20] Baum, S. Social Choice Ethics in Artificial Intelligence [online], available at SSRN.com https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046725, [Accessed 1/10/17].

[21] Santoni de Sio, F. Ethic Theory Moral Prac (2017) 20: 411. https://doi-org.ezproxy.waikato.ac.nz/10.1007/s10677-017-9780-7. [Accessed 1/10/17]

[22] The key principles of vehicle cyber security for connected and automated vehicles (2017) [online], Available at: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles [Accessed 22/1/2018].

[23] Ban on killer robots urgently needed, say scientists (2017), [online] Available at: https://www.theguardian.com/science/2017/nov/13/ban-on-killer-robots-urgently-needed-say-scientists, [Accessed 22/1/2018].

[24] International League of Polygraph Examiners (2018), Polygraph/Lie Detector FAQs. [online]. Available at: http://www.theilpe.com/faq_eng.html. [Accessed 5/1/18].

[25] Rothwell, J., Bandar, Z., O'Shea, J. and McLean, D., (2006). Silent talker: a new computer□based system for the analysis of facial cues to deception. Applied cognitive psychology, 20(6), pp.757-777.
[26] Silent Talker Ltd [online], Available at: https://www.silent-talker.com/ [Accessed 5/1/18].
[27] Crockett, KA and O'shea, J, Szekely, Z, Malamou, A, Boultadakis, G, Zoltan, S (2017), Do Europe's borders need multi-faceted biometric protection. Biometric Technology Today, 2017 (7). pp. 5-8. ISSN 0969-4765.
[28] iBorderCtrl Intelligent Portable Control System [online], Available at http://www.iborderctrl.eu/ [Accessed 12/1/2018]
[29] Kamarinou, D. Millard, C. Singh, J. (2017) Machine Learning with Personal Data: Profiling, Decisions and the EU General Data Protection Regulation. To appear, Journal of Machine Learning Research, 2017. [online] Available at http://www.mlandthelaw.org/papers/kamarinou.pdf, [Accessed 12/1/2018].
[30] Information commissioner's Office (2014),Conducting privacy impact assessments code of practice. [online], Available: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf Accessed [21/12/2017].
[31] Cormack, A. (2017), Preparing for the GDPR - a guide for universities, [online] Available: http://universitybusiness.co.uk/Article/preparing-for-the-gdpr Accessed [21/12/2017].
[32] ICO - Privacy by design (2017) [online], Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/ [Accessed 22/01/2018].
[33] Art. 22 GDPR Automated individual decision-making, including profiling (2017), [online]. Available: https://gdpr-info.eu/art-22-gdpr/ Accessed [21/12/2017].
[34] Ethics and Governance, Manchester Metropolitan University, (2018), [online], Available at: https://www2.mmu.ac.uk/research/staff/ethics-and-governance/ethics/, [Accessed: 28/1/2018].
[35] DeepMind, [online], Available at: https://deepmind.com/ [Accessed: 28/1/2018].
[36] ICO highlights that GDPR requires businesses to understand and explain the rationale of decisions taken by machines, (2017), [online], Available: https://www.out-law.com/en/articles/2017/march/ico-highlights-that-gdpr-requires-businesses-to-understand-and-explain-the-rationale-of-decisions-taken-by-machines/
[37] Article 29 Working Party. (2013) Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation. [online] Available at http://bit.ly/2fIei8K, [Accessed: 28/1/2018].