ALEXA, FORGET MY DATA!: HOW ARTICLE 17 OF THE GDPR PROTECTS PERSONAL DATA PROCESSED BY MACHINE LEARNING ALGORITHMS

ABSTRACT

Article 17 of the General Data Protection Regulation (GDPR) provides individuals with the opportunity to request that their personal data be erased from organisations that are processing it. This paper assesses the ability of companies to correctly implement Article 17 when using machine learning algorithms, and whether Article 17 enhances the protection of an individual's personal data rights in this context. It will be maintained that personal data protection is incredibly important in the twenty-first century, and that the control Article 17 gives individuals over their personal data is crucial to personal data protection. This will be demonstrated by an analysis of the controversies surrounding Article 17, the data shared by individuals, and finally with an analysis of the best practices for erasing data from machine learning models. It will be argued the other provisions in the GDPR can be used to enforce Article 17.

TABLE OF CONTENTS

Introduction

Each time that an individual browses the Internet they leave behind data that social networking websites, search engines, Internet Service Providers, and other companies collect and analyze.[1] Companies using machine learning algorithms are able to harvest the data, including intimate details about the customers visiting their websites.[2] In an attempt to allow individuals to regain control over their personal data, the General Data Protection Regulation (GDPR) includes a right to erasure in Article 17.[3] This paper will answer the question: how does Article 17 enhance the protection of personal data processed by machine learning algorithms? It will be argued that Article 17 provides individuals with the opportunity to regain control over their data, and is therefore an important part of personal data protection. This will be demonstrated through a socio-legal approach, by analysing both the social need for a right to erasure and the legal requirements of Article 17. The effectiveness of Article 17 will be evaluated in relation to the protection it provides an individual's personal data against processing by machine learning algorithms. Moreover, the usefulness of Article 17 can be assessed in relation to the ability of these companies to enforce the right to erasure.

The first section will define artificial intelligence as well as machine learning. Then it will explore the legal background of personal data rights and Article 17. The second section will explore the controversies surrounding the inclusion of Article 17 in the GDPR, in particular the debate on whether forgetting should have a place in the digital world, and if it is possible at all to implement a right to erasure in companies using machine learning algorithms. In order to explore the social need for a right to erasure, the third section will highlight the willingness of individuals to share personal data without realising the effects

[1] Michael Kearns, *Data Intimacy, Machine Learning, and Consumer Privacy,* (University of Pennsylvania Law School, 2.

[2] Ibid, 2.

[3] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/04 (General Data Protection Regulation).

that this has – using the Cambridge Analytica scandal as an example. The fourth section will then argue that Article 17 can still be implemented in these companies when the GDPR is correctly enforced and when data protection is balanced with the machine learning models. There will finally be a discussion on the best form of regulation for machine learning technologies and come to the conclusion that it is simply too early to regulate, thus cementing that Article 17 is an important part of protecting personal data.

1. **Background**

1.1 *Artificial Intelligence and Machine Learning*

Alan Turing laid the initial foundations for Computer Science nearly seven decades ago when he asked "can machines think?"[4] Since then, artificial intelligence and machine learning have quickly become two of the biggest buzzwords of the twenty-first century.[5] While it is difficult to define artificial intelligence, it can be understood as the design and study of algorithms that allow for computer systems to undertake functions normally requiring human intelligence to perform.[6] Although 'machine learning' is sometimes conflated with 'artificial intelligence', it is actually a subset of artificial intelligence.[7] The goal of machine learning is for computers to be able to learn without human assistance based upon the provided data and improve automatically.[8] Self-driving cars, voice assistants, and chatbots used for customer service interactions are all products of machine learning.[9]

Recent progress made in machine learning has been driven by the vast amount of data available online.[10] The more data that machine learning algorithms obtain and process,

[4] Alan Turing, 'Computing Machinery and Intelligence' (1950) 49 Mind 433, 433.

[5] Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?* (HL 100, 2018).

[6] Mark Riedl, 'Human-centered artificial intelligence and machine learning' (2019) 1 (1) Human Behaviour and Emerging Technology 1, 1.

[7] Select Committee on Artificial Intelligence, (n 5), 14.

[8] Michael Jordan and Tom Mitchell, 'Machine Learning: trends, perspectives, and prospects' (2015) 349 (6145) Science 255, 255.

[9] Erik Brynjolfsson and Tom Mitchell, 'What can machine learning do? Workforce implications' (2017) 358 (6370) Science 1530, 1531.

[10] Michael Jordan and Tom Mitchell, (n 8), 255.

the better they become at spotting certain patterns and coming to different conclusions.[11] In order to improve their accuracy machine learning algorithms require large data sets. One recently collected database, for example, included one million three-second videos.[12] By default, this online data that machine learning algorithms learn from is not anonymised and includes characteristics that can be attributed to specific individuals.[13] Say, for example, there is a set of data regarding the increased risk of lung cancer for those who smoke. A computer is presented with a set of data that says person A and B are smokers, and person C and D are not. Then it learns that person A and B have developed lung cancer while person C and D have not. Ultimately, the computer will notice the pattern in the data and come to the conclusion that smoking increases the likelihood of lung cancer. The tensions with personal data rights arise where person A can be identified as 'Jane Smith'. Jane Smith will ultimately have certain rights in relation to her personal data.

1.2 *Personal Data Rights*

As technology has continued to develop, there has been an increasingly high value attached to personal data. In 2011, the World Economic Forum suggested that personal data can be viewed as a new asset class.[14] According to Spiekermann et al, this is due to the unique opportunities that it provides to companies that would be otherwise impossible without the data.[15] For example, companies utilise personal data to create targeted advertisements for individuals, carry out risk assessments, or to create personalised search

[11] Mehdi Jamali and others, 'Social media data and post-disaster recovery' (2019) 44 International Journal of Information Management 25, 26.
[12] Mathew Monfort and others, 'Moments in Time Database: one million videos for event understanding' (2019) IEEE Computer Society 1, 1.
[13] Reuben Binns, Lillian Edwards, and Michael Veale, 'Algorithms that remember: model inversion attacks and data protection law' (2018) The Royal Society <https://doi.org/10.1098/rsta.2018.0083> accessed 18 February 2019.
[14] World Economic Forum, *Personal Data: The Emergence of a New Asset Class,* (World Economic Forum, 2011), 5.
[15] Sarah Spiekermann and others, 'The challenges of personal data markets and privacy' (2015) 25 Institute of Information Management 161, 161.

results.[16] Personal data protection is recognised in Article 8 of the Charter of Fundamental Rights of the European Union (the Charter), which declares that "everyone has the right to the protection of personal data concerning him or her."[17] The second paragraph of the Charter establishes that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[18] The importance of protecting personal data and personal data rights is also interlinked with Article 7 of the Charter, which gives individuals the right to "respect for private and family life."[19] There is a certain standard of privacy that should be and typically is expected when it is related to information concerning a specific individual.[20] The fundamental importance of personal data protection was highlighted with the introduction of the GDPR.

Personal data is defined in the GDPR as information from which a 'data subject' can be determined, this can include their "name, an identification number, location data … [or] physical … genetic, mental … cultural, or social identity" factors specific to that person.[21] A person's name is not required for them to be identifiable. Pseudonymised data, despite the fact that these type of data are processed in such a way that an individual cannot be attributed to it without the use of other information, still falls within the scope of personal data within the GDPR.[22] When an individual is not identifiable through data, this is considered anonymous data and the GDPR does not apply.[23]

The provisions within the GDPR are applicable to data controllers and data processors that process data relating to any citizen within the European Union, including by

[16] Sarah Spiekermann and others, (n 15), 161.

[17] Charter of Fundamental Rights and Freedoms of the European Union [2000] OJ C364/01, Article 8 (1); see also Treaty on the Functioning of the of the European Union (TFEU), Article 16 (1).

[18] Charter of Fundamental Rights and Freedoms of the European Union [2000] OJ C364/01, Article 8 (2).

[19] Ibid, Article 7.

[20] Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 (2) Computer Law & Security Review 179, 180.

[21] General Data Protection Regulation, (n 3), Article 4(2); see also Data Protection Act 2018, s3(3).

[22] General Data Protection Regulation, (n 3), Article 4(5); Recital 26.

[23] Ibid, Recital 26.

organisations that are located outside of the European Union.[24] A data controller is a legal entity or individual that "determines the purposes and means of the processing of personal data."[25] A data processor, meanwhile, is a person that processes personal data on behalf of the data controller.[26] This processing is broadly defined under the GDPR and essentially refers to nearly any activity that is executed on personal data (for example, this may refer to collecting, using, storing, altering, or destroying the data).[27] Moreover, the GDPR gives individuals a number of rights such as the right of access, data portability, to be informed, and, perhaps most controversial of all, the right to be forgotten.[28]

1.3 *The Right to be Forgotten*

The right to be forgotten is only one part of data protection, however it can have a large and beneficial impact for natural persons. Theoretically, the right does as the name suggests – it provides a method for individuals to have their data 'forgotten.'[29] However, forgetting is more than just the erasure of data. As the internet has continued to develop and social media platforms have become a more prominent part of individual's lives, the vast amounts of information available online have made it difficult to abandon one's history.[30] One example of this can be seen in the 'case' of Stacy Snyder.[31] Days before her graduation in 2006, Snyder was denied her teaching degree after a photo of her was found online by a member of staff at the high school she was training at. The photo was of her drinking from a

[24] Mark Watts and Emma Macalister Hall, 'Data Protection in the UK (England and Wales): overview' (*Thomson Reuters Practical Law,* 2019) <https://uk.practicallaw.thomsonreuters.com/w-012-9556?comp=pluk&transitionType=Default&contextData=(sc.Default)> accessed 15 February 2019.

[25] General Data Protection Regulation, (n 3), Article 4(7).

[26] Ibid, Article 4(8).

[27] Ibid, Article 4(2).

[28] Ibid, Article 15, Article 20, Article 13, Article 14, and Article 17.

[29] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press, 2018), 5.

[30] Rolf H Weber, 'The Right to be Forgotten: More Than a Pandora's Box?' (2011) 1 (2) Journal of Intellectual Property, Information Technology and Electronic Commerce 120, 120.

[31] Meg Leta Jones, (n 29), 4.

cup, wearing a pirate hat and had the caption "Drunken Pirate".[32] Stories like this are now more common than ever due to digital memory and data retention.[33]

The controversy surrounding the Right to be Forgotten flared up in the EU in 2014 with the landmark judgment of *C-131/12 Google Spain SL and Google Inc v. AEPD and Mario Costeja González* ('*Google Spain*'). The CJEU held in this case that individuals have the right to have information relating to themselves delisted from search results in certain circumstances.[34] Although rather than the right to be forgotten, what was established in the *Google Spain* judgment was a 'right to be delisted'. Following on from the *Google Spain* case came Article 17 of the GDPR.

Article 17, the right to erasure (also known as the right to be forgotten) is a qualified right for individuals to request that organisations erase their personal data.[35] The right applies when: the individual no longer consents to having their personal data processed and the organization relied on the consent to process the data,[36] where the organization no longer requires the personal data for the reason they originally collected it for,[37] where the entity keeping the personal data have no other legitimate reason to do so,[38] where the data have been processed unlawfully,[39] for compliance with other legal obligations,[40] or it has been collected when the person was under age.[41] The individual must make a request for erasure

[32] Meg Leta Jones, (n 29), 4; Jeffrey Rosen, 'The Web Means the End of Forgetting' (*The New York Times Magazine,* 2010) <https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html> accessed 11 March 2019.
[33] For example, *see* Matthew Haag, 'Woman Who Was Fired for Giving Trump the Middle Finger Sues Former Employer' (*The New York Times,* 2018) <https://www.nytimes.com/2018/04/05/us/juli-briskman-middle-finger-trump.html> accessed 7 March 2019; Dylan Love, '13 People Who Got Fired for Tweeting' (*Business Insider,* 2011) < https://www.businessinsider.com/twitter-fired-2011-5?r=US&IR=T> accessed 7 March 2019.
[34] C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) 317, para 99.
[35] General Data Protection Regulation, (n 3), Article 17.
[36] Ibid, Article 17(1)(b).
[37] Ibid, Article 17(1)(a).
[38] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)* (1. 0. 248, 2018), 118; General Data Protection Regulation, Article 17(1)(c).
[39] General Data Protection Regulation, (n 3), Article 17(1)(d).
[40] Ibid, Article 17(1)(e).
[41] Ibid, Article 17(1)(f).

verbally or in writing and the organizations have one month to respond to the request.[42] However, there are a number of statutory exceptions to the obligation on the data controllers to erase the data.[43] This includes, for example, where processing is necessary for the right of freedom of expression and information,[44] to comply with a legal obligation,[45] or for reasons of public interest.[46] Moreover, the controller must ensure that they take all reasonable steps to inform any other controllers that they have shared the personal data with that there has been a request for erasure.[47]

2. **The Controversies Surrounding Article 17**

2.1 Forgetting in the Twenty-First Century

It is often argued that in this modern, data-driven society, forgetting is an outdated concept which has no place in contemporary legislation. However, forgetting has been known to provide a number of benefits for humans. As many scholars have argued, forgetting is a central part of human life.[48] Perhaps most fundamental to society is the fact that, when data is not retained and is instead forgotten, individuals are allowed a second chance.[49] The ability of individuals to request their data be deleted because they no longer consent to it being processed (and their consent was the basis for it being processed in the first place)[50] is incredibly important for data protection and ensuring that individuals have control over their personal data.

[42] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)* (1. 0. 248, 2018), 119.
[43] Ibid, 118.
[44] General Data Protection Regulation, (n 3), Article 17(3)(a).
[45] Ibid, Article 17(3)(b).
[46] Ibid, Article 17(3)(C).
[47] Ibid Article 17(2).
[48] See for example Jean-Francois Blanchette and Deborah Johnson, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness' (2002) 18 (1) The Information Society 33, 34; Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009); Eugnia Politou and others, 'Backups and the right to be forgotten in the GDPR: An uneasy relationship' (2018) 34 (6) Computer Law & Security Review 1247, 1249.
[49] Jean-Francois Blanchette and Deborah Johnson, (n 48), 33.
[50] General Data Protection Regulation, (n 3), Article 6(1), Article 9(2)(a), Article 17 (1)(a).

Mayer-Schönberger argues that forgetting is essential in order for an individual to learn, and "the erosion of individual privacy is a fundamental challenge we are facing in our times".[51] Supporting this proposition, Burkell suggests that an individual's need to uphold their own identity is threatened by the digital world where everything is "remembered".[52] On the other hand, Rosen suggests that society will ultimately learn to adapt to a world in which everything is remembered.[53] Similarly, Boyd argues that individuals are going to develop ways to cope with the fact that everything remains on the internet.[54] This, however, should not be the case. Ultimately personal data protection is as much about consumer protection when it comes to the use of personal data in machine learning algorithms. It should not be expected that, for example, because an individual has signed up to a mailing list their data should be retained forever, especially if they no longer consent to how the company is processing their data. Individuals should have control over information pertaining to them. Regardless, Article 17 should not be seen as a right to truly 'forget' all information since the term pertains to the human memory.[55]

Instead, it is proposed that Article 17 should be looked at solely as a right to erasure, rather than a right to be forgotten. When one considers that Article 17 is about erasing the data rather than forgetting it, the value of the right for data subjects becomes clearer. To illustrate this point it is perhaps best, as Markou did, to return to the example of Stacey Snyder, asking "if Miss Snyder could 'click and delete' the harmful picture from MySpace,

[51] Viktor Mayer-Schönberger,(n 48), 12.

[52] Jacquelyn A Burkell, 'Remembering me: big data, individual identity, and the psychological necessity of forgetting' (2016) 18 Ethics and Information Technology 17, 20.

[53] Jeffrey Rosen, 'Free speech, privacy, and the web that never forgets' (2011) 9 Telecommunications and High Technology Law 345;

[54] Jessica Winter, 'The Advantages of Amnesia' (*The Boston Globe,* 2007) <http://archive.boston.com/news/education/higher/articles/2007/09/23/the_advantages_of_amnesia/> accessed 18 March 2019 (quoting Boyd).

[55] Elena Esposito, 'Algorithmic Memory and the Right to be Forgotten' (2017) 4 (1) Big Data & Society 1, 5.

would her supervisor and any other person who got to see it, forget about it?"[56] The answer to this question has to be no. Thus, it is not a right to be completely forgotten when you exercise it, but rather it is an opportunity for an individual to regain control over how of their personal data is processed by machine learning algorithms. Article 17 is therefore an incredibly important part of data protection.

2.2 Tensions Between Machine Learning and Article 17

Much of the tension between machine learning and personal data rights in general comes from the need for a large amount of data in order for a machine to learn.[57] Kuner et al highlight this in their article, arguing that machine learning is a threat to data protection not only because of the need for data, but also because of its use of personal data.[58] Importantly, the larger a training data set, the more accurate and specific the results will be.[59] Although the European Commission has proposed ensuring that the EU should facilitate access to data for artificial intelligence in order to be more competitive,[60] there is a level of protection that must be provided when it is personal data.

This does, however, lend itself to the question of how data included in machine learning algorithms can be erased so as to correctly protect an individual's personal data rights. Kieseberg, Villaronga, and Li argue that the "strict deletion requirement" under Article 17 is likely impossible in machine learning environments.[61] Likewise, the Centre for Information Policy Leadership also suggests that the right to erasure could potentially

[56] Christiana Markou, "The '*Right to Be Forgotten':* Ten Reasons Why It Should Be Forgotten" in Serge Gutwirth, Ronald Leenes, Paul and de Hert (eds), *Reforming European Data Protection Law,* (Springer Publishing, 2014), 211.

[57] Chris Kuner and others, 'Expanding the artificial intelligence – data protection debate' (2018) 8 (4) International Data Privacy law 289, 290.

[58] Ibid, 290.

[59] European Commission, 'Artificial Intelligence for Europe' (2018), 11.

[60] Ibid.

[61] Peter Kieseberg, Tiffany Li, and Eduard Fosch Villaronga, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten' (2017) Computer Law and Security Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018186> accessed 10 October 2018.

compromise a complete data operation.[62] Moreno also suggests that the fact that data is stored in multiple places - from when it is originally collected to after it is analysed through the machine learning algorithm - is the key reason that Article 17 conflicts with machine learning.[63] Individuals' data are used to train these algorithms to become smarter over time, the question becomes how these algorithms will 'unlearn' what they have already been taught as their model is based upon this personal data.[64] Academics therefore suggest that privacy regulation is simply unable to handle the complexities of artificial intelligence.[65]

The vagueness of Article 17 also causes difficulty as to the applicability of it in machine learning environments, with no definition of what 'erasure' means anywhere in the text of the Regulation.[66] Kieseberg et al argue that this can cause a number of difficulties for companies using machine learning algorithms as it can be difficult to apply this in machine learning environments.[67] The data that machine learning algorithms use comes from personal data such as location, blogs, characteristics, and messages. After it goes through the algorithm it comes to a different conclusion than the original data may have contained. For example, the fact that those who are vegetarian miss fewer flights.[68] However, these algorithms still rely on the original data, such as who is a vegetarian, to come to their conclusions. Perhaps it is best to ensure the data is only kept for as long as necessary.[69] Although retaining the data is beneficial for machine learning training, there needs to be

[62] Centre for Information Policy Leadership, *Learning from the EU GDPR: What elements should the US Adopt?,* (Centre for Information Policy Leadership, 2019), 6.

[63] Julio Moreno and others, 'Neuralyzer: A Security pattern for the Right to be Forgotten in Big Data' (2018) 24 Pattern Languages of Programs 1, 2.

[64] Wu He, He Li, and Lu Yu, 'The Impact of GDPR on Global Technology Development' (2019) 22 (1) Journal of Global Information Technology Management 1; Chris Kuner and others, (n 57), 291.

[65] Peter Kieseberg, Tiffany Li, and Eduard Fosch Villaronga, (n 61).

[66] General Data Protection Regulation (n 3).

[67] Peter Kieseberg, Tiffany Li, and Eduard Fosch Villaronga, (n 61). .

[68] Elena Espisito, (n 55), 4; Erik Siegel, *Predictive Analysis: the Power to Predict who will click, buy, lie, or die* (John Wiley & Sons, 2013).

[69] Centre for Information Policy Leadership, *Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice,* (Centre for Information Policy Leadership, 2018), 14.

compliance with data protection laws.[70] Nevertheless, this would not avoid an individual enforcing their right to erasure by revoking their consent.[71] There must be a balance found to ensure that machine learning technologies can continue to advance while mitigating the damages of processing personal data. The best way to successfully implement Article 17 will be explored in the fourth part of this paper.

3. **The Modern Reality**

3.1 The Willingness to Share

However, there still remains the question, why should these data be erased from machine learning algorithms if it would apparently be difficult to do so? The answer is that no matter how valuable machine learning may be, a person should have control over data pertaining to themselves. A 2012 study found that in common situations, such as online shopping, people are often unaware of the privacy issues that they face when they fill in forms requiring their personal information.[72] Similarly, websites such as Facebook give individuals the choice to share their data by posting pictures, 'liking' posts, or updating their relationship status, but individuals are not aware of how their data is retained. These information technology companies continue to gather, sell, analyze, and commodify this data that they collect through machine learning algorithms.[73] One 2012 study suggested that if an individual were to spend 8 hours a day reading each privacy policy they encounter in a year, it would take them 76 working days to do so.[74] Once consumers understand how their personal data is being used and retained, they should have the option to have this data erased

[70] Ibid, 15.

[71] General Data Protection Regulation, (n 3), Article 17 (1)(b).

[72] Alastair Beresford, Dorothea Kubler, Soren Preibusch, 'Unwillingness to pay for privacy: a field experiment' (2012) 117 (1) Economics Letters 25; Volker Benndorf and Hans-Theo Normann, 'The willingness to sell personal data' (2017) 120 (4) The Scandinavian Journal of Economics 1, 2.

[73] Alexander Tsesis, 'Data subjects' privacy rights: regulation of personal data retention and erasure' (2019) 90 University of Colorado Law Review 593, 606.

[74] Keith Wagstaff, 'You'd need 76 work days to read all your privacy policies each year' (*Time,* 2012) <http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/> accessed 12 February 2019.

by the company. Article 17 therefore provides a fundamental layer of protection for an individual in particular due to the ability it gives an individual to revoke their consent to have their data processed.[75]

3.2 Cambridge Analytica

The Cambridge Analytica scandal has been widely broadcasted mainly due to the scrutiny shone on Facebook CEO, Mark Zuckerberg, by media outlets and different Governments around the world.[76] The data firm Cambridge Analytica was given access to more than 87 million Facebook users' personal data by Facebook.[77] They received this access after individuals completed a personality quiz through the Amazon platform Mechanical Turk as well as Qualtrics that required the individuals to give access to their Facebook profile, and in turn their Facebook friends' information.[78] Cambridge Analytica then went on to use this information in conjunction with other data from various social media platforms, online purchase histories, voting results, and more in order to establish over 5,000 data points (such as political views, sexuality, and personality traits) on 230 million American adults.[79] From these data they were able to deliver targeted political messages to each individual whose data they had collected for both the 2016 United States Presidential Election and the Brexit referendum.[80]

Much of the personal data that Facebook already collected on its users, and allowed third parties access to, led to Cambridge Analytica being able to create targeted messages

[75] General Data Protection Regulation, (n 3), Article 17(1)(b).

[76] Christian Kurtz and others, *The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems,* (Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019), 3.

[77] Jim Isaak and Mina Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection' (2019) 51 (8) Computer 56, 57.

[78] Ibid, 57.

[79] Ibid, 57.

[80] Carole Cadwalladr, 'The great British Brexit robbery: how our democracy was hijacked' (*The Guardian,* 2017) <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> accessed 18 March 2019.

based on individual profiles. Christopher Wylie, the whistle blower on Cambridge Analytica's troubling operations and former employee, explained in an interview that the algorithms that they built used Facebook users data (such as pages and posts they have 'liked', location, and their contact details) as a training set.[81] This training set was then used to come to various conclusions about the individual, and was used in conjunction with information from other publicly accessible data such as an electoral register. The Cambridge Analytica scandal only serves to strengthen the argument for individuals to have an avenue to erase their personal data that is held by companies. Individuals should not have Facebook, or any other company, retaining their personal data which can then be used by companies such as Cambridge Analytica to target them with political messages without their knowledge, which ultimately threatens democracy.[82] Therefore Article 17 provides an avenue for individuals to regain control over their data and ensure that it is no longer processed when they do not consent to it, or if it is being processed in a way that it should not be.

4. **Erasing Data from Machine Learning Models**

4.1 *The GDPR*

It is then established that Article 17, in theory, provides extensive protection and strengthens an individual's data protection rights.[83] However, it must be able to be enforced in practice. There needs to be a balance between personal data protection and machine learning methods, so as to ensure that data protection is not weakened in order to benefit machine learning. Thus, more attention needs to be given to the provisions in the GDPR, and how they can be used to guarantee Article 17's effectiveness in machine learning algorithms.

[81] Alex Hern, 'Cambridge Analytica: how did it turn clicks into votes?' (*The Guardian,* 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 28 February 2019.

[82] Jim Isaak and Mina Hanna, (n 77), 57.

[83] European Commission, 'Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation' (2018).

The GDPR, while increasing the rights of individuals, also increases the duties of organisations.[84] It is explicit that data controllers are accountable for ensuring compliance with the GDPR and they must also be able to demonstrate this compliance.[85] This principle of accountability means that data must be processed in accordance with the GDPR, and therefore the data must be processed lawfully,[86] and collected and processed for a specific purpose.[87] The data controllers are accountable for ensuring that their internal policies comply with the GDPR, including a process to respond to Article 17 requests. They must also review their machine learning processes and update them when necessary.[88]

There is also a principle of data minimisation, which entails only collecting and using as much personal data as is necessary.[89] It has been argued that this is difficult to employ in machine learning contexts as it is firstly problematic to hypothesise what the algorithm will learn, and secondly it is also possible that the purpose will change the more that the machine learns.[90] However, data minimisation means that the controller should limit the detail that is incorporated in training of the algorithm as well as in the execution of the model. By restricting the type and amount of personal details used in the data collected, the controller will comply with data minimisation.

The GDPR further introduces a data protection impact assessment (DPIA) for companies to undertake, and by doing so they can successfully examine how to best process personal data.[91] A DPIA is a process that must be implemented in order to recognise and reduce any data protection risks that may arise in organisations, while ensuring that there is compliance with GDPR obligations. When using machine learning algorithms, there are a

[84] Norwegian Data Protection Authority, *Artificial Intelligence and Privacy,* (Datatilsynet, 2018), 25.

[85] Chris Kuner and others, (n 57), 292; General Data Protection Regulation, (n 3), Article 5(2).

[86] General Data Protection Regulation, (n 3), Article 5(1)(a).

[87] Ibid, Article 5(1)(b).

[88] Ibid, Article 24 (1), Recital 74-79.

[89] Ibid, Article 5(1)(c); Norwegian Data Protection Authority, (n 84), 18.

[90] Ibid, 18.

[91] General Data Protection Regulation, (n 3), Article 35(1), Article 25 (7), Recital 84, Recital 90.

number of risks that may arise from processing these data.[92] This is legally required for any type of processing that may impact the rights and freedoms of a natural person.[93] The use of new technologies, such as machine learning, can also be taken in to account during the assessment.[94] This would allow the company to see if they can continue to process the data and if they would be able to comply with Article 17 requests.[95] It would also ensure that there is a lawful basis for processing the data.

Another requirement of the GDPR is privacy by design found in Article 25 of the GDPR. This means that the organisation must implement technical and organisational measures to ensure the data in their systems are protected.[96] Companies that are still developing their machine learning algorithms must therefore plan a processing system with the ability to identify and remove an individual's data should they need to.[97] Although privacy by design under the GDPR leaves it open to the company as to the protective measures that they can take, they suggest the pseudonymisation of personal data as one potential method.[98] It is important to note that simply because the data is pseudonymised it still falls within the scope of personal data under the GDPR due to the fact that, in conjunction with the use of other data, it can be used to identify an individual.[99] Despite this, pseudonymising the data would still help data controllers to meet their obligations under the GDPR as they comply with the 'data minimisation' principle, as well as the 'storage limitation' principle.[100] The storage limitation principle means that companies should only process personal data for no longer than is required to complete the purpose that it was

[92] Norwegian Data Protection Authority, (n 84), 25.
[93] Information Commissioner's Office, (n 42), 160.
[94] Norwegian Data Protection Authority, (n 84), 25.
[95] General Data Protection Regulation, (n 3), Article 17(1)(a)-(f).
[96] Ibid, Article 25.
[97] Ibid, Article 25, Recital 78.
[98] Ibid Recital 78, Article 4(3)(b).
[99] Ibid, Recital 26.
[100] Ibid, Article 5(1)(d), Article 5(1)(e).

originally collected for.[101] If companies were to ensure that the data they retain complies with Article 5 of the GDPR, then it would make compliance with Article 17 easier. There would be no requests for erasure due to the fact that it is unlawfully processed, or that it is being processed for a reason other than why it was originally collected.[102] The protection of data would therefore be considered from the start.

To ensure compliance with the GDPR, a data protection officer (DPO) is required by the GDPR for companies that store or process a large amount of personal data, and for all public authorities, or where the processing involves a large amount of 'special categories of personal data' (for example, race or religion).[103] Those companies that are not required to by the GDPR may appoint a DPO if they wish to. Having a DPO would be incredibly beneficial to ensure that Article 17 can be correctly enforced. The DPO's tasks include monitoring compliance, advising on data protection impact assessments, as well as acting as the first point of contact for those whose data is processed.[104] By having a DPO, companies utilising machine learning algorithms can be better informed as to whether they are effectively complying with an Article 17 requests as the DPO is legally required to hold expert knowledge of data protection law.[105] Additionally, a DPO would ensure that the data that is being processed in a machine learning algorithm is for the reason that they first collected the data for.

As is necessary under the GDPR, machine learning algorithms must be coded based on the privacy by design principle.[106] It is suggested that in order to fully demonstrate that companies using machine learning algorithms meet the principle of privacy by design that they anonymise the data that they retain. While it is possible that it would affect the

[101] Ibid, Article 5(1)(e).
[102] Ibid, Article 17(1)(a), Article 17(1)(d).
[103] General Data Protection Regulation, (n 3), Article 9.
[104] Ibid, Article 39.
[105] Ibid, Article 37(5).
[106] Ibid, Article 25.

performance of machine learning models, this is something that will need to be accepted in order to enhance the protection of personal data rights.[107] If data were to be anonymised and it can no longer be attributed to an identifiable person, then the Regulation does not apply to the processing of this information.[108] There is currently research being done in to privacy-aware data management systems which would satisfy this; [109] prominent examples of this are k-anonymity,[110] data aggregation,[111] differential privacy,[112] and data obfuscation.[113] Data obfuscation in particular involves covering up original data with altered content.[114]

Ultimately, it is clear that for future machine learning algorithms the ability to erase or anonymise data should be programmed in order to protect personal data rights.[115] Moreover, machine learning models should be able to encode universal patterns that cannot be attributed to a specific individual.[116] Goodfellow and Papernot even go as far as suggesting that when machine learning algorithms are designed with data protection in mind, it produces "better-behaved models" that can both protect an individual's data while advancing machine learning development.[117]

4.2 *Is Specific Regulation for Machine Learning Necessary?*

If a company is compliant with the GDPR then they should be able to ensure that they can successfully comply with Article 17 requests, particularly by ensuring that all

[107] Julio Moreno and others, (n 63), 1.

[108] General Data Protection Regulation, (n 3), Recital 26.

[109] Bernd Malle, Peter Kieseberg, and Andreas Holzinger, 'Interactive Anonymization for Privacy aware Machine Learning' (2017) Institute for Medical Informatics, Statistics & Documentation 15, 16.

[110] Latanya Sweeney, 'K-Anonymity: a model for protecting privacy' (2002) 10 (5) International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 557.

[111] Qinghua Li, Guohong Cao, Thomas La Porta, 'Efficient and Privacy-Aware Data Aggregation in Mobile Sensing' (2014) 11 (2) IEEE Transactions on Dependable and Secure Computing 115.

[112] Cynthia Dwork, 'Differential privacy' (2006) 4052 Automata, Languages, and Programming 1.

[113] David Bakken and others, 'Data obfuscation: anonymity and desensitization of usable data sets' (2004) 2 (6) IEEE Security & Privacy 34.

[114] Ibid, 34.

[115] Jean-Francois Blanchette and Deborah Johnson, (n 48), 3.

[116] Ian Goodfellow and Nicolas Papernot, 'Privacy and machine learning: two unexpected allies?' (*Cleverhans Blog,* 2018) <http://www.cleverhans.io/privacy/2018/04/29/privacy-and-machine-learning.html> accessed 13 March 2019.

[117] Ibid.

machine learning algorithms are created based on the privacy by design principle, that they employ a DPO, complete a DPIA for all new machine learning algorithms produced, and overall that they are accountable for the work that they do. It is important, however, to end this paper with a consideration of how artificial intelligence and machine learning more specifically should be regulated in general. Some have suggested that there be new forms of regulation for artificial intelligence.[118] Morley and Lawrence uphold that there is a crucial need for the Government to regulate.[119] However, specifically with machine learning, it is difficult for the government to legislate in a way that would apply to all types of machine learning. Moreover, it is likely that if the Government were to regulate in a reactive way that it would curb the development of new technologies.[120]

The Law Society of England and Wales argues that it is important to wait for machine learning to continue to develop before its form and arising consequences can be fully understood.[121] It can therefore be argued that the existing laws should be enough to cover machine learning algorithms and artificial intelligence more generally. The GDPR, and Article 17 more specifically, provides extensive protection for an individual's data rights. The Government creating a set of regulations specifically to regulate machine learning in the interest of protecting personal data rights would ultimately be risky. These technologies are continuing to advance and change, and any form of specific regulation would struggle to keep up with how quickly technology is altering. It is impossible to know what new personal data protection risks may arise in a few years' time. Thus, the GDPR provides adequate protection for personal data rights when data controllers and processors

[118] Select Committee on Artificial Intelligence, (n 5), 114.

[119] Select Committee on Artificial Intelligence, *Future Technology - Written Evidence Volume* (AIC0024, 2018), 848.

[120] Select Committee on Artificial Intelligence, (n 5), 113.

[121] Select Committee on Artificial Intelligence, (n 119).

are held accountable for compliance, and for now is the best form of regulation for machine learning.

Conclusion

It may be difficult for Article 17 requests to be fulfilled by companies using machine learning algorithms but it has been shown that there are sufficient provisions within the GDPR for companies to ensure that they can enforce the right to erasure. These include anonymising the data, hiring a DPO, completing a DPIA, and ensuring complete compliance with all GDPR provisions. It has been argued in this paper that through the control that Article 17 gives to individuals over their data, it enhances the protection of personal data that is processed by machine learning algorithms to an essential degree. Article 17 is an important aspect of data protection that needs to be enforced. This was made evident through an examination of Article 17, the amount of personal data that is shared online, and the way in which Article 17 works to enhance data protection in conjunction with other GDPR provisions. As individuals become more aware of the ways that different organisations utilise their data, it is perhaps best if companies use the GDPR, and Article 17 more specifically, as an opportunity to compete for consumers on the basis of data protection.

BIBLIOGRAPHY

Cases

C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) 317;

Legislation

Charter of Fundamental Rights and Freedoms of the European Union [2000] OJ C364/01;

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR);

Council Directive (EC) 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive);

Data Protection Act 2018;

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/04 (General Data Protection Regulation);

Treaty on the Functioning of the of the European Union (TFEU);

Books

Fuster G, *The Emergence of Personal Data Protection as a Fundamental Rights of the EU* (Springer International Publishing, 2014);

Jones ML, *Ctrl + Z: The Right to Be Forgotten* (NYU Press, 2018);

Mayer-Schönberger V, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009);

Siegel E, *Predictive Analysis: the Power to Predict who will click, buy, lie, or die* (John Wiley & Sons, 2013);

Solove DJ, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press, 2007);

Witten I and others, *Data Mining: Practical Machine Learning Tools and Techniques* (Morgan Kaufmann, 2016);

Contribution to Edited Books

Markou C, "The '*Right to Be Forgotten':* Ten Reasons Why It Should Be Forgotten" in Gutwirth S, Leenes R, and de Hert P (eds), *Reforming European Data Protection Law,* (Springer Publishing, 2014);

Porcedda MG, "On Boundaries – Finding the Essence of the Right to the Protection of Personal Data" in De Hert P, Gutwirth S, Leenes R, and van Brakel R (eds), *Data Protection and Privacy: The Internet of Bodies,* (Hart Publishing, 2018);

European Commission Publications

European Commission, 'Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation' (2018);

European Commission, 'Artificial Intelligence for Europe' (2018);

Government Publications

Information Commissioner's Office, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (2.2, 2017);

Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)* (1. 0. 248, 2018);

Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?* (HL 100, 2018);

Select Committee on Artificial Intelligence, *Artificial Intelligence to Improve the UK's Health and Social Care* (HL AIC0060, 2018);

Select Committee on Artificial Intelligence, *Future Technology - Written Evidence Volume* (HL AIC0024, 2018);

Journal Articles

Ambrose LM, 'You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship' (2012) 17 (7) International Review of Information Ethics 21;

Bakken D and others, 'Data obfuscation: anonymity and desensitization of usable data sets' (2004) 2 (6) IEEE Security & Privacy 34;

Beckett P, 'GDPR compliance: your tech department's next big opportunity' (2017) 5 Computer Fraud & Security 9;

Benndorf V and Normann H, 'The willingness to sell personal data' (2017) 120 (4) The Scandinavian Journal of Economics 1;

Beresford A, Kubler D, Preibusch S, 'Unwillingness to pay for privacy: a field experiment' (2012) 117 (1) Economics Letters 25;

Blanchette J and Johnson D, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness' (2002) 18 (1) The Information Society 33;

Brynjolfsson E and Mitchell T, 'What can machine learning do? Workforce implications' (2017) 358 (6370) Science 1530;

Burkell JA, 'Remembering me: big data, individual identity, and the psychological necessity of forgetting' (2016) 18 Ethics and Information Technology 17;

Cofone I, 'Google v. Spain: A Right to Be Forgotten?' (2015) 15 (1) Chicago-Kent Journal of International and Comparative Law 1;

De Hert P and Papakonstantinou V, ‘The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?’ (2016) 32 (2) Computer Law & Security Review 179;

Dwork C, ‘Differential privacy’ (2006) 4052 Automata, Languages, and Programming 1;

Elzweig M, Gandhi A, Lee S, and Serrato JK, ‘Navigating Personal Data Rights in an Increasingly Digital and Machine World’ (2018) 1 (4) Journal of Financial Compliance 357;

Esposito E, ‘Algorithmic Memory and the Right to be Forgotten’ (2017) 4 (1) Big Data & Society 1;

Guihot M, Matthew A, and Suzor N, ‘Nudging Robots: innovative solutions to regulate artificial intelligence’ (2017) 2 Vanderilt Journal of Entertainment & Technology Law 386;

He W, Li H, and Yu L, ‘The Impact of GDPR on Global Technology Development’ (2019) 22 (1) Journal of Global Information Technology Management 1;

Holzinger A, Kieseberg P, Malle B, and Weippl E, ‘The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases’ (2016) 9817 Lecture Notes in Computer Science 251;

Isaak J and Hanna M, ‘User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection’ (2019) 51 (8) Computer 56;

Jamali M and others, ‘Social media data and post-disaster recovery’ (2019) 44 International Journal of Information Management 25;

Jordan M and Mitchell T, ‘Machine Learning: trends, perspectives, and prospects’ (2015) 349 (6145) Science 255;

Kuner C and others, ‘Expanding the artificial intelligence – data protection debate’ (2018) 8 (4) International Data Privacy law 289;

Kuner C and others, ‘Machine learning with personal data: is data protection law smart enough to meet the challenge?’ (2017) 7 (1) International Data Privacy Law 1;

Li Q, Cao G, La Porta T, ‘Efficient and Privacy-Aware Data Aggregation in Mobile Sensing’ (2014) 11 (2) IEEE Transactions on Dependable and Secure Computing 115;

Lim S and others, ‘Consumer valuation of personal information in the age of big data’ (2017) 69 (1) Journal of the Association for Information Science and Technology 60;

Malle B, Kieseberg P, and Holzinger A, ‘Interactive Anonymization for Privacy aware Machine Learning’ (2017) Institute for Medical Informatics, Statistics & Documentation 15;

Monfort M and others, ‘Moments in Time Database: one million videos for event understanding’ (2019) IEEE Computer Society 1;

Moreno J and others, ‘Neuralyzer: A Security pattern for the Right to be Forgotten in Big Data’ (2018) 24 Pattern Languages of Programs 1;

Obar J and Oeldorf-Hirsch A, ‘The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services’ (2018) Information Communication and Society 1;

Politou E and others, ‘Backups and the right to be forgotten in the GDPR: An uneasy relationship’ (2018) 34 (6) Computer Law & Security Review 1247;

Politou E, Alepis E, and Patsakis C, ‘Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions’ (2018) 4 (1) Journal of Cybersecurity 1;

Reed C, ‘How should we regulate artificial intelligence?’ (2018) 376 (2128) Phil Trans R Soc 1;

Riedl M, ‘Human-centered artificial intelligence and machine learning’ (2019) 1 (1) Human Behaviour and Emerging Technology 1;

Rosen J, ‘Free speech, privacy, and the web that never forgets’ (2011) 9 Telecommunications and High Technology Law 345;

Rosen J, ‘The right to be forgotten’ (2011) 64 Stanford Law Review 88;

Spiekermann S and others, ‘The challenges of personal data markets and privacy’ (2015) 25 Institute of Information Management 161;

Sweeney L, ‘K-Anonymity: a model for protecting privacy’ (2002) 10 (5) International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 557;

Tsesis A, ‘Data subjects’ privacy rights: regulation of personal data retention and erasure’ (2019) 90 University of Colorado Law Review 593;

Turing A, ‘Computing Machinery and Intelligence’ (1950) 49 Mind 433;

Weber RH, ‘The Right to be Forgotten: More Than a Pandora’s Box?’ (2011) 1 (2) Journal of Intellectual Property, Information Technology and Electronic Commerce 120;

Journal Articles (Online)

Binns R, Edwards L, and Veale M, ‘Algorithms that remember: model inversion attacks and data protection law’ (2018) The Royal Society <https://doi.org/10.1098/rsta.2018.0083> accessed 18 February 2019;

Kieseberg P, Li T, and Villaronga EF, ‘Humans Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten’ (2017) Computer Law and Security Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018186> accessed 10 October 2018;

Other Print Sources

Centre for Information Policy Leadership, *Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice,* (Centre for Information Policy Leadership, 2018);

Centre for Information Policy Leadership, *Learning from the EU GDPR: What elements should the US Adopt?,* (Centre for Information Policy Leadership, 2019);

Kearns M, *Data Intimacy, Machine Learning, and Consumer Privacy,* (University of Pennsylvania Law School, 2018);

Kurtz C and others, *The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems,* (Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019);

Norwegian Data Protection Authority, *Artificial Intelligence and Privacy,* (Datatilsynet, 2018);

World Economic Forum, *Personal Data: The Emergence of a New Asset Class,* (World Economic Forum, 2011);

<u>Other Online Sources</u>

Cadwalladr C, 'The great British Brexit robbery: how our democracy was hijacked' (*The Guardian,* 2017) <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> accessed 18 March 2019;

Goodfellow I and Papernot N, 'Privacy and machine learning: two unexpected allies?' (*Cleverhans Blog,* 2018) <http://www.cleverhans.io/privacy/2018/04/29/privacy-and-machine-learning.html> accessed 13 March 2019;

Haag M, 'Woman Who Was Fired for Giving Trump the Middle Finger Sues Former Employer' (*The New York Times,* 2018) <https://www.nytimes.com/2018/04/05/us/juli-briskman-middle-finger-trump.html> accessed 7 March 2019;

Hern A, 'Cambridge Analytica: how did it turn clicks into votes?' (*The Guardian,* 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 28 February 2019;

Love D, '13 People Who Got Fired for Tweeting' (*Business Insider,* 2011) < https://www.businessinsider.com/twitter-fired-2011-5?r=US&IR=T> accessed 7 March 2019;

Rosen J, 'The Web Means the End of Forgetting' (*The New York Times Magazine,* 2010) <https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html> accessed 11 March 2019;

Wagstaff K, 'You'd need 76 work days to read all your privacy policies each year' (*Time,* 2012) <http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/> accessed 12 February 2019;

Watts M and Macalister Hall E, 'Data Protection in the UK (England and Wales): overview' (*Thomson Reuters Practical Law,* 2019) <https://uk.practicallaw.thomsonreuters.com/w-012-9556?comp=pluk&transitionType=Default&contextData=(sc.Default)> accessed 15 February 2019;

Winter J, ‘The Advantages of Amnesia’ (*The Boston Globe,* 2007) <http://archive.boston.com/news/education/higher/articles/2007/09/23/the_advantages_of_amnesia/> accessed 18 March 2019.