Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 34 | Issue 4 Article 3

5-3-2018

Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence

Humerick, Matthew

Follow this and additional works at: https://digitalcommons.law.scu.edu/chtlj

Part of the Intellectual Property Law Commons, and the Science and Technology Law Commons

Recommended Citation

Humerick, Matthew, *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, 34 Santa Clara High Tech. L.J. 393 (2018).
Available at: https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized editor of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com, pamjadi@scu.edu.

TAKING AI PERSONALLY: HOW THE E.U. MUST LEARN TO BALANCE THE INTERESTS OF PERSONAL DATA PRIVACY & ARTIFICIAL INTELLIGENCE

***Matthew Humerick*†**

The race to develop artificial intelligence has begun, where countries are heavily backing efforts to be the world leader. While this technology promises to create a smarter, autonomous world, it is not without its concerns. Perhaps most prevalent are concerns regarding consumer personal data privacy and protection. While nations worldwide have adopted varying degrees of personal data protection, the European Union has established itself as the leader on this front. Soon, the European Union will implement its most comprehensive regulation yet on consumer personal data privacy and protection: the General Data Protection Regulation ("GDPR"). However, several aspects of this Regulation pose concerns as to the impact of its enforcement on the algorithms and machine learning required for the development of artificial intelligence. Until these concerns are addressed, it remains to be seen whether artificial intelligence can be developed in the European Union in compliance with the new GDPR's provisions.

† Matthew Humerick holds a J.D. from Michigan State University College of Law (class of 2018) and will sit for the Massachusetts Bar in July of 2018.

TABLE OF CONTENTS

INTRODUCTION

Technology is continuously evolving to create a smart, autonomous world. At the forefront of this technological revolution is the innovation of artificial intelligence ("AI"). As stated by Russian President Vladimir Putin, "[w]hoever becomes the leader in [artificial intelligence] will become the ruler of the world."[1] President Putin's words express the breadth of concern to which many have over the rapid expansion of this sort of super-intelligence.[2] However, whether or not AI is a concern, its exponential development and use may soon stall as the European Union ("E.U.") prepares to implement its General Data Protection Regulation ("GDPR") on May 25, 2018.[3]

While AI is subject to different definitions, it is generally understood to consist of machine learning, based on algorithms that collect, process, and adapt to data from the real world.[4] AI cannot thrive without a steady supply of data to expand its knowledge base. To supplement its development, controllers collect vast amounts of consumer personal data to enable algorithms to learn. Algorithms cannot accurately learn from its environment without large amounts of personal data. Instead, companies collect, store, process, and maintain large sets of consumer data. As a result, data privacy and protection have become cause for greater concerns for companies and governments alike. Enter the E.U.'s GDPR.

The GDPR emphasizes consumer control over personally identifiable information ("PII"), which creates stricter legal and operational obstacles for those seeking to control and process it.[5] The

[1] David Meyer, *Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World*, FORTUNE (Sept. 4, 2017), http://bit.do/Meyer_Putin (citing a recent quote by Vladimir Putin when discussing the concept of artificial intelligence and its impact on the world).

[2] *See* Maureen Dowd, *Elon Musk's Billion-Dollar Crusade to Stop the AI Apocalypse*, VANITY FAIR (Apr. 2017), http://bit.do/Dowd_Elon-Musk. Elon Musk, arguably one of the greatest innovators of the 21st Century, has openly combatted the rise of AI along with only highly-regarded minds, such as Stephen Hawking and Bill Gates. *Id.* This article discusses Musk's concerns over the development of AI and how its ability to learn from humans, only to outthink them, casts a grim outlook on humanity's future. *Id.*

[3] *GDPR Portal: Site Overview*, EU GDPR, http://bit.do/EUGDPR (last visited Oct. 2, 2017) [hereinafter *GDPR Portal*].

[4] *See* Jordan Novet, *Everyone Keeps Talking About AI – Here's What It Really Is and Why It's So Hot Now*, CNBC (June 17, 2017), http://bit.do/Novet_AI (citing the first scholarly definition of AI, as defined in 1956 by John McCarthy, a math professor at Dartmouth College, who defined AI as "every aspect of learning or any other feature of intelligence [that] can in principle be so precisely described that a machine can be made to simulate it"). Nowadays, AI has developed to include terms, such as "machine learning" and "deep learning," which describe the complexity of technological processes used to collect and utilize data. *Id.*

[5] *See Guide to the General Data Protection Regulation (GDPR)*, INFO. COMM'R'S OFFICE, http://bit.do/ICO_Overview (last visited Oct. 4, 2017).

GDPR codifies several E.U. consumer rights in PII that cannot coexist with AI, including: the requirement of explicit consent, the right of erasure, the right to explanation of automated decisions, and data portability rights.[6] While these aforementioned rights are only afforded to E.U. citizens, the territorial scope of the GDPR applies to those processing this protected data, wherever they may be located or established.[7] As a result, business leaders and legislatures across the globe must address these compliance issues to determine whether they can lawfully sustain AI development under the GDPR. To remain competitive within the AI field, the E.U. must find a way to balance its interest in data privacy against those in the advancement of AI.

Part I of this Comment provides an overview of what AI is and how it utilizes personal data to develop. Contained within Part I is also a brief overview of the current international AI situation and how the E.U.'s relevance is rapidly declining. Part II discusses data privacy and AI law within the European Union, and how new regulations may adversely impact sustained algorithmic development under the current AI model. Part III proposes two courses of action on how the E.U. should adapt its views on data privacy and protection to better facilitate the use and development of AI.

I. WHAT IS ARTIFICIAL INTELLIGENCE?

At its most basic level, AI is "a system that can learn how to learn."[8] Humans write initial algorithms for a system that enables the computer to subsequently write its own algorithms, without additional human oversight or interaction.[9] This process allows AI to continuously learn from, and solve new problems within, an ever-changing environment, based on its continuing collection of data.[10] While AI may seem straightforward by this definition, there are

[6] *See* Bernard Marr, *New Report: Revealing the Secrets of AI or Killing Machine Learning?*, FORBES (Jan. 12, 2017), http://bit.do/Marr_New-Report; *see also* Rand Hindi, *Will Artificial Intelligence Be Illegal in Europe Next Year?*, ENTREPRENEUR (Aug. 9, 2017), http://bit.do/Hindi_AI-illegal.

[7] *See* Regulation 2016/679, of the European Parliament and of the Council 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 (General Data Protection Regulation), arts. 1-3, 2016 O.J. (L 119) 32, 33 [hereinafter GDPR].

[8] FRANCESCO COREA, ARTIFICIAL INTELLIGENCE AND EXPONENTIAL TECHNOLOGIES: BUSINESS MODELS EVOLUTION AND NEW INVESTMENT OPPORTUNITIES 1-2 (2017).

[9] *Id.* at 2.

[10] *Id.* "While human being actions proceed from observing the physical world and deriving underlying relationships that link cause and effect in natural phenomena, an artificial intelligence is moved entirely by data and has no prior knowledge of the nature of the relationship among those data." *Id.*

numerous definitions and types of AI. Additionally, because of its continuously learning nature, AI is expected to develop tremendously over the next decade, making the impact of the GDPR even more significant.

A. Big Data, Machine Learning, and AI

Big data supplies the basis for AI by supplying the environment from which it is able to learn. While, like AI, no single definition exists, companies and organizations commonly define "big data" as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[11] Under this construction, its three V's conceptualize big data, where "volume relates to massive datasets, velocity relates to real-time data and variety relates to different sources of data."[12] This concentration of data includes an abundance of information, ranging from PII to anonymous data collections, such as Internet of Things devices,[13] machine logs, or company reference data collections.[14] This supply of big data is instrumental to AI's machine learning.

Intel, a leading company in AI development, defines machine learning as "the set of techniques and tools that allow computers to 'think' by creating mathematical algorithms based on accumulated data."[15] While this is a broad definition, machine learning functions through complex means. For example, there are two broad categories

[11] *Big Data*, GARTNER: IT GLOSSARY, http://bit.do/Gartner_Big-Data (last visited Apr. 28, 2018).

[12] *See Big Data, Artificial Intelligence, Machine Learning, and Data Protection*, INFO. COMM'R'S OFFICE, 1, 6 [hereinafter *Big Data*]. *But see* Sean Jackson, *Big Data in Big Numbers – It's Time to Forget the "Three V's" and Look at Real-World Figures*, COMPUTING (Feb. 18, 2016), http://bit.do/Jackson_3Vs (redefining "big data" in a way that emphasizes its presence here and now, rather than as a number or size).

[13] *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014), http://bit.do/Morgan_Simple-Explanation ("Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig.").

[14] *See* Ian Murphy, *Could AI Lead to Breaches of GDPR?*, ENTERPRISE TIMES (June 21, 2017), http://bit.do/Murphy_AI.

[15] *See* Deb Miller Landau, *Artificial Intelligence and Machine Learning: How Computers Learn*, IQ (Aug. 17, 2016), http://bit.do/Landau_AI. Through machine learning, AI undergoes a three-step process: "[S]tep one is perceiving the world, using data to detect patterns. Step two is recognizing those patterns, and step three is taking an action based on that recognition." *Id. See generally* ETHEM ALPAYDIN, INTRODUCTION TO MACHINE LEARNING *passim* (Thomas Dietterich et al. eds., 2d ed. 2010).

of machine learning: supervised and unsupervised.[16] With supervised learning, the AI processes and learns from labeled data sets to develop algorithms.[17] This supervised approach "trains" the algorithms to create models that can accurately map data inputs to outputs, which allows the algorithms to predict future events.[18] With supervised learning, it is easier for programmers and analysts to oversee and observe the AI's development. This additional control allows those overseeing the AI development to more easily follow its logic and introduce new data sets necessary for its continual processing. Conversely, unsupervised learning supplies the algorithms with no labels or prior input-output relationships, and instead leaves the algorithms on its own to learn.[19] Machine learning is also categorized based on the depth of its learning.

The depth of machine learning is either shallow or deep. Typically, shallow learning is less utilized because it only involves one layer of data, which limits the amount of data that AI can use to expand its knowledge.[20] Alternatively, deep learning involves the use of algorithms, modeled after the human brain, to create multiple layers of neural networks.[21] Such neural networks allow data to be clustered, classified, and recognized as larger patterns, which can then be modeled to predict future tendencies and events.[22] This simplistic overview illustrates how AI incorporates vast amounts of data to teach its algorithms to learn in a way that builds connections between seemingly unrelated data.

B. AI, its Expected Development, and the E.U.

Because many countries share Vladimir Putin's sentiment towards AI,[23] experts predict rapid expansion in AI research and development over the next decade. Currently, the leaders in this field

[16] *See also Big Data*, *supra* note 12, at 7.

[17] *Id.*

[18] *Id.* at 8.

[19] *Id.*

[20] *See* Jürgen Schmidhuber, *Deep Learning in Neural Networks: An Overview*, 61 NEURAL NETWORKS 85, 86-87 (2015).

[21] *See id.*; COREA, *supra* note 8, at 12-13. *See also id.* at 13 ("There exist many types of ANNs [artificial neural networks] . . . but the most known ones are Recurrent Neural Networks (RNNs); Convolutional Neural Networks (CNNs); and Biological Neural Networks (BNNs)); *Introduction to Deep Neural Networks*, DEEPLEARNING4J, http://bit.do/DeepLearning4J_Intro (last visited Oct. 13, 2017).

[22] *See* sources cited *supra* note 21.

[23] *See* Dave Gershgorn, *AI is the New Space Race. Here's What the Biggest Countries are Doing*, QUARTZ (May 2, 2018), http://bit.do/Greshgorn_AI; Meyer, *supra* note 1.

are the United States, China, and India.[24] In what is becoming a technical arms race, these three leaders have taken different approaches to developing AI: the United States relies heavily on the efforts of individual companies; China's government funds AI research; and, India relies on its work through its $143 billion outsourcing industry.[25] These leaders share similar aspects with regard to balancing interests in AI and data privacy. In each country, the respective government facilitates AI advancement by either encouraging, or minimally interfering with, its development. Additionally, personal data is either not overly regulated or, the use of personal data for AI purposes is separate and distinct from other data privacy and protection regulations.

While the E.U. attempts to assert itself as a leading AI entity,[26] the United Kingdom (U.K.) dominates the region's research and development.[27] Although Europe is currently a pioneer in the advancement of AI, it is largely because the U.K. makes up the majority of its efforts.[28] However, in a recent move commonly known as "Brexit,"[29] the U.K. voted to leave the E.U., thus potentially affecting the E.U.'s status in the AI field.[30] While there were numerous

[24] *See* Rishi Iyengar, *These Three Countries are Winning the Global Robot Race*, CNN (Aug. 21, 2017), http://bit.do/Iyengar_3-countries.

[25] *Id.* China's government is perhaps the largest proponent of AI development, as demonstrated by its plans to become the world leader of AI in 2030 through a $150 billion-dollar plan. *Id. See also* Sherisse Pham, *China Wants to Build a $150 Billion AI Industry*, CNN (July 21, 2017), http://bit.do/Pham_China.

[26] *See* European Commission Press Release IP/18/3362, Artificial intelligence: Commission outlines a European approach to boost investment and set ethical guidelines (Apr. 25, 2018) (detailing a recent collaborative effort amongst E.U. Member States to invest "at least €20 billion [in AI investments and research] by the end of 2020"); *see also* Tania Rabesandratana, *With €1.5 Billion for Artificial Intelligence Research, Europe Pins Hopes on Ethics*, SCI. (Apr. 25, 2018, 12:35 PM), http://bit.do/Rabesandratana (commenting on the E.U.'s recent plans to invest in AI and how various issues remain unaddressed).

[27] *See* Simon Baker, *Which Countries and Universities Are Leading on AI Research*, TIMES HIGHER EDUC. (May 22, 2017), http://bit.do/Baker_AI-research; Fabian, *The European Artificial Intelligence Landscape | More Than 400 AI Companies Built in Europe*, ASGARD (July 31, 2017), http://bit.do/Fabian_European-AI (showing that the majority of AI startups in the E.U. are located within London (97), compared to the next closest city, Berlin (30)).

[28] *See* Fabian, *supra* note 27 (discussing how the U.K. has "by far the strongest AI ecosystem" in Europe, including five of Europe's top ten funded AI companies). Since 2005, Europe has submitted the third-most AI-related patent applications, trailing behind only the U.S. and China. *China May Match or Beat America in AI*, ECONOMIST (July 15, 2017), http://bit.do/Economist_China-match-beat. At the same time, Britain has more than double the amount of AI companies than that of any other European country, ranking at third overall and followed by Germany at seventh. *Id.*

[29] Alex Hunt & Brian Wheeler, *Brexit: All You Need to Know About the UK Leaving the EU*, BBC (Apr. 12, 2018), http://bit.do/Hunt_Brexit.

[30] *See* Rachel Pells, *UK and Europe 'Must Join Forces' on AI Research Despite Brexit*, TIMES HIGHER EDUC. (May 3, 2018), http://bit.do/Pells_Brexit (discussing the U.K.'s expertise

reasons for and against the U.K.'s decision to part from the E.U.—not discussed in this Comment—a commissioned report to the U.K. Parliament projects that AI could lead to a £630 billion boon in the U.K.'s economy by 2035.[31] Presumably, the U.K. will use its exit from the E.U. to develop its own laws for data privacy and AI in a timelier and more efficient fashion than the E.U., so as to seize this competitive advantage.[32] Not only will Brexit call into question the GDPR's applicability and territorial scope, but the U.K. will also use less restrictive provisions to better balance the interests of consumer data privacy rights with AI.[33] Similar to the actions of the United States, China, and India, the U.K. plans to balance consumer interests with AI interests rather than overregulating one or the other.[34]

While Brexit may ultimately lead to a boon in the U.K.'s AI efforts, the E.U.'s AI industry will suffer greatly from the loss of the U.K. The E.U should encourage AI efforts so that it remains competitive in the technological arms race. However, the provisions of the GDPR may be the primary inhibiting factor in the development of AI by remaining E.U. Member States and, if unaddressed, may lead to future departures by Member States.[35] Whereas the top AI countries have minimally regulated AI and the use of PII in big data, the E.U.'s GDPR creates heightened standards for PII.[36] Ultimately, the E.U., through its efforts to become the world-leader in consumer data

in AI research and why it is necessary for the E.U. and the U.K. to collaborate their efforts in order to remain competitive in the AI sector).

[31] *See* DAME WENDY HALL & JÉRÔME PESENTI, DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT AND DEPARTMENT FOR BUSINESS, ENERGY & INDUSTRIAL STRATEGY, GROWING THE ARTIFICIAL INTELLIGENCE INDUSTRY IN THE UK, 2017, at 1-2; Sam Shead, *A New Report Tells the Government How It Can 'Supercharge' AI*, BUS. INSIDER (Oct. 14, 2017, 7:01 PM), http://bit.do/Shead_Supercharge-AI.

[32] *See* sources cited *supra* note 31.

[33] *See* sources cited *supra* note 31.

[34] *See* HALL & PESENTI, *supra* note 31, at 5, 66-74 (arguing that while regulation is necessary, the report recommends that the industry and government work collaboratively to establish a U.K. AI Council that oversees, rather than curbs, the development of AI).

[35] While this is only speculative, support for the E.U. has declined in nearly all of its Member States. *See* Rebecca Flood, *REVEALED: Which Countries Could Be Next to Leave the EU?*, EXPRESS (last updated Oct. 2, 2016, 2:34 PM), http://bit.do/Flood_Next-to-leave (quoting a joint statement issued after the Brexit vote by the foreign ministers of prominent Member States, "We are aware that discontent with the functioning of the EU as it is today is manifest in parts of our societies . . . . We take this very seriously and are determined to make the EU work better for all our citizens.). Were the E.U. to incidentally hinder the use and development of AI in comparison to the rest of the developing world, it is possible that additional Member States will contemplate exits so as not to fall behind.

[36] *See* Nick Wallace & Daniel Castro, Center for Data Innovation, The Impact of the EU's New Data Protection Regulation on AI 1-4, 25-27 (2018), http://bit.do/Wallace_Impact.

privacy, may be posturing itself out of relevancy in the race to develop AI.

II. E.U. DATA PRIVACY & AI LAW

The European Union is the world leader in setting consumer data privacy standards. In fact, the E.U. considers data privacy a fundamental right for its citizens.[37] Article 8 of the E.U.'s Charter of Fundamental Rights provides E.U. citizens four main data privacy rights, including the right to: protection of personal data, fair data processing, access and rectification of collected data, and compliance of data protection laws.[38] With this mindset, the E.U. voted to replace its existing Data Protection Directive (DPD)[39] with the more onerous GDPR, which is set for implementation on May 25, 2018.[40] However, the GDPR does not specifically address AI, though the primary current model of AI is directly within the GDPR's scope.[41] Accordingly, the E.U. is beginning discussions on legislative proposals to specifically address AI.[42] Until the E.U. implements these measures, there remains a high likelihood that current AI models are in direct violation of the GDPR, which may significantly impact worldwide AI development efforts.

[37] *See* Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) [hereinafter Charter]. While Article 7 of the Charter of Fundamental Rights, *id.* art. 7, provides a general right to respect one's private communications, Article 8, *id.* art. 8, explicitly addresses the protection of personal data.

[38] Charter, *supra* note 37, art. 8.

[39] *See* Directive 95/46/EC, of the European Parliament and of the Council 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 O.J. (L 281) 31 [hereinafter DPD]. As a Directive, the DPD held less authority on the E.U. Member States where each could "determine more precisely the conditions under which the processing of personal data is lawful." *Id.* art. 5. However, because the DPD is only a directive, its authority was limited to setting minimum standards rather than prescribing a uniform standard of regulation like the way the GDPR will. *See* Courtney M. Bowman, *A Primer on the GDPR: What You Need to Know*, PROSKAUER (Dec. 23, 2015), http://bit.do/Bowman_Primer; DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 849, 1135 (Erwin Chemerinsky et al. eds., 5th ed. 2015).

[40] *GDPR Portal*, *supra* note 3.

[41] *See* Sven Jacobs & Christoph Ritzer, *Data Privacy: AI and the GDPR*, NORTON ROSE FULBRIGHT: DATA PROTECTION BLOG (Nov. 2, 2017), http://bit.do/Jacobs_DataPrivacy.

[42] European Parliament Press Release 20170110IPR57613, Robots: Legal Affairs Committee calls for EU-Wide Rules (Jan. 12, 2017). While there is recognition in the E.U. that it must promulgate AI laws, discussions have mostly centered on robotics and its potential liabilities but not how to develop AI.

A. The Scope of the General Data Protection Regulation ("GDPR")

The GDPR grants extensive data privacy and protection rights to E.U. citizens, particularly through its material[43] and territorial[44] scope provisions. The Regulation broadly defines "personal data" to mean:

> [A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[45]

Important within the definition are the terms "identified," "identifiable," "directly," and "indirectly." Rather than setting limiting parameters on the applicable data, such as that which would only directly identify a natural person, the definition broadens the material scope of the Regulation. Additionally, the GDPR defines "processing" as:

> [A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;[46]

Together, the definitions of "personal data" and "processing" serve to expand the material scope of the GDPR, which further expands the already liberal interpretation of data privacy laws by the E.U. courts.

[43] GDPR, *supra* note 7, art. 2. Subject to a few narrow exceptions in subsection (2) of Article 2, the GDPR's material scope is "to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." *Id.* art. 2(1).

[44] *Id.* art. 3. According to the GDPR, its scope "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." *Id.* art. 3(1). In addition, the rest of the article expands the GDPR's territorial scope to those controllers and processors not established in the union generally, and to those where Member State law applies through public international law. *Id.* arts. 3(2)-(3).

[45] *Id.* art. 4(1). Not elsewhere defined in the GDPR, a "data subject" is an "identified or identifiable natural person." *Id.*

[46] *Id.* art. 4(2).

Even prior to the GDPR, the European Court of Justice (ECJ), the E.U.'s highest court, liberally read data privacy laws where personal data may be processed or at risk through a convoluted process. For example, on October 19, 2016, the ECJ heard a case that involved the German government and its practice of capturing dynamic IP addresses.[47] Here, the ECJ broadly interpreted the DPD to protect certain IP addresses because controllers could "likely reasonably" compare their data with a third-party's separate system, which contains identifying information, to identify individual users.[48] By broadly holding that seemingly anonymous information can be identifying if possibly used by a third-party, the ECJ demonstrated a liberal interpretation of data protection policies. Since this broad holding occurred under the less exhaustive DPD, it is fair to speculate that there will almost be a presumption of violation in the more restrictive, but broadly defined, GDPR.

In addition to its material scope, the GPDR attempts to create international law through an expansive territorial scope.[49] According to Article 3, the GDPR applies to controllers or processors who process the personal data of E.U. citizens, and who are: (1) established in the E.U.;[50] (2) not established in the E.U., but the activities concern data subjects in the E.U.;[51] and, (3) to those subject to Member State law.[52] While Article 3's broad territorial scope is likely to face legal challenges by non-E.U. companies and countries prosecuted under this

[47] *See* Case C-582/14, Breyer v. Bundesrepublik Deutschland, 2016 E.C.R. II-779. A dynamic IP address is an IP address assigned to a device when using a public network or internet service that changes each time the user reconnects. This practice allows a single user to a new IP address each time a page is reconnected to.

[48] *Id.* Here, the German government collected reported PII when users logged into its system while a separate system captured IP addresses. These captured IP addresses were not logged as PII; however, because an in-depth comparison of the two systems could ultimately identify a user, the ECJ found that consumer data could be traced back to an individual.

[49] *See* GDPR, *supra* note 7, art. 3.

[50] *Id.* art. 3(1). The first territorial component of Article 3 states that the GDPR "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." *Id.*

[51] *Id.* art. 3(2). The second territorial provision of Article 3 states that the GDPR

> applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Id.

[52] *Id.* art. 3(3). The final territorial provision of Article 3 states that the GDPR "applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law." *Id.*

jurisdictional component, on its face the GDPR applies to any processing of personal data not subject to Article 2's exceptions.[53] Importantly, organizations must determine (1) whether they are a "controller"[54] or "processor,"[55] under the GDPR; (2) whether their operations involve the "processing of personal data;"[56] and, (3) whether they have measures in place to comply with the GDPR.[57] While issues one and two are more easily discernable, companies and organizations continue to scramble to understand what the GDPR entails and whether they are in compliance.[58] Organizations cannot guarantee compliance with the GDPR, especially for AI, where the data encompassed within big data fields can often trace back to individuals.

While the intent of the GDPR is to ease data processing through uniform data privacy and protection standards,[59] its rapid implementation, coupled with its high standards, threaten to result in tremendous liability risks for data controllers and processors worldwide. Specifically, based on the existing AI development models, machine learning and big data will cause organizations worldwide to fall under the scope of the GDPR, whether they know it or not. This potential for liability would be even greater in unsupervised AI models, which inherently have minimal to no human oversight. Once deemed within its scope, organizations will need to comply with the GDPR's provisions, which is easier said than done. Even if located outside of the E.U., Article 3 presumably may hold anyone liable, especially those controllers interested in conducting business with companies either within the E.U., or who trade with E.U.-based companies. If held liable, companies stand to face severe penalties in the form of "administrative fines up to 20[,]000[,]000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."[60] The penalties alone may dissuade the

[53] *Id.* art. 3.

[54] *Id.* art. 4(7). A "controller" is

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Id.

[55] *Id.* art. 4(8). A "processor" is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." *Id.*

[56] *Id.* art. 3.

[57] *See id.* at 39-41.

[58] *See, e.g.*, Bob Violino, *Many Firms Clueless on How to Prepare for GDPR*, INFO. MGMT. (July 3, 2017, 7:09 AM), http://bit.do/Violino_Clueless.

[59] *See* GDPR, *supra* note 7, at 1-3.

[60] *Id.* art. 83(5). An "undertaking" is not defined by the GDPR or within Articles 101 or

development of AI by certain organizations. There are several provisions in particular that threaten to impede the development of AI because its current development model does not comply with the GDPR's provisions: (1) the right to consent; (2) the right to be forgotten (erasure); (3) the right to data portability; and (4) the right to explanation.[61]

1. Right to Consent

While the GDPR outlines several means by which the processing of personal information is lawful, the primary method for lawfully processing consumer PII is through explicit consent for one or more specific purposes.[62] The E.U. adopts an opt-in approach to data privacy, meaning that controllers may only process personal data if the data subject unambiguously consents.[63] Under Article 7, the burden is on the controller to prove that the data subject unambiguously and freely consented, among other conditions.[64] Additional burdens exist with regard to children.[65] Under the GDPR, a child under the age of 16 cannot give consent, though individual Member States may lower the age down to thirteen.[66] A controller may mitigate its liability by making "reasonable efforts" to verify consent, either by the parent or through the child's age, but these efforts must take into account available technology.[67] However, the GDPR does not define "reasonable efforts" and, because available technology must be taken into account, this may heighten the scrutiny placed upon controllers and processors by the

102 of the Treaty, which are cited within the GDPR, *see* 2012 O.J. (C 326) 88, 89. Based on its use, it may be inferred to mean the actions of one or a collective group. *See id.*

[61] *See* GDPR, *supra* note 7, arts. 7, 13(f), 14(g), 15(h), 17, 20-22.

[62] *Id*. arts. 6-7.

[63] "Consent" under the GDPR is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." *Id.* art. 4(11).

[64] *See id.* art. 7 (listing conditions on consent, such as how controllers must prove that consent was freely given).

[65] *Id.* art. 8 (Under the standards of Article 8, consent for children refers to "the offer of information society services directly to a child"). The GDPR cross-references the definition of the term "information society services" to Directive (EU) 2015/1535 of the European Parliament and of the Council, *id.* art. 4(25). This Directive defines the term broadly as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." Directive 2015/1535, of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, art. 1(b), 2015 O.J. (L 241) 1, 3 [hereinafter Information Society].

[66] *See* GDPR, *supra* note 7, art. 8(1). If a child is below the minimum age, only "the holder of parental responsibility over the child" may authorize consent. *Id.*

[67] *Id.* art. 8(2).

courts. While the process of simply receiving consent may be navigable, the greater obstacle is the right to withdraw consent.

Under Article 7, data subjects retain the right to withdraw consent *at any time*.[68] While controllers and processors may attempt to continue to process the data through other means of lawful processing,[69] such continued processing following withdrawn consent risks violating the GDPR.[70] Both the need for consent and the right withdraw consent threaten the development of AI because it could limit the amount of data available to learn from. Additionally, data subjects, in certain situations, can exercise a right to restrict the processing of their information.[71] For example, an organization may collect a large vat of big data for the sole purpose of machine learning. Assuming each data subject consented, this model of AI would be lawful and uninhibited, regardless of its methodology. Conversely, suppose a data subject, or a group of data subjects, withdraws consent. While the prior processing would be lawful, further processing of and learning from these specific data points would constitute a violation of the GDPR. Because AI continues to learn from past data, the issue becomes how to simultaneously stop AI's learning from this data, without impacting its prior development.

The current model of deep learning through neural networks demonstrates how AI's development hinges on utilizing multitudes of data to continuously adapt to the surrounding environment.[72] In theory, the withdrawal of consent, coupled by the continuation of learning through the processing of prior learned behaviors, would constitute a violation of the GDPR. For example, consider an AI system, which

[68] *Id.* art. 7(3).

[69] *See id.* art. 6(1).

[70] *See* Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 3 – Consent*, IAPP (Jan. 20, 2016), http://bit.do/Maldoff_10.

[71] *See* GDPR, *supra* note 7, art. 18. Under Article 18, a data subject may restrict a controller's processing of their PII when any one of the following situations applies:

> (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
>
> (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
>
> (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
>
> the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Id. art. 18(1).

[72] Roger Parloff, *Why Deep Learning is Suddenly Changing Your Life*, FORTUNE (Sept. 28, 2016, 5:00 PM), http://bit.do/Parloff_Learning.

uses a collection of data to learn how to respond to irate consumers through tonal tendencies. Then, one of the data subjects withdraws consent from the processing of its personal data, which in this case is their voice. While all prior learning would be valid under the GDPR, the AI could no longer use these specific data references to develop its algorithms. Presumably, the AI could no longer continue its learning through this data because any further processing of the learning would be a derivative of the original set containing the withdrawn data. Instead, the AI would need to receive new data to relearn its function, unless the processor could somehow isolate the strand of learning, which incorporated the now nonconsensual data. But, because the current AI model hinges around neural networks that interweave all sets of data, this isolation is unlikely to occur. It is likely that the GDPR's consent provision will result in either large scale AI regression or continual liability risks for those continuing to derive learnings from unlawfully processed information.

2. Right to be Forgotten (Erasure)

In addition to the right to give and withdraw consent, Article 17 of the GDPR grants data subjects the right to erasure.[73] Under Article 17, controllers have an "obligation" to erase all personal data, "without undue delay," when one of several conditions occur, including the withdrawal of consent.[74] Additionally, in instances where the data requested to be erased exists in the public domain, the controller is obligated to take reasonable steps to inform other controllers that the information, and any links or copies of it, must be erased.[75] By

[73] *See* GDPR, *supra* note 7, art. 17. In addition to a right to erasure, data subjects also have a right to the restriction of processing, *id.* art. 18, which, while not as potentially catastrophic, will lead to the same or similar cumbersome results.

[74] *Id.* art. 17. A controller must erase personal data when any of the following applies:

> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
>
> (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
>
> (d) the personal data have been unlawfully processed;
>
> (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
>
> (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Id. art. 17(1).

[75] *Id.* art. 17(2).

requiring all copies of the data to be erased, the potential detrimental impact on AI operations may span numerous controllers with a single exercise of the Article 17 right to be forgotten.

Similar to the right to consent, an exercise of the right to be forgotten stands to severely impair the development of AI. While controllers may easily identify individual strands of PII within a database and delete it, the erasure of personal data that is a part of a set of big data may impact the AI's accuracy and reliability. For example, when AI algorithms undergo the process of machine learning, they use the existing data to learn specific functions.[76] By deleting parts of the data, the future behaviors of the algorithms may not behave as they would have when the data was present, making it unstable, less reliable, and less accurate. For this reason, personal data utilized by AI, even when deleted, can arguably still remain integrated as part of the neural network.

One solution to the fear of unlawfully retaining personal data is for companies to retrain their existing AI models using the modified data set. However, this solution would result in the creation of AI that is constantly at risk of destruction. The AI would then have to relearn everything it had previously learned, which would result in additional research, development costs, and time delays.[77] In effect, the AI market within the E.U. would create additional risks, liabilities, and costs not associated with other global AI markets, which could cause companies to cease operations with, and within, the E.U.

Alternatively, companies can develop AI models to combat this issue by designing algorithms specifically to unlearn certain data inputs without needing to retrain the entire AI neural network. This approach requires increased research and development costs, additional time to build, and may still face GDPR compliance issues.[78] Though the logistics of forgetting information remain murky, companies need to develop operations that allow for the isolation and deletion of an individual's PII from a data set.

3. Right to Data Portability

Another hindrance for AI development exists through Article 20's right to data portability.[79] Article 20 gives data subjects two main rights: (1) the right to retrieve their personal data from a controller, and

[76] Parloff, *supra* note 72.

[77] WALLACE & CASTRO, *supra* note 36, at 11-13.

[78] *See generally* WALLACE & CASTRO, *supra* note 36 (discussing how the GDPR will inhibit the use and development of AI in Europe).

[79] GDPR, *supra* note 7, art. 20.

(2) the right to then transmit this data to another controller, without hindrance.[80] These rights allow data subjects to facilitate the spread of information, which may ease data collection efforts by smaller controllers. On the other hand, the right to portability poses similar problems to those inherent in the rights to consent and erasure.[81]

The right to portability requires that controllers maintain processes to identify and isolate an individual's PII.[82] This, and the requirement to provide a structured report to the data subject, are fairly simple tasks. The second right, embedded within Article 20, will potentially cause issues for controllers: the right to transmit data to another controller.[83] In addition to the ability to exercise the right to be forgotten, and all its associated issues,[84] the data subject may now require controllers to relinquish their competitive advantages.

Development of AI under its current model hinges on the collection of big data; large data sets provide a distinct competitive advantage. Companies spend millions of dollars solely to improve the data collection processes.[85] By allowing a data subject to retrieve or extract this data, smaller companies can collect comparable amounts of PII without needing to spend as much on their collection processes.[86] In theory, Article 20's requirements may lead to data parity, which could in turn create more competitive AI markets that ultimately benefit consumers.[87] Companies would then have a less distinct advantage, or disadvantage, based on the amount of data available to them. While it is possible that this data parity may help with the overall development of AI, it may also lead to greater risks for companies and negatively impact AI.

Since consumers will be able to choose who retains their information, companies will need to emphasize their public relations and data security—otherwise, data subjects may not trust controllers with their information. For example, when large scale data breaches occur, consumers immediately feel violated. Here, the loss of trust and desire for remedial action will likely result in consumers requiring

[80] *Id.* art. 20(1). Upon request, a controller has an obligation to deliver the personal data in a "structured, commonly used and machine-readable format." *Id.*

[81] *See* discussion *supra* Sections II.A.1 – II.A.2.

[82] *See* Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, EUR. COMM'N DOC. WP 242 rev.01 (Apr. 5, 2017).

[83] *Id.* at 4-5.

[84] *See* discussion *supra* Section II.A.2.

[85] Data & Analytics Survey: Big Data and Its Use Cases Keep Growing, IDG (2016), http://bit.do/IDG_Survey.

[86] See Ruth Janal, Data Portability – A Tale of Two Concepts, 8 J. INTELL. PROP., INFO. TECH. & E-COM. L. 59, 60-61 (2017).

[87] See id. for further discussion on this theory.

companies to transmit their data elsewhere, or to delete it entirely. In turn, heavily funded AI operations may consequentially become unlawful, or lack the necessary resources to continue its development. While not going so far as to suggest that corporate espionage and sabotage amongst AI companies would increase, the potential impact of breaches and negative publicity could be catastrophic for certain companies. Ultimately, consumer rights to data portability inherently contain the risk that one bad instance of public relations could result in the downfall of promising AI operations.

4. Right to Explanation

Article 22 grants data subjects the right to not be subject to decisions based solely on automated processing.[88] Instead, the data subjects may, at the very least, exercise a right to human intervention and explanation.[89] While several exceptions to this rule exist,[90] processors and controllers remain obligated to protecting a data subject's rights, freedoms, and interests.[91] Even if subject to automated decision-making, individuals still have a right to know of its existence, including profiling,[92] and, if requested, must be provided with "meaningful information about the logic involved, as well as the

[88] GDPR, *supra* note 7, art. 22(1) ("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.").

[89] *Id.* art. 22(3).

[90] *Id.* art. 22(2). The right not to be subject to an automated decision does not apply if the decision:

> (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
>
> (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> (c) is based on the data subject's explicit consent.

Id.

[91] *Id.* art. 22(3) (When automated decisions are made either to perform a contract or with explicit consent, as outlined in Article 22(2), a controller must still "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.").

[92] "Profiling" is defined as:

> [A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[.]

Id. art. 4(4), at 33.

significance and the envisaged consequences of such processing for the data subject."[93]

Data subjects also have a right to object to automated processing[94] when data processing is for either public interest reasons or when the data subject's fundamental rights and freedoms outweigh the interests of the processing controller or third party.[95] Here, the burden is on the controller to demonstrate that it has "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."[96] Essentially, the controller must persuade the court that its personal objectives outweigh the highly emphasized and protected data privacy rights of individuals. Since the ECJ liberally protects consumer data privacy rights, a controller must determine whether the risk of violating the GDPR is worth the continuance of processing. However, even if the ECJ were to find for the controller, a data subject may still be able to limit the processing of its PII through Article 18's right to restrict processing.[97]

For those organizations utilizing AI, it is impractical to employ unsupervised models of machine learning. Article 22's right to human intervention and explanation of logic requires that AI decisions be

[93] *Id.* art. 15(1)(h), at 43. Under Article 15, data subjects are given a right of access to their controlled personal data, including but not limited to, the purpose of the processing, the categories of data, and the envisaged time period. *See id.* art. 15(1).

[94] *Id.* art. 21(1), at 45 ("The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."). Additionally, the right to object to processing must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information." *Id.* art. 21(4), at 46. Because of this, consumers know they can object to unfavorable decisions made using their individual PII.

[95] *Id.* art. 6(1)(e), (f), at 36. As referenced, the relevant portions of Article 6(1) referred to by Article 21(1) include when:

> (d) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [and]
>
> (e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Id.

[96] *Id.* art. 21(1), at 45.

[97] *See id.* art. 18(1), at 44.

explainable.[98] While a supervised model of learning uses labeled sets of data to develop algorithms, supplemented by human oversight, unsupervised models allow AI to evolve on its own.[99] With unsupervised models, it may not be possible to trace the AI's learning processes or to explain its decisions, due to a lack of data labels and relationships. Even supervised models may be too hard to explain, which would impair one of AI's most useful purposes: automated decisions and forecasts.[100] As a result, the GDPR's extensive protection of data privacy rights restrains the use of AI's most useful features: autonomy and automation.

Even if explainable, protections against the profiling of individuals also stands to eliminate the commercial usefulness of AI, along with its ability to learn. To be effective, most commercial uses of AI oriented towards consumers rely on analysis and forecasts based on an individual's unique characteristics.[101] However, under the GDPR, individuals may object to processing used to "analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[.]"[102] By restricting profiling, AI cannot learn from human, group, or individual behaviors, and may not be viable for extensive operational uses. Additionally, the right to object expressly identifies direct marketing, a marketing tactic which uses individual buyer behaviors to forecast future purposes so as to tailor advertisements to a specific individual, as an objectionable processing purpose.[103] Objections to direct marketing do not have a rebuttable aspect that allows controllers to continue their operations if

[98] *See id.* art. 22(3), at 46.

[99] For an explanation of supervised and unsupervised AI learning, see Bernard Marr, *Supervised V Unsupervised Machine Learning—What's The Difference?*, FORBES (Mar. 16, 2017, 3:13 AM), http://bit.do/Marr_Supervised.

[100] *See, e.g.*, Nick Wallace, *EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence*, TECHZONE360 (Jan. 25, 2017), http://bit.do/Wallace_EU-Right-to-Explanation (explaining why algorithms and AI decisions are often not easily explained, because "[a]n algorithm can spot a correlation, but it cannot explain the link between them because it cannot infer meaning the way a human can").

[101] *See generally* Mike Kaput, *How Brands Target Consumers Better and Sell More with Artificial Intelligence*, MKTG. ARTIFICIAL INTELL. INST. BLOG (Jul. 12, 2017), http://bit.do/Kaput_Brands (provides general background information on consumer profiling, along with some specific examples).

[102] *See* GDPR, *supra* note 7, arts. 4(4), 21, at 33, 45-46.

[103] *See id.* art. 21(2)-(3), at 45. "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing." *Id.* art. 21(2).

they can show a legitimate purpose.[104] Consequently, the commercial application of AI is limited under the GDPR, which may cause businesses to forgo future investments in the technology.

B. E.U.'s AI Law Efforts

The E.U. has recognized that AI is rapidly developing and needing regulation of sorts.[105] Based on a report written by the E.U. Parliament's Committee on Legal Affairs,[106] the E.U. Parliament is calling for the creation of a European Agency to provide technical, ethical, and regulatory expertise in the field of robotics and AI.[107] Though the report broadly states the purpose for this agency,[108] the context of the report suggests greater emphasis on combatting potential liabilities rather than assisting AI development.[109] Also, while the report addresses concerns regarding the protection of data privacy and protection in the context of AI development and regulation, it does not suggest changing existing regulations.[110]

The Information Commissioner's Office ("ICO") has also examined the relationship between AI, data privacy, and data protection.[111] In this report, the ICO examines the inherent data protection implications that exist from the use and development of AI.[112] However, the ICO report continues to support the GDPR, even

[104] *Compare id.* art. 21(1), *with id.* art. 21(2), (3) (while controllers may defend their continued processing when lawfully conducted under Article 6(1)(e), (f), processing for the purposes of direct marketing is objectionable without rebuttal).

[105] *See The Future of Robotics and Artificial Intelligence in Europe*, EUR. COMM'N: DIG. SINGLE MKT. BLOG (Feb. 16, 2017), http://bit.do/DSM-blog (discussing the E.U. Commission's adoption of the Digitising European Industry Strategy in 2016, which recognizes robotics and AI as cornerstone technologies). *See also* Rich Haridy, *EU Move to Bring in AI Laws, but Reject Robot Tax Proposal,* NEWS ATLAS (Feb. 16, 2017), http://bit.do/Haridy_EU-move. According to this article, the E.U. Parliament voted 396 to 123, with 85 abstentions, to pass a resolution to regulate the development of AI and robotics. *Id.* This resolution has since passed to the E.U. Commission, the E.U.'s executive branch, to determine whether or not to accept or reject the proposal to regulate. *Id.* The E.U. Parliament's decision to regulate was based on a report sent to the E.U.'s Legal Affairs Committee, which called for regulation of AI and robotics. *Id.*

[106] *See* Eur. Parl. Comm'n. on Legal Affairs, *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics*, 2015/2103(INL) (May 31, 2016), http://bit.do/EuroParl_Initial-report [hereinafter *Draft Report*].

[107] *See id.* at 7.

[108] *Id.* ("to ensure a timely and well-informed response to the new opportunities and challenges arising from the technological development of robotics").

[109] *See id.* at 10-12.

[110] *See id.* at 8 (noting that regulation must pay particular attention to data privacy and protection as it concerns technical integration into hardware and software, necessity and proportionality standards, and the use of personal data as currency).

[111] *Big Data*, *supra* note 12, at 19-56.

[112] *Id.* (listing a multitude of liability and operation concerns for the use and development of AI, including: fairness of processing, conditions for processing, and data minimization, among

after it points out a multitude of provisions that will negatively impact AI and machine learning.[113] As part of its conclusion, the ICO stated:

> We are aware of the view that, given some of the challenges of applying data protection principles to big data analytics, a different legal or regulatory approach is required. However, we do not accept the idea that data protection, as currently embodied in legislation, does not work in a big data context. We maintain that big data is not a game played by different rules. We acknowledge the increasing importance of accountability in addressing some of these challenges, but we do not see it as a replacement for the more traditional principle of transparency. Transparency still has a significant role to play and we argue it can still be achieved, even in a complex world of AI and machine learning.[114]

Instead of suggesting repairs to the current system, the ICO reinforces the current E.U. stance to stay their current regulatory course. As a result, it is likely that, even if the E.U. promulgates a new regulatory agency and subsequent AI standards, the standards would need to comply with the GDPR's provisions.

The GDPR will affect the way that companies use and develop AI. Even though the E.U. plans to regulate AI specifically, these regulations will exist harmoniously with the GDPR's expectations.[115] As a result, AI regulatory action is unlikely to assist in circumventing the difficulties for AI presented by the GDPR. While the E.U. may think that this is the best course of action, its immediate detrimental impact will likely cause the E.U.to explore alternatives in regulating AI with respect to data privacy.

III. WHERE DOES THE E.U. GO FROM HERE?

The E.U.'s imminent GDPR implementation and its approach towards AI, coupled with the current, predominant model of AI, threaten to stagnate AI research and development in the E.U.

others).

[113] *Id.*

[114] *Id.* at 95.

[115] *See, e.g.*, *Draft Report*, *supra* note 106 (emphasizing that privacy and data protection guarantees must be embedded in the E.U.'s regulatory framework for robotics and AI). The E.U.'s cautious approach to the development of AI is evident in its policy. *Id.* at 7 (noting that the "potential for empowerment through the use of robotics is nuanced by a set of tensions or risks relating to human safety, privacy, integrity, dignity, autonomy and data ownership"). In response to the growing commercialization of the robotics and AI sector, the E.U. has stressed the importance of consumer protection (pointing out that the "use of personal data as a 'currency' with which services can be 'bought' . . . may not lead to a circumvention of the basic principles governing the right to privacy and data protection). *Id.* at 8.

Additionally, if the ECJ liberally interprets the GDPR and fully exercises its territorial jurisdiction, international issues regarding AI are to be expected. Alternatively, countries and companies may instead develop AI without the use of PII from the E.U., which could impact its ability to function there. To address these issues, the European Council and Commission should choose to either (a) carve AI out of the GDPR's scope and form an E.U. AI Council, or (b) assist in funding the development and use of alternative AI models that would comply with current GDPR standards.

A. AI as a Carve-Out of GDPR

Although the E.U. is currently exploring opportunities to regulate AI,[116] the 2018 implementation of the GDPR is imminent. Once effective, controllers and processors of E.U. personal data will be subject to the GDPR's terms. While the GDPR's provisions stand to govern all who fall within its material scope, due to its extensive territorial jurisdiction, the question remains of how those outside of the E.U. will respond to the GDPR's provisions. In theory, any controller or processor that processes personal data belonging to an E.U. citizen will fall within the GDPR's material and territorial domain.[117] However, the potentially negative impact of the GDPR[118] on AI use and development will result in an unwillingness to abide by its terms. Instead, the GDPR will face significant legal challenges by those controllers and processors prosecuted under Article 3's territorial scope.

While the GDPR's intent is to govern all those who use personal data belonging to E.U. citizens, legal challenges against its scope and extraterritorial reach may lessen its effectiveness or result in a blatant disregard for the regulation altogether.[119] Instead, only E.U.-based controllers and processors would bear the burden of trying to comply

[116] *See* discussion *supra* Section II.B.

[117] *See* GDPR, *supra* note 7, arts. 2-3, at 32-33.

[118] *See* discussion *supra* Section II (detailing articles of the GDPR that may severely impact the development and use of AI).

[119] *See* Dennis Dayman, *GDPR Impact for Non-EU Companies*, RETURN PATH (Mar. 14, 2018), http://bit.do/Dayman_Non-EU (speculating that enforcement of the GDPR against non-E.U. companies could be executed through court injunctions or potential seizures of physical goods). Alternatively, GDPR compliance could also be regulated through international cooperation agreements, especially between the U.S. and E.U. law enforcement agencies, such as implementing mechanisms that allow the E.U. to issue complaints and fines against American companies. *See* Aaron Winston, *How the EU Can Fine US companies for Violating GDPR*, SPICEWORKS (June 21, 2017), http://bit.do/Violating_GDPR (information based on an interview with former Deputy General Counsel and Ethics Official of the White House Office of Drug Policy Linda V. Priebe, a specialist in data privacy and security in both the U.S. and E.U.).

with the GDPR while simultaneously developing AI. While GDPR compliance would be necessary for those conducting business in or with E.U.-based controllers, the E.U. market may not be worth the efforts to comply or the potential liabilities for noncompliance. Instead, top AI companies and organizations could choose to avoid the GDPR. In effect, avoiding the GDPR would allow the AI development in other countries to progress unencumbered, versus those within the E.U and subject to the GDPR. Rather than rely on the GDPR to retain global jurisdiction, the E.U. should recognize its potential adverse impact on AI within its own borders.

Many countries have recognized the effects of overregulating technological advancement. These countries have chosen not to overly protect consumer personal data or have carved out AI uses of personal data from more onerous PII regulations.[120] Because AI requires large sets of data to develop, overregulation of personal data stagnates AI use and limits research. While it is evident that the E.U. intends to develop AI laws that mesh with the GDPR's provisions, it should instead carve out AI from the GDPR.[121] In particular, AI regulations need to address the issues surrounding the erasure of data, in favor of controllers and processors. For example, rather than requiring a complete erasure of personal data, controllers and processors should be able to retain information up to the point of erasure. In this way, the AI's machine learning would remain at the point where it progressed, rather than creating forced amnesia. However, all future machine learning would not include the erased personal data. Presumably, this would balance the interests of deleting the individual's PII without causing the AI to regress.

Ultimately, the existing AI model emulates the neural activity of a human. Like humans, AI observes and learns from its external environment. While humans learn from the real world, AI learns from big data. Rather than treating AI like ordinary data collection and processing systems, the E.U. should recognize that AI most closely resembles human information processing. Instead of requiring AI to forget and unlearn, it is best for the E.U. to treat learned behaviors as separate from the personal data it is derived from.

B. E.U. Funding of Alternative AI Models

If the E.U. remains steadfast in not carving AI out of the GDPR, its next best solution may be to fund AI development. Similar to China,

[120] *See* discussion *supra* Section I.B.

[121] *See supra* Section II.B (discussing the detrimental effects of creating a new regulatory framework for AI that is forced to coexist with the GDPR).

government AI funding would help to expedite and sustain AI development.[122] Additionally, government funding would entice AI companies to stay within the E.U., even though they would remain subject to the GDPR. Because the government would assist in funding the AI, it may be more willing to relax its enforcement of the GDPR against those acting on behalf of the E.U. or its Member States. With government funding, controllers would have greater incentive and resources to research newer models of AI that better fit within the scope of the GDPR.

Though the current model of AI allows reverse-engineering to trace PII to a specific individual, research suggests that there may be ways to combat this threat to consumer data.[123] For example, Google and OpenAI have found that it is possible to build algorithms less traceable to a particular individual by using "differential privacy."[124] Google's theoretical model allows algorithms to function as if the algorithm had learned from personal data without actually ever seeing it.[125] While not quite as accurate as the traditional model of AI, early results indicate that this model is within an accuracy rate of 2% of the traditional model, versus 5% by any other alternative model.[126] These early indications support an ability for AI technology to eventually evolve in a manner consistent with the GDPR.

[122] *See* Pham, *supra* note 25.

[123] *See* Nicolas Papernot et al., *Semi-Supervised Knowledge Transfer for Deep Learning from Private Training Data*, 5 INT'L CONF. ON LEARNING REPRESENTATIONS PROC. (2017), http://bit.do/Semi-Supervised.

[124] *See* Dave Gershgorn, *AI Can Learn From Data Without Ever Having Access to It*, QUARTZ (Oct. 24, 2016), http://bit.do/Gershgorn_AI-can-learn (discussing differential privacy, which allows for the protection of individual PII in a large data set and "addresses the paradox of learning nothing about an individual while learning useful information about a population").

[125] *Id.*

[126] *Id.*

CONCLUSION

If the E.U. desires to remain competitive in the race to develop AI, it must balance its interests in protecting personal data against its interest in developing new AI technologies. The implementation of the GDPR, without carveouts to ease the use of personal data in AI systems, demonstrates the E.U.'s favor toward data privacy. Incidentally, the GDPR's restrictions on personal data will burden the ability of AI to learn and develop. As a result, the E.U.'s AI industry is likely to suffer as organizations seek ways to circumvent the GDPR's provisions. Until the E.U. recognizes and addresses the potential impact of the GDPR on its AI industry, the E.U. will fall behind in its AI efforts.