GDR INSIGHT

HANDBOOK 2020

HANDBOOK
2020

Reproduced with permission from Law Business Research Ltd
This article was first published in November 2019
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-235-0

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Privacy

Cybersecurity

Data in Practice

PREFACE

Global Data Review is delighted to publish this inaugural edition of the *GDR Insight Handbook*.

The handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of legislation that affects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of artificial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust. A chapter is dedicated to assessing how companies should respond to the GDPR enforcement regime.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at October 2019. Although every effort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing field of practice, and therefore specific legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

Global Data Review
London
October 2019

PART 3

Data in practice

UNITED STATES: ARTIFICIAL INTELLIGENCE

H Mark Lyon, Cassandra L Gaedt-Sheckter and Frances Waldmann
Gibson, Dunn & Crutcher LLP

Introduction

Over the past several years, lawmakers and government agencies have sought to develop artificial intelligence (AI) strategies and policy with the aim of balancing the tension between protecting the public from the potentially harmful effects of AI technologies, and encouraging positive innovation and competitiveness. As AI technologies become increasingly commercially viable, one of the most interesting challenges lawmakers face in the governance of AI is determining which of its challenges can be safely left to ethics (appearing as informal guidance or voluntary standards), and which rules should be codified in law.[1]

The first half of 2019 saw a surge in debate about the role of governance in the AI ecosystem and the gap between technological change and regulatory response in the digital economy. In the United States, this trend was manifested in particular by calls for regulation of certain 'controversial' AI technologies or use cases, in turn increasingly empowering lawmakers to take fledgling steps to control the scope of AI and automated systems in the public and private sectors. While it remains too soon to herald the arrival of a comprehensive federal regulatory strategy in the United States, there have been a number of recent high-profile draft bills addressing the role of AI and how it should be governed at the US federal level, and US state and local governments are already pressing forward with concrete legislative proposals regulating the use of AI. Likewise, the European Union has taken numerous

1 See, eg, Paul Nemitz, Constitutional Democracy and Technology in the Age of Artificial Intelligence, Phil. Trans. R. Soc. A 376: 20180089 (Nov. 15, 2018), available at https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0089.

steps to demonstrate its commitment toward the advancement of AI technology through funding,[2] while simultaneously pressing for companies and governments to develop ethical applications of AI.[3]

Similarly, US federal, state and local government agencies are beginning to show a willingness to take concrete positions on that spectrum, resulting in a variety of policy approaches to AI regulation – many of which eschew informal guidance and voluntary standards and favour outright technology bans. We should expect that high-profile or contentious AI use cases or failures will continue to generate similar public support for, and ultimately trigger, accelerated federal and state action.[4] For the most part, the trend in favour of more individual and nuanced assessments of how best to regulate AI systems specific to their end uses by regulators in the United States has been welcome. Even so, there is an inherent risk that reactionary legislative responses will result in a disharmonious, fragmented national regulatory framework. Such developments will yield important insights into what it means to govern and regulate AI over the coming year.

Further, as the use of AI expands into different sectors and the need for data multiplies, legislation that traditionally has not focused on AI is starting to have a growing impact on AI technology development. This impact can be seen in areas such as privacy, discrimination, and antitrust laws. While some of these areas may help alleviate some of the ethical concerns AI engenders (eg, eliminating bias), others may unnecessarily inhibit development and make it difficult to operate (eg, complying with consumer deletion requests under privacy laws).

The following section in this chapter will discuss the general regulatory framework of AI technology in the United States, contrasting the approach with other jurisdictions that have invested in AI research and development where appropriate, and will highlight differences in how AI technology is regulated by use in various key sectors.

2 The European Commission (EC) enacted a proposal titled: 'The Communication From the Commission to the European Parliament, the European Council, the European Economic and Social Committee, and the Committee of the Regions: Artificial Intelligence for Europe' (25 April 2018), https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe. The Communication set out the following regulatory proposals for AI: calls for new funding, pledges for investment in explainable AI 'beyond 2020', plans for evaluation of AI regulation, proposes that the Commission will support the use of AI in the justice system, pledges to draft AI ethics guidelines by the end of the year, proposes dedicated retraining schemes, and calls for prompt adoption of the proposed ePrivacy Regulation. Likewise, an April 2018 UK Select Committee Report on AI encouraged the UK government to establish a national AI strategy and proposed an 'AI Code' with five principles, emphasising ideals such as fairness and developing for the common good – mirroring the EU's AI Ethics Guidelines. 'AI Policy – United Kingdom,' available at https://futureoflife.org/ai-policy-united-kingdom/?cn-reloaded=1.

3 High-Level Expert Group on Artificial Intelligence (HLEG), a team of 52 experts who, on 8 April 2019, published 'Ethics Guidelines for Trustworthy AI', available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

4 See, eg, the House Intelligence Committee's hearing on Deepfakes and AI on 13 June 2019 (US House of Representatives, Permanent Select Committee on Intelligence, Press Release: House Intelligence Committee To Hold Open Hearing on Deepfakes and AI (7 June 2019)); see also Makena Kelly, 'Congress grapples with how to regulate deepfakes', *The Verge* (13 June 2019), available at https://www.theverge.com/2019/6/13/18677847/deep-fakes-regulation-facebook-adam-schiff-congress-artificial-intelligence.

The final section in this chapter will discuss certain areas of existing and proposed legislation and policies that may distinctly affect AI technologies and companies, even though they are not directly targeting them, and what effects may result.

AI-specific regulations and policies – existing and proposed

Legislation promoting and evaluating AI ethics and development

By early 2019, despite its position at the forefront of commercial AI innovation, the United States still lacked an overall federal AI strategy and policy.[5] By contrast, observers noted other governments' concerted efforts and considerable expenditures to strengthen their domestic AI research and development,[6] particularly China's plan to become a world leader in AI by 2030.[7] These developments abroad prompted many to call for a comprehensive government strategy and similar investments by the United States' government to ensure its position as a global leader in AI development and application.[8]

5 The only notable legislative proposal was the Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence Act of 2017, also known as the FUTURE of Artificial Intelligence Act, which did not aim to regulate AI directly, but instead proposed a Federal Advisory Committee on the Development and Implementation of Artificial Intelligence. The Act has not been re-introduced in the new Congress.

6 For example, in June 2017, the UK established a government committee to further consider the economic, ethical and social implications of advances in artificial intelligence, and to make recommendations. 'AI – United Kingdom', available at https://futureoflife.org/ai-policy-united-kingdom. It also published an Industrial Strategy White Paper that set out a five-part structure by which it will coordinate policies to secure higher investment and productivity. HM Government, 'Industrial Strategy: Building a Britain fit for the future' (November 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730048/industrial-strategy-white-paper-web-ready-a4-version.pdf. The White Paper also announced an 'Artificial Intelligence Sector Deal to boost the UK's global position as a leader in developing AI technologies' which the government hopes would increase its GDP by 10.3 per cent. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730048/industrial-strategy-white-paper-web-ready-a4-version.pdf. And, in a March 2018 sector deal for AI, the UK established an AI Council to bring together respected leaders in the field, and a new body within the government – the Office for Artificial Intelligence – to support it. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702810/180425_BEIS_AI_Sector_Deal__4_.pd

7 See, eg, Jamie Condliffe, 'In 2017, China is Doubling Down on AI', *MIT Technology Review* (17 January 2017), available at https://www.technologyreview.com/s/603378/in-2017-china-is-doubling-down-on-ai/; Cade Metz, 'As China Marches Forward on A.I., the White House Is Silent', *NY Times* (12 February 2018), available at https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html?module=inline; Jessica Baron, 'Will Trump's New Artificial Intelligence Initiative Make The U.S. The World Leader In AI?', *Forbes* (11 February 2019), available at https://www.forbes.com/sites/jessicabaron/2019/02/11/will-trumps-new-artificial-intelligence-initiative-make-the-u-s-the-world-leader-in-ai/#70d3ea99a017 (noting that, after Canada in March 2017, the US will be the 19th country to announce a formal strategy for the future of AI); see also the German government's new AI strategy, published in November 2018, which promises an investment of €3 billion before 2025 with the aim of promoting AI research, protecting data privacy and digitalising businesses (available at https://www.bundesregierung.de/breg-en/chancellor/ai-a-brand-for-germany-1551432).

8 Joshua New, 'Why the United States Needs a National Artificial Intelligence Strategy and What It Should Look Like', The Center for Data Innovation (4 December 2018), available at http://www2.datainnovation.org/2018-national-ai-strategy.pdf.

The federal government thus began to prioritise both the development and regulation of AI technology. On 11 February 2019, President Donald Trump signed an executive order (EO) creating the 'American AI Initiative',[9] intended to spur the development and regulation of AI and fortify the United States' global position by directing federal agencies to prioritise investments in research and development of AI.[10] The EO, which was titled 'Maintaining American Leadership in Artificial Intelligence,' outlined five key areas: research and development,[11] 'unleashing' AI resources,[12] establishing AI governance standards,[13] building an AI workforce,[14] and international collaboration and protection.[15] The AI Initiative is coordinated through the National Science and Technology Council (NSTC) Select Committee on Artificial Intelligence (Select Committee).

The full impact of the AI Initiative is not yet known: while it sets some specific deadlines for formalising plans by agencies under the direction of the Select Committee, the EO is not self-executing and is generally thin on details. Therefore, the long-term impact will be

9 Donald J Trump, Executive Order on Maintaining American Leadership in Artificial Intelligence, The White House (11 February 2019), available at https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence.

10 The White House, Accelerating America's Leadership in Artificial Intelligence, Office of Science and Technology Policy (11 February 2019), available at https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-is-accelerating-americas-leadership-in-artificial-intelligence.

11 Supra note 1, section 2(a) (directing federal agencies to prioritise AI investments in their 'R&D missions' to encourage 'sustained investment in AI R&D in collaboration with industry, academia, international partners and allies, and other non-Federal entities to generate technological breakthroughs in AI and related technologies and to rapidly transition those breakthroughs into capabilities that contribute to our economic and national security.').

12 id., section 5 (stating that '[h]eads of all agencies shall review their Federal data and models to identify opportunities to increase access and use by the greater non-Federal AI research community in a manner that benefits that community, while protecting safety, security, privacy, and confidentiality').

13 Aiming to foster public trust in AI by using federal agencies to develop and maintain approaches for safe and trustworthy creation and adoption of new AI technologies (for example, the EO calls on the National Institute of Standards and Technology (NIST) to lead the development of appropriate technical standards). Within 180 days of the EO, the Secretary of Commerce, through the Director of NIST, shall 'issue a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies' with participation from relevant agencies as the Secretary of Commerce shall determine. The plan is intended to include 'Federal priority needs for standardization of AI systems development and deployment,' the identification of 'standards development entities in which Federal agencies should seek membership with the goal of establishing or supporting United States technical leadership roles,' and 'opportunities for and challenges to United States leadership in standardization related to AI technologies'. See id., section 6(d)(i)(A)-(C). Accordingly, we can expect to see proposals from the General Services Administration (GSA), OMB, NIST, and other agencies on topics such as data formatting and availability, standards, and other potential regulatory efforts. NIST's indirect participation in the development of AI-related standards through the International Organization for Standardization (ISO) may prove to be an early bellwether for future developments.

14 The EO asks federal agencies to prioritise fellowship and training programs to prepare for changes relating to AI technologies and promoting science, technology, engineering and mathematics (STEM) education.

15 In addition, the EO encourages federal agencies to work with other nations in AI development, but also to safeguard the country's AI resources against adversaries.

in the actions recommended and taken as a result of those consultations and reports, not the EO itself.[16] Moreover, although the AI Initiative is designed to dedicate resources and funnel investments into AI research, the EO does not set aside specific financial resources or provide details on how available resources will be structured.[17] On 19 March 2019, the White House launched ai.gov as a platform to share AI initiatives from the Trump administration and federal agencies. These initiatives track along the key points of the AI EO, and ai.gov is intended to function as an ongoing press release.[18]

A couple of months later, on 11 April 2019, the Growing Artificial Intelligence Through Research (GrAITR) Act was introduced to establish a coordinated federal initiative aimed at accelerating AI research and development for US economic and national security and closing the existing funding gap.[19] The Act would create a strategic plan to invest US$1.6 billion over 10 years in research, development and application of AI across the private sector, academia and government agencies, including the National Institute of Standards and Technology (NIST), and the National Science Foundation and the Department of Energy – aimed at helping the United States catch up to other countries, including the United Kingdom, who are 'already cultivating workforces to create and use AI-enabled devices'. The bill has been referred to the House Committee on Science, Space, and Technology.

16 For instance, the EO established an internal deadline for agencies to submit responsive plans and memoranda for 10 August 2019. The EO directs the Office of Management and Budget (OMB) director, in coordination with the directors of the Office of Science and Technology Police, Domestic Policy Council, and National Economic Council, and in consultation with other relevant agencies and key stakeholders (as determined by OMB), to issue a memorandum to the heads of all agencies to 'inform the development of regulatory and non-regulatory approaches' to AI that 'advance American innovation while upholding civil liberties, privacy, and American values' and consider ways to reduce barriers to the use of AI technologies in order to promote their innovative application. See supra note 1, section 6(a).

17 By contrast, the EU has demonstrated its commitment toward the advancement of AI technology through using its resources to fund projects that involve the technology, such as the MURAB (MRI and Ultrasound Robotic Assisted Biopsy) project, which is developing technology to allow more precise and effective biopsies (tissue samples) in order to diagnose cancer. The EU is covering roughly 90 per cent of MURAB's budget (https://ec.europa.eu/digital-single-market/en/news/using-artificial-intelligence-detect-cancer-and-other-diseases).

18 Donald J Trump, Artificial Intelligence for the American People, the White House (2019), available at https://www.whitehouse.gov/ai/. For example, three years after the release of the initial National Artificial Intelligence Research and Development Strategic Plan, in June 2019 the Trump administration issued an update – previewed in the administration's February 2019 executive order – highlighting the benefits of strategically leveraging resources, including facilities, data sets and expertise, to advance science and engineering innovations, bringing forward the original seven focus areas (long-term investments in AI research; effective methods for human-AI collaboration; ethical, legal and societal implications of AI; safety and security of AI systems; shared public data sets and environments for AI training and testing; measuring and evaluating AI technologies through standards and benchmarks; and national AI research-and-development workforce needs) and adding an eighth: public-private partnerships.

19 HR 2022, 116th Cong (2019). See https://www.congress.gov/bill/116th-congress/house-bill/2202 or https://lipinski.house.gov/press-releases/lipinski-introduces-bipartisan-legislation-to-bolster-us-leadership-in-ai-research.

A companion bill to GrAITR, the Artificial Intelligence Government Act, would attempt to create a national, overarching strategy 'tailored to the US political economy', for developing AI with a US$2.2 billion federal investment over the next five years.[20] The Act would task branches of the federal government to use AI where possible in operation of its systems. Specifically, it includes the establishment of a national office to coordinate AI efforts across the federal system, requests that NIST establish ethical standards, and proposes that the National Science Foundation set educational goals for AI and STEM learning.[21] The draft legislation complements the formation of the bipartisan Senate AI Caucus in March 2019 to address transformative technology with implications spanning a number of fields including transportation, healthcare, agriculture, manufacturing and national security.[22]

More recently, Congress has expressed the need for ethical guidelines and labour protection to address AI's potential for bias and discrimination. In February 2019, the House introduced Resolution 153 with the intent of '[s]upporting the development of guidelines for ethical development of artificial intelligence' and emphasising the 'far-reaching societal impacts of AI' as well as the need for AI's 'safe, responsible and democratic development.'[23] Similar to California's adoption last year of the Asilomar Principles[24] and the OECD's recent adoption of five 'democratic' AI principles,[25] the House Resolution provides that the guidelines must be consonant with certain specified goals, including 'transparency and explainability', 'information privacy and the protection of one's personal data', 'accountability and oversight for all automated decisionmaking', and 'access and fairness'. This Resolution puts ethics at the forefront of policy, which differs from other legislation that considers ethics only as an ancillary topic. Yet, while this resolution signals a call to action by the government to come up with ethical guidelines for the use of AI technology, the details and scope of such ethical regulations remain unclear.

20 S. 1558 – Artificial Intelligence Initiative Act, 116th Cong (2019–2010).

21 The bill also establishes the National AI Research and Development Initiative to identify and minimise 'inappropriate bias and data sets algorithms'. The requirement for NIST to identify metrics used to establish standards for evaluating AI algorithms and their effectiveness, as well as the quality of training data sets, may be of particular interest to businesses. Moreover, the bill requires the Department of Energy to create an AI research programme, building state-of-the-art computing facilities that will be made available to private sector users on a cost-recovery basis.

22 Press Release, Senator Martin Heinrich, 'Heinrich, Portman, Schatz Propose National Strategy For Artificial Intelligence; Call For $2.2 Billion Investment In Education, Research & Development' (21 May 2019), available at https://www.heinrich.senate.gov/press-releases/heinrich-portman-schatz-propose-national-strategy-for-artificial-intelligence-call-for-22-billion-investment-in-education-research-and-development.

23 HR Res 153, 116th Cong (1st Sess 2019).

24 Assemb Con Res 215, Reg Sess 2018–2019 (Cal 2018) (enacted) (expressing the support of the legislature for the 'Asilomar AI Principles' – a set of 23 principles developed through a collaboration between AI researchers, economists, legal scholars, ethicists and philosophers that met in Asilomar, California, in January 2017 and categorised into 'research issues', 'ethics and values' and 'longer-term issues' designed to promote the safe and beneficial development of AI – as 'guiding values for the development of artificial intelligence and of related public policy).

25 OECD Principles on AI (22 May 2019) (stating that AI systems should benefit people, be inclusive, transparent and safe, and their creators should be accountable), available at http://www.oecd.org/going-digital/ai/principles.

Further, the proposed AI JOBS Act of 2019, introduced on 28 January 2019, would authorise the Department of Labor to work with businesses and education institutions in creating a report that analyses the future of AI and its impact on the American labour landscape.[26] Similar to the house resolution on ethics, this Act indicates federal recognition of the threat the introduction of AI technology poses; however, there is no indication as to what actions the federal government might take in order to offer labour protection.

Regulation of AI technologies and algorithms

There are no presently enacted federal regulations that specifically apply to AI technology. However, there are two proposed pieces of legislation that seek to do so. The Bot Disclosure and Accountability Act, first introduced on 25 June 2018 and reintroduced on 16 July 2019, mandates that the FTC come up with regulations that force digital platforms to publicly disclose their use of an 'automated software program or process intended to replicate human activity online'.[27] It also prohibits political candidates or parties from using these automated software programs in order to share or disseminate any information targeting political elections. The Act hands the task of defining 'automated software program' to the FTC, which leaves wide latitude in interpretation beyond the narrow bot purpose for which the bill is intended. Also, commentators even express that this bill goes too far in regulating otherwise protected free speech and free expression, in violation of constitutional rights.

On 10 April 2019, a number of Senate Democrats introduced the Algorithmic Accountability Act, which 'requires companies to study and fix flawed computer algorithms that result in inaccurate, unfair, biased or discriminatory decisions impacting Americans.'[28] The bill stands to be Congress's first serious foray into the regulation of AI and the first legislative attempt in the United States to impose regulation on AI systems in general, as opposed to regulating a specific technology area, such as autonomous vehicles. While observers have noted congressional reticence to regulate AI in past years, the bill hints at a dramatic shift in Washington's stance amid growing public awareness for AI's potential to create bias or harm certain groups.[29] The bill casts a wide net, such that many technology companies would find common practices to fall within the purview of the Act. The Act would not only regulate AI systems

26 HR 827 – AI JOBS Act of 2019, 116th Cong (2019), available at https://www.congress.gov/bill/116th-congress/house-bill/827/text.

27 S.3127 – Bot Disclosure and Accountability Act of 2018, 115th Cong (2018), available at https://www.congress.gov/bill/115th-congress/senate-bill/3127 and S.2125 Bot Disclosure and Accountability Act of 2019, 116th Cong (2019), available at https://www.congress.gov/bill/116th-congress/senate-bill/2125.

28 Cory Booker, Booker, Wyden, Clarke Introduce Bill Requiring Companies To Target Bias In Corporate Algorithms, United States Senate (10 April 2019), available at https://www.booker.senate.gov/?p=press_release&id=903; see also S.1108 – Algorithmic Accountability Act, 116th Cong (2019).

29 See, eg, Karen Hao, 'Congress Wants To Protect You From Biased Algorithms, Deepfakes, And Other Bad AI', *MIT Review* (15 April 2019), available at https://www.technologyreview.com/s/613310/congress-wants-to-protect-you-from-biased-algorithms-deepfakes-and-other-bad-ai/; Meredith Whittaker, et al, 'AI Now Report 2018', AI Now Institute, 2.2.1 (December 2018), available at https://ainowinstitute.org/AI_Now_2018_Report.pdf; Russell Brandom, 'Congress Thinks Google Has a Bias Problem—Does It?', *The Verge* (12 December 2018), available at https://www.theverge.com/2018/12/12/18136619/google-bias-sundar-pichai-google-hearing.

but also any 'automated decision system,' which is broadly defined as any 'computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers'.[30] Additional regulations will be needed to give these key terms meaning but the bill is a harbinger for AI regulation that identifies areas of concern.

The bill reflects a step back from the previously favoured approach of industry self-regulation, since it would force companies to actively monitor use of any potentially discriminatory algorithms. Although it does not provide for a private right of action or enforcement by state attorneys general, it would give the Federal Trade Commission the authority to enforce and regulate these audit procedures and requirements. Further congressional action on this subject can certainly be anticipated.

At the state level, California passed a bill in September 2018, the 'Bolstering Online Transparency Act',[31] which was the first of its kind and (similar to the federal bot bill) is intended to combat malicious bots operating on digital platforms. This state law does not attempt to ban bots outright, but requires companies to disclose whether they are using a bot to communicate with the public on their internet platforms. The law went into effect on 1 July 2019.

In May 2019, Illinois passed a piece of legislation, the Artificial Intelligence Video Interview Act, that limits an employer's ability to incorporate AI into the hiring process.[32] Employers must meet certain requirements to use AI technology for hiring, which includes obtaining informed consent by explaining how the AI works, and what characteristics the technology examines, and employers must delete any video content within 30 days. However, the bill does not define what 'AI' means, and other requirements for the informed consent provisions are considered vague and subject to wide latitude.

National security and military use

In the last few years, the US federal government has been very active in coordinating cross-agency leadership and planning for bolstering continued research and development of artificial intelligence technologies for use by the government itself. Along these lines, a principle focus for a number of key legislative and executive actions was the growth and development of such technologies for national security and military uses. As a result of the passing of

30 The bill would allow regulators to take a closer look at any 'high-risk automated decision system' – those that involve 'privacy or security of personal information of consumers', 'sensitive aspects of [consumers'] lives, such as their work performance, economic situation, health, personal preferences, interests, behavior, location, or movements', 'a significant number of consumers regarding race [and several other sensitive topics]', or 'systematically monitors a large, publicly accessible physical place'. For these 'high-risk' topics, regulators would be permitted to conduct an 'impact assessment' and examine a host of proprietary aspects relating to the system.

31 SB 1001, Bolstering Online Transparency Act (Ca 2017), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

32 HB 2557, 101st General Assembly (Ill 2019), available at http://www.ilga.gov/legislation/BillStatus.asp?DocNum=2557&GAID=15&DocTypeID=HB&SessionID=108&GA=101.

the John S. McCain National Defense Authorization Act for 2019 (the 2019 NDAA),[33] the National Security Commission on Artificial Intelligence was established to study current advancements in artificial intelligence and machine learning, and their potential application to national security and military uses.[34] In addition, in response to the 2019 NDAA, the Department of Defense created the Joint Artificial Intelligence Center (JAIC) as a vehicle for developing and executing an overall AI strategy, and named its director to oversee the coordination of this strategy for the military.[35] While these actions clearly indicate an interest in ensuring that advanced technologies like AI also benefit the US military and intelligence communities, the limited availability of funding from Congress may hinder the ability of these newly formed entities to fully accomplish their stated goals.

Still, the JAIC is becoming the key focal point for the Department of Defense (DOD) in executing its overall AI strategy. As set out in a 2018 summary of AI strategy provided by the DOD,[36] the JAIC will work with the Defense Advanced Research Projects Agency (DARPA),[37] various DOD laboratories, and other entities within the DOD to not only identify and deliver AI-enabled capabilities for national defence, but also to establish ethical guidelines for the development and use of AI by the military.[38]

33 https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

34 id.

35 See Cronk, Terri Moon, 'DOD Unveils Its Artificial Intelligence Strategy' (12 February 2019) at https://www.defense.gov/Newsroom/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/. In particular, the JAIC director's duties include, among other things, developing plans for the adoption of artificial intelligence technologies by the military and working with private companies, universities and non-profit research institutions toward that end.

36 Summary of the 2018 Department of Defense Artificial Intelligence Strategy, Harnessing AI to Advance Our Security and Prosperity (https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF).

37 Another potentially significant effort is the work currently being performed under the direction of DARPA on developing explainable AI systems. See https://www.darpa.mil/program/explainable-artificial-intelligence. Because it can be difficult to understand exactly how a machine learning algorithm arrives at a particular conclusion or decision, some have referred to artificial intelligence as being a 'black box' that is opaque in its reasoning. However, a black box is not always an acceptable operating paradigm, particularly in the context of battlefield decisions, within which it will be important for human operators of AI-driven systems to understand why particular decisions are being made to ensure trust and appropriate oversight of critical decisions. As a result, DARPA has been encouraging the development of new technologies to explain and improve machine–human understanding and interaction. See also DARPA's 'AI Next Campaign' (https://www.darpa.mil/work-with-us/ai-next-campaign).

38 id. at 9. See also id. at 15 (the JAIC 'will articulate its vision and guiding principles for using AI in a lawful and ethical manner to promote our values'.); in addition, under the 2019 NDAA, one duty of the JAIC director is to develop legal and ethical guidelines for the use of AI systems. https://www.govinfo.gov/content/pkg/BILLS-115hr5515enr/pdf/BILLS-115hr5515enr.pdf

The JAIC's efforts to be a leader in defining ethical uses of AI in military applications may further prove challenging because one of the most hotly debated uses of AI is in connection with autonomous weaponry.[39] Even indirectly weaponised uses of AI, such as Project Maven, which utilised machine learning and image recognition technologies to improve real-time interpretation of full-motion video data, have been the subject of hostile public reaction and boycott efforts.[40] Thus, while time will tell, the tension between the confidentiality that may be needed for national security and the desire for transparency with regard to the use of AI may be a difficult line for the JAIC to walk.[41]

Healthcare

Unsurprisingly, the use of AI in healthcare draws some of the most exciting prospects and deepest trepidation, given potential risks.[42] As of yet, there are few regulations directed at AI in healthcare specifically, but regulators have recently acknowledged that existing frameworks for medical device approval are not well-suited to AI-related technologies. The US Food and Drug Administration (FDA) has therefore proposed a specific review framework for AI-related medical devices, intended to encourage a pathway for innovative and life-changing AI technologies, while maintaining the FDA's patient safety standards.

The FDA recently published a discussion paper – 'Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)' – offering that new framework for regulating health products using AI, and seeking comment. The paper introduces that one of the primary benefits of

39 Calls for bans or at least limits on so-called 'killer robots' go back several years, and even provoked several thousand signatories, including many leading AI researchers, to the Future of Life Institute's pledge. See https://futureoflife.org/lethal-autonomous-weapons-pledge.

40 Indeed, Google was forced to withdraw from Project Maven because of employee activism. See https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

41 Congress seems to recognise that the military penchant for secrecy may require further oversight, as the draft version of the 2020 NDAA (see https://www.congress.gov/116/bills/s1790/BILLS-116s1790rs.pdf), recently passed by the House of Representatives, would require increased reporting on weapon developments as well as the creation of a plan to improve transparency for military uses of AI.

42 For example, AI has been used in robot-assisted surgery in select fields for years, and studies have shown that AI-assisted procedures can result in far fewer complications. Brian Kalis, Matt Collier and Richard Fu, '10 Promising AI Applications in Health Care', *Harvard Business Review* (10 May 2018), available at https://hbr.org/2018/05/10-promising-ai-applications-in-health-care. Yet, *The New York Times* published an article in March 2019 warning of healthcare AI's potential failures, including small changes in vernacular leading to vastly disparate results (eg, 'alcohol abuse' leading to a different diagnosis than 'alcohol dependence'); see Cade Metz and Craig S Smith, 'Warning of a Dark Side to A.I. in Health Care', *The New York Times* (21 March 2019), available at nytimes.com/2019/03/21/science/health-medicine-artificial-intelligence.html. And these issues are backed by studies, including one released by *Science* – one of the highest acclaimed journals – just prior to the article, which discusses how 'vulnerabilities allow a small, carefully designed change in how inputs are presented to a system to completely alter its outputs, causing it to confidently arrive at manifestly wrong conclusions.' Samuel G Finlayson, et al, 'Adversarial attacks on medical machine learning', *SCIENCE* 363:6433, pp. 1287–1289 (22 March 2019) https://science.sciencemag.org/content/363/6433/1287. In the realm of healthcare, this could mean misdiagnosis, mistreatment and death.

using AI in an SaMD product is the ability of the product to continuously update in light of an infinite feed of real-world data, which presumably will lead to 'earlier disease detection, more accurate diagnosis, identification of new observations or patterns on human physiology, and development of personalized diagnostics and therapeutics'.[43] But the current review system for medical devices requires a pre-market review, and pre-market review of any modifications, depending on the significance of the modification.[44] If AI-based SaMDs are intended to constantly adjust, the FDA posits that many of these modifications will require pre-market review – a potentially unsustainable framework in its current form. The paper instead proposes an initial pre-market review for AI-related SaMDs that anticipates the expected changes, describes the methodology, and requires manufacturers to provide certain transparency and monitoring, as well as updates to the FDA about the changes that in fact resulted in accordance with the information provided in the initial review. The FDA published the paper on 2 April 2019, and requested comments by 3 June 2019 on various issues, including whether the categories of modifications described are ones that would require pre-market review, defining 'Good Machine Learning Practices', and in what ways might a manufacturer can 'demonstrate transparency'. Additional discussion and guidance is expected following the FDA's review of the comments.[45]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) incorporates a Privacy Rule[46] that also may unintentionally hinder AI development. For example, one of the basic tenets of the Privacy Rule is that use and disclosure of protected health information should be limited to only the 'minimum necessary' to carry out the particular transaction or

43 US Food & Drug Administration, Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD), at 2 (2 April 2019), available at https://www.fda.gov/media/122535/download.

44 The paper mentions that AI-based SaMDs have been approved by the FDA, but they are generally 'locked' algorithms, and any changes would be expected to go through pre-market review. This proposal attempts to anticipate continuously-adapting AI-based SaMD products.

45 Identified as the health AI hub of Europe by a report by MMC Ventures, in partnership with Barclays, the United Kingdom is similarly recognising that current aspects of healthcare regulation may be inconsistent with needs for AI development. MMC Ventures, The State of AI 2019: Divergence (2019), available at https://www.stateofai2019.com/introduction. For example, the Health Secretary described that the current system is unfavourable to new companies, as it requires long periods of testing. The Secretary announced in 2019 a new unit called NHSX, which is intended to bring together tech leadership, and a separate funding agency to support PhD students to use AI technology to address healthcare issues, among other concerns. The NHS chief executive also spoke on trying to motivate scientists to offer AI technologies, including based on changing the financial framework currently in use. 'NHS aims to be a world leader in artificial intelligence and machine learning within 5 years', NHS England (5 June 2019), available at https://www.england.nhs.uk/2019/06/nhs-aims-to-be-a-world-leader-in-ai-and-machine-learning-within-5-years.

46 See, eg, Health Insurance Portability and Accountability Act, 45 CFR. section 264(a)–(b) (2006).

action.[47] While there are innumerable ways how AI could be used (and may be part of treatment, an enumerated exception), such limitations on use can affect the ability to develop AI related to healthcare.[48]

Facial recognition and other biometric surveillance technologies

Perhaps no single area of application for artificial intelligence technology has sparked as fervent an effort to regulate or ban its use in the United States as has the adoption of facial recognition technology by law enforcement and other public officials.[49] Like other biometric data, data involving facial geometries and structures is often considered some of the most personal and private data about an individual, leading privacy advocates to urge extra care in protecting against unauthorised or malicious uses. As a result, many public interest groups and other vocal opponents of facial recognition technology have been quick to raise alarms about problems with the underlying technology as well as potential or actual misuse by

47 If the use or disclosure is related to treating an individual, then the rule is generally not applicable.

48 Various newer technologies may allow for use of this data in a way that could avoid certain privacy rules. For example, homomorphic encryption allows machine learning algorithms to operate on data that is still encrypted, which could permit a hospital to share encrypted data, allow a remote machine to run analyses, and then receive encrypted results that the hospital could unlock and interpret. See, eg, Kyle Wiggers, 'Intel open-sources HE-Transformer, a tool that allows AI models to operate on encrypted data' (3 December 2018), available at https://venturebeat.com/2018/12/03/intel-open-sources-he-transformer-a-tool-that-allows-ai-models-to-operate-on-encrypted-data. Given its novelty, it is not clear how this would work within the confines of, for example, HIPAA, but could offer a means to keep personal health information private, while also encouraging AI development.

49 Interestingly, while a number of public interest groups, such as the American Civil Liberties Union (ACLU), have come out strongly against the governmental use of facial recognition software (see, eg, infra, n. 51), there also seems to be widespread resistance to law enforcement and governmental use of the technology across the political legislative spectrum. Drew Harwell, 'Both Democrats and Republicans blast facial-recognition technology in a rare bipartisan moment', *The Washington Post* (22 May 2019), available at, https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control/.

governmental authorities.[50] While much of the regulatory activity to date has been at the local level, momentum is also building for additional regulatory actions at both the state and federal levels.[51]

Indeed, municipal and city governments have been the ones to take up the banner and adopt ordinances governing the use of facial recognition software by police and local officials. While San Francisco was the first such city to enact an outright ban with regard to the use of facial recognition information by public officials including law enforcement, at the time of writing, three additional cities have also approved comparable bans on the technology, while similar bans remain under consideration in even more cities.[52]

However, the current lack of US state and federal restrictions on facial recognition technology noted above may soon change. For example, a federal bill introduced in the Senate by Senator Roy Blunt, the 'Commercial Facial Recognition Privacy Act of 2019,' would, if approved, preclude the commercial use of facial recognition technology for the tracking

50 The ACLU has been one of the most vocal groups when it comes to the potential dangers of both law enforcement and other governmental use of facial recognition technology as well as private use. See, eg, Jacob Snow, 'Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots' (26 July 2018) at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28; see also, Stanley, Jay, 'A Looming Implication of Face Recognition: Private Photo Blacklists' (16 April 2018) at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/looming-implication-face-recognition-private-photo.

51 See, eg, 116th Congress, S. 847, the Commercial Facial Recognition Privacy Act of 2019, introduced by Sen. Blunt (R-MO), https://www.congress.gov/bill/116th-congress/senate-bill/847/text (which would preclude the use of facial recognition software by certain private entities without first obtaining consent); New York Senate Bill S5687 and Assembly Bill A7790, https://www.nysenate.gov/legislation/bills/2019/S5687 and https://www.nysenate.gov/legislation/bills/2019/a7790 (both of which would preclude the use of facial recognition software on residential premises); California AB1215, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215 (which would preclude the use of facial recognition software and other biometric surveillance by police body cameras); and California AB1281, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1281 (which would preclude the use of facial recognition software on any physical premises without conspicuous notice of the use on premises).

52 See San Francisco Ordinance No. 103-19, the 'Stop Secret Surveillance' ordinance, effective 31 May 2019 (banning the use of facial recognition software by public departments within San Francisco, California); Somerville Ordinance No. 2019-16, the 'Face Surveillance Full Ban Ordinance', effective 27 June 2019 (banning use of facial recognition by the City of Somerville, Massachusetts or any of its officials); Oakland Ordinance No. 18-1891, 'Ordinance Amending Oakland Municipal Code Chapter 9.65 to Prohibit the City of Oakland from Acquiring and/or Using Real-Time Face Recognition Technology', preliminary approval 16 July 2019, final approval 17 September 2019 (bans use by city of Oakland, California and public officials of real-time facial recognition); Proposed Amendment attached to Cambridge Policy Order POR 2019 #255, approved on 30 July 2019 for review by Public Safety Committee (proposing ban on use of facial recognition technology by City of Cambridge, Massachusetts or any City staff); Attachment 5 to Berkeley Action Calendar for 11 June 2019, 'Amending Berkeley Municipal Code Chapter 2.99 to Prohibit City Use of Face Recognition Technology', voted for review by Public Safety Committee on 11 June 2019 and voted for continued review by Public Safety Committee on 17 July 2019 (proposing ban on use of facial recognition technology by staff and City of Berkeley, California). All of these ordinances incorporated an outright ban of use of facial recognition technology, regardless of the actual form or application of such technology. For a view on how such a reactionary ban is an inappropriate way to regulate AI technologies, see Lyon, H Mark, 'Before We Regulate', *Daily Journal* (26 June 2019) available at https://www.gibsondunn.com/before-we-regulate.

and collection of data relating to consumers absent consent.[53] Similarly, several states are currently considering legislation that would either ban or at least restrict the use of facial recognition software and information derived from such technology at the state level.[54]

In addition, other states have also enacted more general biometric data protection laws that are not limited to facial recognition, but which nevertheless regulate the collection, processing and use of an individual's biometric data (which, at least in some cases, includes facial geometry data). At the time of writing, Illinois, Texas and Washington have all enacted legislation directed to providing specific data protections for their residents' biometric information.[55] Only the Illinois Biometric Information Privacy Act provides for a private right of action as a means of enforcement.[56] In addition, once it goes into effect, the California Consumer Privacy Act will also extend its protections to an individual's biometric information, including that used in facial recognition technology.[57] Still other states have included biometric data privacy as part of their data breach laws, or are currently considering the adoption of more general privacy bills that would include protection of biometric information.[58]

Autonomous vehicles and the automobile industry

There was a flurry of legislative activity in Congress in 2017 and early 2018 towards a national regulatory framework for autonomous vehicles. The US House of Representatives passed the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution (SELF DRIVE) Act[59] in September 2017, but its companion bill (the American Vision for Safer Transportation

53 See supra., n. 52.

54 id.

55 See Illinois 'Biometric Information Privacy Act', 740 ILCS 14/1 (P.A. 95-994, effective 3 October 2008) (Illinois BIPA); Texas Business and Commerce Code Sec. 503.001 'Capture or Use of Biometric Identifier'; and Title 19 of the Revised Code of Washington, Chapter 19.375, 'Biometric Identifiers'.

56 See Illinois BIPA, Section 20 (providing for statutory damages and a private right of action). The Illinois Supreme Court has further held that pleading an actual injury is not required in order to maintain a private right of action under the Illinois BIPA. See *Rosenbach v Six Flags Entertainment Corporation*, 2019 IL 123186 (25 January 2019); see also *Patel v Facebook, Inc*, No. 18-15982 (9th Cir. 8 August 2019) (finding Article III standing for an individual to bring a suit under the Illinois BIPA due to the BIPA's protection of concrete privacy interests, such that violations of the procedures required by the BIPA amount to actual or threatened harm to such privacy interests).

57 See California Civil Code Section 1798.100, et seq (definition of 'personal information' under the Act specifically includes 'biometric information,' which itself includes 'imagery of the . . . face' and 'a faceprint'; see CCC Sec. 1798.140 (o)(1)(e) and (b), respectively). Note that 'publicly available' information is generally excluded from the definition of 'personal information,' but that there is a carve-out to this exclusion for biometric information that is collected without the consumer's knowledge. See CCC Sec. 1798.140 (o)(2).

58 See McGinley, Molly K, 'The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States', *Nat. Law Rvw* (27 August 2019) at https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states (discussing efforts by Arizona, Florida, and Massachusetts to pass biometric privacy legislation).

59 HR 3388, 115th Cong (2017).

through Advancement of Revolutionary Technologies (AV START) Act),[60] stalled in the Senate as a result of holds from Democratic senators who expressed concerns that the proposed legislation remains underdeveloped in that it 'indefinitely' pre-empts state and local safety regulations even in the absence of federal standards.[61] At the time of writing, the bill has not been re-introduced since expiring with the close of the 115th Congress last December, and, even if efforts to reintroduce it are ultimately successful, the measure may not be enough to assuage safety concerns as long as it lacks an enforceable federal safety framework.

In practice, therefore, autonomous vehicles (AVs) continue to operate largely under a complex patchwork of state and local rules, with tangible federal oversight limited to the US Department of Transportation's (DoT) informal guidance. In 3 October 2018, the DoT's National Highway Traffic Safety Administration (NHTSA) released its road map on the design, testing and deployment of driverless vehicles: 'Preparing for the Future of Transportation: Automated Vehicles 3.0' (AV 3.0).[62] AV 3.0 reinforces that federal officials are eager to take the wheel on safety standards and that any state laws on automated vehicle design and performance will be pre-empted. But the thread running throughout is the commitment to voluntary, consensus-based technical standards, and the removal of unnecessary barriers to the innovation of AV technologies.

During 2019, several federal agencies announced proposed rule-making to facilitate the integration of autonomous vehicles onto public roads. In May 2019, in the wake of a petition filed by General Motors requesting temporary exemption from Federal Motor Vehicle Safety Standards (FMVSSs) which require manual controls or have requirements that are specific to a human driver,[63] NHTSA announced that it was seeking comments about the possibility of removing 'regulatory barriers' relating to the introduction of automated vehicles in the

60 US Senate Committee on Commerce, Science and Transportation, Press Release (24 October 2017), available at https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=BA5E2D29-2BF3-4FC7-A79D-58B9E186412C.

61 Letter from Democratic Senators to US Senate Committee on Commerce, Science and Transportation (14 March 2018), available at https://morningconsult.com/wp-content/uploads/2018/11/2018.03.14-AV-START-Act-letter.pdf.

62 US Dept of Transp, 'Preparing for the Future of Transportation: Automated Vehicles 3.0' (September 2017), available at https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

63 General Motors, 'LLC-Receipt of Petition for Temporary Exemption from Various Requirements of the Safety Standards for an All Electric Vehicle with an Automated Driving System', 84 Fed. Reg. 10182.

United States.[64] It is likely that regulatory changes to testing procedures (including pre-programmed execution, simulation, use of external controls, use of a surrogate vehicle with human controls and technical documentation) and modifications to current FMVSSs (such as crashworthiness, crash avoidance and indicator standards) will be finalised in 2021.

Meanwhile, legislative activity at the US state level is stepping up to advance integration of autonomous vehicles.[65] State regulations vary significantly, ranging from allowing testing under certain specific and confined conditions to the more extreme, which allow for testing and operating AVs with no human passenger behind the wheel. Some states, such as Florida, take a generally permissive approach to AV regulation in that they do not require that there be a human driver present in the vehicle.[66] California is considered to have the most comprehensive body of AV regulations, permitting testing on public roads and establishing its own set of regulations just for driverless testing.[67] In April 2019, the California DMV published proposed AV regulations that allow the testing and deployment of autonomous motor trucks (delivery vehicles) weighing less than 10,001 pounds on California's public roads.[68] In the

64 Docket No. NHTSA-2019-0036, 'Removing Regulatory Barriers for Vehicles With Automated Driving Systems', 84 Fed Reg 24,433 (28 May 2019) (to be codified at 49 CFR 571); see also 'Removing Regulatory Barriers for Vehicles with Automated Driving Systems', 83 Fed Reg 2607, 2607 (proposed 5 March 2018) (to be codified at 49 CFR 571). Thus far, the comments submitted generally support GM's petition for temporary exemption and the removal of regulatory barriers to the compliance certification of ADS-DVs. Some commentators have raised concerns that there is insufficient information in the petition to establish safety equivalence between traditionally operated vehicles and ADS-DVs, and regarding the ability of ADS-DVs to safely operate in unexpected and emergency situations. However, it is likely that NHTSA will grant petitions for temporary exemption to facilitate the development of ADS technology, contingent on extensive data-sharing requirements and a narrow geographic scope of operation. In addition, the Federal Motor Carrier Safety Administration also issued a request for comments on proposed rule-making for Federal Motor Carrier Safety Regulations that may need to be reconsidered for Automated Driving System-Dedicated Vehicles (ADS-DVs). Docket No. FMCSA-2018-0037. Safe Integration of Automated Driving Systems-Equipped Commercial Motor Vehicles, 84 Fed Reg 24,449 (28 May 2019).

65 In Washington, Governor Jay Inslee signed into law HB 1325, a measure that will create a regulatory framework for personal delivery devices (PDDs) that deliver property via sidewalks and crosswalks (eg, wheeled robots). [63] 2019 Wash Sess Laws, Ch 214. Washington is now the eighth US state to permit the use of delivery bots in public locations. The other states are Virginia, Idaho, Wisconsin, Florida, Ohio, Utah and Arizona.

66 On 13 June 2019, Florida Governor Ron DeSantis signed CS/HB 311: Autonomous vehicles into law, which went into effect on 1 July CS/HB 311 establishes a statewide statutory framework, permits fully automated vehicles to operate on public roads, and removes obstacles that hinder the development of self-driving cars. See, eg, 'Governor Ron DeSantis Signs CS/HB 311: Autonomous Vehicles' (13 June 2019), available at https://www.flgov.com/2019/06/13/governor-ron-desantis-signs-cs-hb-311-autonomous-vehicles/.

67 For testing both with and without drivers, users must give information to Cal DoT, as well as have a minimum of US$5 million in insurance.

68 State of California Department of Motor Vehicles, Autonomous Light-Duty Motor Trucks (Delivery Vehicles), available at https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/bkgd. The DMV held a public hearing on 30 May 2019, at its headquarters in Sacramento to gather input and discuss the regulations. [57] The DMV's regulations continue to exclude the autonomous testing or deployment of vehicles weighing more than 10,001 pounds.

California legislature, two new bills related to AVs have been introduced: SB 59[69] would establish a working group on autonomous passenger vehicle policy development while SB 336[70] would require transit operators to ensure certain automated transit vehicles are staffed by employees. A majority of states either dictate that manufacturers are not responsible for AV crashes unless defects were present at the time of crash (eg, DC), or that AV crash liability is subject to applicable federal, state or common law.[71] However, some US states have established provisions for liability in the event of a crash.[72]

Also at the local level, some states expressly forbid local governments from prohibiting pilot programmes within the state (eg, Oklahoma,[73] Georgia, Texas, Illinois, Tennessee and Nevada), while others are less restrictive and merely dictate that companies looking to start pilot AV programmes should inform municipalities in writing (eg, California).[74]

Non-AI specific regulation likely affecting AI technologies

Data privacy

Following the General Data Protection Regulation (GDPR) in Europe, and various high-profile privacy incidents over the past few years, lawmakers at both the state and federal level are proposing privacy-related bills at a record rate. Among these are the California Consumer Privacy Act (CCPA), taking effect on 1 January 2020, and the New York Privacy Act, which lost steam mid-way through 2019. Although most are not specific to AI technologies, some include provisions related to automated decision-making, and most have the capacity to greatly affect – and unintentionally stifle progression of – AI technologies.

Legislation proposed in Minnesota and Washington would regulate potential AI technologies directly.[75] For example, Minnesota's pending comprehensive privacy law includes a specific right for a consumer to request information if 'the processing [of personal data] is carried out by automated means,' and limits entities' abilities to make 'a decision based solely on profiling which produces legal effects concerning such consumer,' absent consent or particular circumstances. Here, 'profiling' is broadly defined as 'automated processing of personal data that consists of using personal data to evaluate certain personal aspects relating

69 SB 59, 2019–2020 Reg Sess (Cal 2019).

70 SB 336, 2019–2020 Reg Sess (Cal 2019).

71 However, there is currently no federal framework covering liability for crashes linked to AVs. Note that the UK passed the Autonomous and Electric Vehicles Act in July 2018. The Act requires insurers to deal with all claims even when the vehicle is operating in automated technology mode. Insurers will also have a right of recovery against manufacturers and the right to exclude liability where the relevant individual fails to keep the software up to date.

72 For example, Nebraska assigns liability to human driver unless the autonomous driving system is engaged, in which case the manufacturer is liable.

73 Governor Kevin Stitt signed legislation (SB 365) restricting city and county governments from legislating autonomous vehicles, ensuring that such legislation would be entirely in the hands of state and federal lawmakers. SB 365, 57th Leg, Reg Sess (Okla 2019).

74 Autonomous Vehicle Pilots Across America, National League of Cities (October 2018), available at https://www.nlc.org/sites/default/files/2018-10/AV%20MAG%20Web.pdf

75 See SF 2912 (Mn 2019) in Minnesota, and SB 5376, 66th Leg, Reg Session (Wa 2019) in Washington.

to a natural person, including analyzing or predicting aspects concerning the natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.' And if the entity engages in profiling, it must disclose that fact, and 'information regarding the logic involved, and the significance and potential consequences of the profiling.' Companies using AI technologies may find solace in a potentially significant carve-out through the use of the term 'solely'; as with GDPR, if there is human intervention at some point in the decision-making process, then the regulation is not invoked.[76] Washington's proposed Privacy Act includes very similar provisions, and as additional states develop their own legislation, it is anticipated that this framework may continue.[77]

Further, broadly applicable privacy laws – even without provisions specific to AI – are often fundamentally at odds with AI, and likely to generate headaches for companies developing and using AI technologies.[78] At bottom, AI technologies require large data sets, and those data sets are likely to contain some elements of personal information. This may trigger an avalanche of requirements under privacy laws.[79] For example, as the first and broadest privacy act in the United States, the CCPA allows consumers to request businesses to delete personal information without explanation. For an AI data system, this can be not only impossible, but, to the extent it is possible, it may result in skewed decision-making, a risk to the AI technology's integrity. While CCPA includes several exceptions to this general right (including for reasons of security, transactions, public interest research or internal use aligned with the consumer's expectations), it is unclear how these exceptions will be applied, and whether an entity can use the exceptions as a broad permission to include data in the data sets. The uncertainty is compounded by the fact that there are yet unreleased regulations

76 See, eg, GDPR article 22, and Recital 71 ('the data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention').

77 SB 5376, 66th Leg, Reg Session (Wa 2019), available at http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376.pdf. At the time of writing, it appears both the bill in Minnesota and Washington have lost traction, but it is clear that there is an increased focus on AI from a privacy perspective.

78 For a related analysis on how GDPR may hinder AI made in Europe, see Ahmed Baladi, 'Can GDPR Hinder AI Made in Europe?', Cybersecurity Law Report (10 July 2019) available at https://www.gibsondunn.com/can-gdpr-hinder-ai-made-in-europe.

79 CCPA's broad definition of 'personal information' further contributes to this issue. The CCPA will generally define personal information to be 'information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.' Note, however, that certain requirements present in GDPR that are not present in CCPA, make the risk of stifling AI development less prominent under CCPA. For example, one is the need to have a legal basis for processing under GDPR. This requirement is likely to inhibit development even more, because obtaining consent, or supporting legitimate interests for AI technologies may be difficult, particularly where (1) it may be unknown how exactly the technology works, (2) it may not have a clear use at the company, and (3) it may be in developmental stages. This is similarly the case for the data minimisation principles under GDPR. While data minimisation may be assumed under CCPA, it is not explicitly required, and minimising data can be fundamentally at odds with AI development.

from the California Attorney General's office,[80] several pending amendments to the CCPA awaiting approval by the Governor, and a proposed ballot initiative that could overhaul the CCPA in 2021.[81]

Further, CCPA's security, transparency and sale provisions may pose additional concerns for AI development. The CCPA is set to be enforced in large part by the California Attorney General, but also provides a private right of action based on certain data breaches. With more data comes more vulnerability, making AI companies particularly at risk of litigation for cybersecurity incidents. Further, consumers' right to transparency of what data is collected, how it is used, and where it originates, may simply be impossible for potentially 'black box' AI algorithms. Understanding what data is collected may be feasible, but disclosing how it is used, and in what detail, poses complex issues for AI. And even where disclosure is feasible, companies may face conflicts between not wanting to disclose exactly how such information is used for trade secret purposes, but also complying with consumer notification requirements under privacy regulations where the acceptable level of detail is yet undefined.

On the other hand, these privacy laws may not apply in various circumstances. For example, companies with data of 50,000 consumers or less, that have limited revenues, or are not-for-profit, may not be subject to the CCPA. While this may allow freer range for start-ups, it may have the unintended consequence of decreasing protection (as a result of unsophisticated security systems), and increasing potential of bias (smaller data sets, and less mature anti-bias systems). Also, proposed privacy laws generally do not apply to aggregated or de-identified data. While those definitions can at times be stringent, it may be that AI uses of data can fall out of the scope of regulations by the mere fact that they may not actually use 'personal information' in the form the data is in. That said, given the scope of information potentially used by AI technologies, and that the ability to identify a person based on various data points is increasingly possible, companies focusing on AI technologies are likely to be affected by privacy laws.

80 The California Attorney General's Office is expected to promulgate regulations by October 2019. These regulations are expected to clarify and further define certain aspects of the CCPA, including 'exceptions to CCPA.' See, eg, Public Forum PPT, California Consumer Privacy Act (CCPA), Department of Justice, Office of the California Attorney General, available at https://oag.ca.gov/privacy/ccpa; Cal. Civ. Code section 1798.185.

81 See, eg, Tony Romm, 'Privacy Activist in California launches new ballot initiative for 2020 election', *Washington Post*, 24 September 2019, available at https://www.washingtonpost.com/technology/2019/09/25/privacy-activist-california-launches-new-ballot-initiative-election.

This wave of proposed privacy-related federal and state regulation is likely to continue, potentially affecting AI technologies, even where provisions are not directly applied to automated processes. As a result, companies involved in this area are certain to be focused on these issues in the coming months, and tackling how to balance these requirements with further development.[82]

Discrimination

While the federal laws the United States Equal Employment Opportunity Commission (EEOC) enforces[83] – and its guidelines – have not changed, AI is recognised as a new medium for such discrimination.

Indeed, US Senators Kamala Harris, Patty Murray and Elizabeth Warren probed the EEOC in a September 2018 letter requesting that the Commission draft guidelines on the use of facial recognition technology in the workplace (eg, for attendance and security), and hiring (eg, for emotional or social cues presumably associated with the quality of a candidate).[84] The letter cites various studies showing that facial recognition algorithms are significantly less accurate for darker-skinned individuals,[85] and discusses legal scholars' views on how such algorithms may 'violate workplace anti-discrimination laws, exacerbating employment

82 Various federal bills are also likely to affect AI companies, including the BROWSER Act, HR 2520, 115th Cong (2017), and the CONSENT Act, S. 2639 115th Cong (2018). The CONSENT Act requires online companies with whom consumers have an account (edge providers) to disclose the collection and use of sensitive information (including financial, health, browsing and usage history), and require an opt-in for the use of that information. The BROWSER ACT, proposed one year after the CONSENT Act, requires various communications and technology companies to provide clear evidence of their privacy policies, and allows consumers to opt-in to the collection of sensitive information, and opt-out of the collection of even non-sensitive information. This could greatly hinder the collection and use of information for building AI algorithms.

83 The EEOC enforces federal laws protecting job applicants and employees from discrimination based on protected categories (including race, colour, religion, sex, national origin, age, disability and genetic information), including Civil Rights Act of 1964 section 7, 42 USC section 2000e et seq (1964), Equal Pay Act of 1963, 29 USC section 206(d), Age Discrimination in Employment Act of 1967, 29 USC sections 621–634, Rehabilitation Act of 1973, 29 USC section 701 et seq, and the Civil Rights Act of 1991, S. 1745, 102nd Cong (1991).

84 Kamala D Harris, Patty Murray and Elizabeth Warren, Letter to US Equal Employment Opportunity Commission (17 September 2018), available at https://www.scribd.com/embeds/388920670/content#from_embed.

85 For example, MIT and the ACLU both performed studies questioning facial recognition technologies' ability to accurately process faces of darker-skinned individuals. See, eg, Jacob Snow, 'Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots', ACLU (26 July 2018), available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28, and Inioluwa Deborah Raji and Joy Buolamwini, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products', Massachusetts Institute of Technology (January 2019), available at http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf.

discrimination while simultaneously making it harder to identify or explain' in a court, where such violations may be remediated. Similarly focused letters were sent to the FTC and FBI by varying groups of senators.[86]

For example, US Senators Warren and Doug Jones also sent a letter in June 2019 to various federal financial institutions (the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Consumer Financial Protection Bureau) regarding the use of AI by financial technology companies that have resulted in discriminatory lending practices. The Senators requested answers to various questions to 'help [them] understand the role that [the agencies] can play in addressing FinTech discrimination'.[87]

These concerns are based on an already realised dilemma. Various human resources and financial lending tools have fallen susceptible to inadvertent biases. For example, a hiring tool from Amazon was found to incorporate and extrapolate a pre-existing bias towards men, resulting in a penalisation of resumes referencing women-related terms and institutions (eg, all-women colleges, the word 'women's').[88] And a recent Haas School of Business (UC Berkeley) study found that algorithmic scoring by Fannie Mae and Freddie Mac resulted in charging higher interest rates for Latinx and African-American borrowers, which could violate US anti-discrimination law, including under the Fair Housing Act.[89]

As a result of recent focus on the potential for discrimination and bias in AI, we may see anti-discrimination laws used with more frequency – and potentially additional proposed regulations – against AI-focused technologies.

Antitrust

Government agencies are showing an increasing willingness to scrutinise the business practices of large technology companies on antitrust issues. While not affecting AI directly, these large technology companies are often the companies doing a significant amount of work building, utilising and testing AI, and any threatened 'breakup' of such companies could adversely affect their ability to continue building AI technologies. Centralised concentrations of data – potentially a problem in the antitrust world – may actually promote AI development, given the need for large data sets for use in the development of machine learning systems.

86 Kamala D Harris, Cory A Booker and Cedric L Richmond, Letter to Bureau of Investigation, (17 September 2018), available at https://www.scribd.com/embeds/388920671/content#from_embed; Kamala D Harris, Richard Blumenthal, Cory A Booker and Ron Wyden, Letter to Federal Trade Commission (17 September 2018), available at https://www.scribd.com/embeds/388920672/content#from_embed.

87 Elizabeth Warren and Doug Jones, Letter to The Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, The Office of the Comptroller of the Currency, and The Consumer Financial Protection Bureau (10 June 2019), available at https://www.warren.senate.gov/imo/media/doc/2019.6.10%20Letter%20to%20Regulators%20on%20Fintech%20FINAL.pdf.

88 See, eg, Jeffrey Dastin, 'Amazon scraps secret AI' https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. The tool has since been decommissioned.

89 See, eg, Robert Bartlett, et al, 'Consumer-Lending Discrimination in the FinTech Era' (May 2019), available at https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf. The Fair Housing Act is a part of the Civil Rights Act of 1968, and in part prohibits discrimination in home lending. 42 USC sections 3601–3619.

In July 2019, the Department of Justice announced that its Antitrust Division would review 'whether and how market-leading online platforms have achieved market power and are engaging in practices that have reduced competition, stifled innovation or otherwise harmed consumers.'[90] The Federal Trade Commission also is reportedly investigating online platforms,[91] and the House Judiciary Committee opened a bipartisan investigation into competition in digital markets, which includes holding hearings and subpoenaing documents.[92] In justifying these investigations, proponents often cite criticisms of the advertising practices (which often include AI technologies) of large companies such as Google and Amazon, and the resulting extraordinary influence these large companies have on communications and commerce.[93] On the other hand, because this would be a new area for the application of antitrust laws, critics expect that the federal government will face various challenges in this context.[94]

The Federal Trade Commission's Bureau of Competition also considered earlier in the year potential implications of using AI technology that may violate competition laws. For example, in discussing the launching of an FTC Technology Task Force, the Director of the Bureau of Competition Bruce Hoffman noted the myriad ways AI could itself pose antitrust concerns, namely (1) AI could collude by itself and explicitly agree on price, output and other indicators often left to market forces, (2) machines may independently reach 'oligopoly outcome' more consistently, even if they do not collude, (3) AI could monitor market and competitor activity much more effectively and quickly than humans, which could allow machines to identify and eliminate competitive threats in a way that the human mind cannot conceive, and (4) a broad category of feared unknowns.[95] Director Hoffman further stated that the FTC wanted to be careful of regulating without a 'fact-based, theoretical framework', but clearly recognised the possibility that AI will be subject to antitrust regulation as it continues to

90 Justice Department Reviewing the Practices of Market-Leading Online Platforms, Department of Justice, Office of Public Affairs, Press Release No. 19-799 (23 July 2019), available at https://www.justice.gov/opa/pr/justice-department-reviewing-practices-market-leading-online-platforms.

91 Ben Brody and Daniel Stoller, 'Facebook Acquisitions Probed by FTC in Broad Antitrust Inquiry', *Bloomberg* (1 August 2019), available at https://www.bloomberg.com/news/articles/2019-08-01/facebook-acquisitions-probed-by-ftc-in-broad-antitrust-inquiry.

92 House Judiciary Committee Launches Bipartisan Investigation into Competition in Digital Markets, U.S. House Committee on The Judiciary, Press Release (3 June 2019), available at https://judiciary.house.gov/news/press-releases/house-judiciary-committee-launches-bipartisan-investigation-competition-digital.

93 See, eg, Irina Ivanova, 'Why Big Tech's big breakup may never come', *CBS News* (4 June 2019), available at https://www.cbsnews.com/news/feds-eye-google-facebook-amazon-apple-for-antitrust-issues.

94 For example, it is expected that the government will face issues with the fast-paced changes of technology, with defining the companies individually as a monopoly (rather than potentially combined together), and with simply being up against several of the largest companies in the world. See, eg, Jon Swartz, 'Four reasons why antitrust actions will likely fail to break up Big Tech', *MarketWatch* (15 June 2019), available at https://www.marketwatch.com/story/breaking-up-big-tech-is-a-big-task-2019-06-10.

95 D Bruce Hoffman, 'Competition and Consumer Protection Implications of Algorithms, Artificial Intelligence, and Predictive Analysis, Remarks at Competition and Consumer Protection in the 21st Century' (14 November 2018), available at https://www.ftc.gov/system/files/documents/public_statements/1431041/hoffman_-_ai_intro_speech_11-14-18.pdf.

increase in utilisation.[96] As a result, as these efforts continue, AI growth may be inhibited by antitrust laws indirectly, by affecting the companies that develop the technologies, and also directly, through regulation and investigation targeting AI technologies.

Conclusion

Discussion around regulating AI technologies has grown immensely over the last few years, resulting in a multitude of proposals across sectors from local and federal legislatures. The laws that have passed, and pending regulations and policies, raise significant questions about whether AI technology should be regulated, when, and how, including whether additional growth is required to understand the potential effects and address them adequately, without overzealously inhibiting the United States' position as a world leader in AI. Similarly, non-AI specific laws, including privacy regulation, may have an unintentional disparate impact on AI technologies, given their need for data. The next few years will prove exceedingly interesting with respect to regulation of AI as companies continue to incorporate AI across business lines, and as laws continue to develop and affect AI, directly and indirectly. Given the fast-paced nature of these developments, it is expected that even between the drafting of this chapter and its publication, the landscape of this sector will change dramatically.

The authors would like to acknowledge and thank Virginia Baldwin, Zak Baron, Allie Begin, and Iman Charania for their assistance in compiling the underlying research for this chapter.

96 id.

H Mark Lyon
Gibson, Dunn & Crutcher LLP

H Mark Lyon is chair of Gibson Dunn's artificial intelligence and automated systems practice group, and brings nearly three decades of experience as a trial lawyer and trusted corporate legal adviser to companies in a wide range of technology areas.

Mr Lyon has extensive experience representing and advising clients on the legal, ethical, regulatory and policy issues arising from emerging technologies like artificial intelligence. He regularly acts as a strategic adviser to clients in their development of AI-related products and services, their acquisition and sale of technology-related businesses, and in their development of appropriate legal and ethical policies and procedures pertaining to AI-focused business operations.

In the rapidly advancing area of automated and autonomous vehicles, Mr Lyon has guided clients through the numerous hurdles of U.S. federal and state regulations and requirements for vehicle testing and deployment, as well as advising and assisting clients in exercising their voice before key agencies and legislative bodies. Mr Lyon also brings a global focus to help his clients develop, implement, and audit appropriate policies and procedures to comply with applicable data privacy and cybersecurity regulation as well as assisting clients in the acquisition, protection and enforcement of strategic intellectual property rights.

Cassandra L Gaedt-Sheckter
Gibson, Dunn & Crutcher LLP

Cassandra Gaedt-Sheckter is a technology-focused litigator, with expertise in data privacy and cybersecurity counselling, emerging technologies such as AI, class actions and IP disputes. Ms Gaedt-Sheckter has represented leading technology companies in federal and state courts throughout the United States, on a variety of technologies, including relating to medical devices, pharmaceuticals, mobile gaming, telecommunications, enterprise software and consumer electronics.

She has significant experience in all aspects and phases of litigation and has substantial experience counselling clients in multiple industries on privacy and AI issues, including relating to regulatory compliance (including federal, state and international laws, such as GDPR and PIPEDA), privacy training, privacy and security incident response plans, crisis management during investigations of suspected and actual data breaches, and product development.

Ms Gaedt-Sheckter frequently writes and speaks on issues relating to privacy, AI, and cybersecurity. Ms Gaedt-Sheckter is also licensed to practice before the US Patent and Trademark Office as a patent attorney, and is a Certified Information Privacy Professional (CIPP/US).

Frances Waldmann
Gibson, Dunn & Crutcher LLP

Frances Waldmann is a senior litigation attorney whose practice is focused on white-collar criminal defence and antitrust matters, including litigation, internal investigations, and regulatory enforcement. As a native German speaker, she has particular experience of transnational investigations by UK, US and German regulators, and internal investigations connected thereto. In addition, she regularly represents clients in complex domestic and international litigation and arbitration as well as data privacy and artificial intelligence matters. Prior to joining Gibson Dunn, Ms Waldmann was at a leading set of barristers' chambers in London. Called to the bar in 2010, she both prosecuted and defended cases as sole or junior advocate in a variety of courts of first instance and appellate courts, specialising in matters related to complex criminal and civil fraud and corporate crime.

GIBSON DUNN

Gibson Dunn is a full-service international law firm and is renowned for excellent legal service and commitment to our clients. Our litigators have been involved in numerous high-profile cases, and our transactional lawyers have handled some of the world's largest and most complex matters. Gibson Dunn is a recognised leader in representing companies ranging from start-up ventures to multinational corporations in all major industries, including manufacturing, consumer services, hospitality and leisure, and technology, as well as commercial and investment banks, emerging growth businesses, partnerships, government entities and individuals. Consistently achieving top rankings in industry surveys and major publications, Gibson Dunn is distinctively positioned in today's global marketplace with more than 1,300 lawyers and 20 offices, including Beijing, Brussels, Century City, Dallas, Denver, Dubai, Frankfurt, Hong Kong, Houston, London, Los Angeles, Munich, New York, Orange County, Palo Alto, Paris, San Francisco, São Paulo, Singapore, and Washington, D.C. All of our offices are operated as part of a single enterprise and our attorneys work together seamlessly with other practice groups and offices to deliver the full range of skills and services in the best interests of our clients. For more information on Gibson Dunn, please visit our website.

333 South Grand Avenue
Los Angeles, CA 90071-3197
United States
Tel: +1 213 229 7000
Fax: +1 213 229 7520
www.gibsondunn.com

H Mark Lyon
mlyon@gibsondunn.com

Cassandra L Gaedt-Sheckter
cgaedt-sheckter@gibsondunn.com

Frances Waldmann
fwaldmann@gibsondunn.com

The GDR Insight Handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-235-0