GDR INSIGHT

HANDBOOK 2021

HANDBOOK

2021

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

GDR
INSIGHT

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

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at November 2020, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the editor – tom.webb@globaldatareview.com.

ISBN: 978-1-83862-266-4

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 second 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 datasets, and the intersection of privacy, data and antitrust. A chapter is dedicated to the use of artificial intelligence in cross-border forensic investigations.

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 November 2020. 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
November 2020

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, US 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 suggested approaches should be codified in law.[1]

Recent years saw a surge in debate about the role of governance and accountability 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. Between 2019 and 2020, there were a number of high-profile draft bills addressing the role of AI and how it should be governed at the US federal level, while US state and local governments continue to press forward with concrete legislative proposals regulating the use of AI. Likewise, the European Union has taken numerous steps to demonstrate its commitment toward the advancement of AI technology through funding,[2] while

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

[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

simultaneously pressing for companies and governments to develop ethical applications of AI.[3] However, in the first half of 2020, the effect of the unprecedented covid-19 pandemic stalled much of the promised legislative progress, and many of the ambitious bills intended to build a regulatory framework for AI have languished in committee and have not been passed.

Nonetheless, US federal, state and local government agencies continue to show a willingness to take concrete positions on the regulatory spectrum, including in light of recent events and social movements, 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-risk 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

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. Early this year, the EC also released the 'White Paper on Artificial Intelligence – A European approach to excellence and trust' on 19 February 2020. The White Paper outlines the EC's proposed comprehensive AI legislative framework to be put into place in late 2020, including investments in data and infrastructure and measures to strengthen the digital rights of individuals. The EC's policy measures aim to foster a European 'data economy' with common European data spaces, and will work with strategic sectors of the economy to develop sector-specific solutions. EC, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 (19 February 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[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. Expanding on HLEG's findings, Germany's Data Ethics Commission released its report containing 75 recommendations for regulating data, algorithmic systems and AI. German Federal Ministry for Justice and Consumer Protection, Opinion of the Data Ethics Commission, Executive Summary (October 2019), available at http://bit.ly/373RGql. This report is a blueprint of binding legal rules for AI in Europe with varying regulatory obligations based on an algorithmic system's risk of harm. Id., at 19-20. The Ethics Commission recommends an overhaul of product liability laws as they pertain to autonomous technologies, such as adding vicarious liability for human operators of algorithmic systems that cause harm. Id., at 10. The Ethics Commission also notices companies using AI software that measures may be taken against 'ethically indefensible uses of data,' which may include 'total surveillance, profiling that poses a threat to personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, methods of influencing political elections that are incompatible with the principle of democracy, vendor lock-in and systematic consumer detriment, and many practices that involve trading in personal data.' Id., at 26.

[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. Indeed, after this hearing, separate legislation was introduced to require the Department of Homeland Security to report on deepfakes (the Senate passed S. 2065 on 24 October 2019) and to require NIST and NSF support for research and reporting on generative adversarial networks (HR 4355 passed the House on 09 December 2019).

welcome. Even so, there is an inherent risk that reactionary legislative responses will result in a disharmonious, fragmented national regulatory framework. Such developments will continue to 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, antitrust and labour-related immigration laws. While some of these areas may help alleviate ethical concerns that AI sometimes engenders (eg, eliminating bias), others may unnecessarily inhibit development and make it difficult to operate (eg, complying with consumer deletion requests under privacy laws or securing the workforce needed to develop AI technology).

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.

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, research and federal policy

Even in 2020, 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

[5] The only notable legislative proposal before 2019 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 was reintroduced on 9 July 2020 by Representatives Pete Olson (R-TX) and Jerry McNerney (D-CA) as the FUTURE of Artificial Intelligence Act of 2020. The House bill (HR 7559) would require the Director of the National Science Foundation, in consultation with the Director of the Office of Science and Technology Policy, to establish an advisory committee to advise the President on matters relating to the development of AI. A similar bill in the Senate (S. 3771), also titled FUTURE of Artificial Intelligence Act of 2020, was introduced by bipartisan lawmakers on 20 May 2020 and was ordered to be reported with an amendment favourably on 22 July 2020 after passing the Senate Committee on Commerce, Science, and Transportation.

[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://

2030. 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.[7]

In 2019, the federal government 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',[8] 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.[9] The EO, which was titled 'Maintaining American Leadership in Artificial Intelligence,' outlined five key areas: research and development,[10]

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] 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.

[8] 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.

[9] 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.

[10] 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.').

'unleashing' AI resources,[11] establishing AI governance standards,[12] building an AI workforce,[13] and international collaboration and protection.[14] 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. The long-term impact will be in the actions recommended and taken as a result of those consultations and reports, not the EO itself.[15] Moreover, although the AI Initiative is designed to dedicate resources and funnel investments

[11] 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').

[12] 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.

[13] 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.

[14] 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.

[15] 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). The draft outlines OMB's proposed 'light-touch' regulatory approach and features 10 AI Principles for agencies to follow, including building public trust in AI and including public participation in the formation of regulations, maintaining scientific integrity, risk assessment and management, balancing benefit with cost, creating flexible regulatory approaches, fairness and non-discrimination, disclosure and transparency, safety and security, and interagency coordination. Director of the Office of Management and Budget, Guidance for Regulation of Artificial Intelligence Applications (7 January 2020), available at https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf. The comment period on the draft closed 13 March 2020, and the final memorandum is forthcoming.

into AI research, the EO does not set aside specific financial resources or provide details on how available resources will be structured.[16] In the American AI Initiative Year One Report, issued in February 2020, the Trump Administration announced that it would double the funding for the AI Initiative's R&D for the next two years.[17] This report follows from the prior launch of ai.gov, 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 after the EO, 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 was referred to the House Committee on Science, Space, and Technology but has not progressed.

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

[16] 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).

[17] The White House Office of Science and Technology Policy, American Artificial Intelligence Initiative: Year One Annual Report (Feb 2020), available at https://www.whitehouse.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.

[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, datasets 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 datasets 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 2202, 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.

[20] S. 1558 – Artificial Intelligence Initiative Act, 116th Cong (2019–2020).

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] While the bill also has not been passed, further legislation introduced in the House of Representatives in March 2020 – the National Artificial Intelligence Initiative Act – would establish a National Artificial Intelligence Initiative to promote AI research and interagency cooperation and to develop AI best practices and standards to ensure US leadership in the responsible development of AI.[23] The Act, the most ambitious attempt by Congress to advance the development of AI in the United States, would also authorise over $1.1B of funding over the next five fiscal years. Further, the National Cloud Computing Task Force Act proposes a task force to plan a national cloud computing system for AI research to provide students and researchers across scientific disciplines with access to cloud computing resources, government and non-government datasets and a research environment.[24]

May 2020 saw the introduction of the Generating Artificial Intelligence Networking Security (GAINS) Act, which directs the Department of Commerce and the Federal Trade Commission to identify the benefits and barriers to AI adoption in the United States; survey other nations' AI strategies and rank how the United States compares; and assess the supply chain risks and how to address them.[25] The bill requires the agencies to report the results to Congress, along with recommendations to develop a national AI strategy. After previously expressing reluctance due to fears that the initiative's recommendations would harm

[21] The bill also establishes the National AI Research and Development Initiative to identify and minimise 'inappropriate bias and datasets 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 datasets, 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. Similar legislation, the Advancing Artificial Intelligence Research Act of 2020, was introduced on 4 June 2020 by Senator Cory Gardner. The Act establishes the National Program to Advance Artificial Intelligence Research under NIST to support research and development of technical standards and guidelines that promote the US's AI goals. See S. 3891, 116th Cong (2nd Sess 2020). Finally, the AI Scholarship-for-Service Act (S. 3901) provides AI practitioners, data engineers, data scientists, and data analysts with higher education scholarships in exchange for a commitment to work for a federal, state, local, or tribal government, or a state, local, or tribal-affiliated non-profit deemed as critical infrastructure.

[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 6216, 116th Cong (2nd Sess 2020). If passed, the bill would authorise $391 million for the National Institute of Standards and Technology (NIST) to develop voluntary standards for trustworthy AI systems, establish a risk assessment framework for AI systems and develop guidance on best practices for public-private data sharing.

[24] S. 3890, 116th Cong (2019–2020). A companion bill (H.R. 7096) has been introduced in the House.

[25] H.R. 6950, 116th Cong (2019–2020).

innovation, on 28 May 2020, the US Department of State announced that the United States had joined the Global Partnership on AI – becoming the last of the Group of Seven (G7) countries to sign on – reportedly 'as a check on China's approach to AI.'

In September 2020, the AI in Government Act of 2020 (H.R. 2575) was passed by the House by voice vote. The bill aims to promote the efforts of the federal government in developing innovative uses of AI by establishing the 'AI Center of Excellence' within the General Services Administration (GSA), and requiring that the Office of Management and Budget (OMB) issue a memorandum to federal agencies regarding AI governance approaches. It also requires the Office of Science and Technology Policy to issue guidance to federal agencies on AI acquisition and best practices. Just a few days later, House Representatives introduced a concurrent resolution calling for the creation of a cohesive national AI strategy, based on four pillars: workforce; national security; research and development; and ethics.

Congress has also 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.'[26] Similar to California's adoption last year of the Asilomar Principles[27] and the OECD's recent adoption of five 'democratic' AI principles,[28] 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 put 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.

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.[29]

[26] HR Res 153, 116th Cong (1st Sess 2019).

[27] 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).

[28] 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.

[29] HR 827 – AI JOBS Act of 2019, 116th Cong (2019), available at https://www.congress.gov/bill/116th-congress/house-bill/827/text. Another proposal introduced on 19 May 2020, the Generating Artificial Intelligence Networking Security Act, would fund a Department of Commerce study on the impact of artificial intelligence on interstate commerce. See HR 6950, 116th Cong (2nd Sess 2020).

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 and the bill has not progressed.[30]

Regulation of AI technologies and algorithms

Intellectual property

Issuing a long-anticipated decision, the US Patent and Trademark Office (USPTO) accelerated efforts to support private-sector AI development in late 2019. The USPTO requested public comment on patent-related AI issues, including whether AI could be considered an inventor on a patent.[31] Following the lead of the European Patent Office, and in light of its public comment process, the USPTO ruled in April 2020 that only natural persons, not AI systems, can be registered as inventors on a patent.[32] This decision has the potential to put into dispute any inventions developed in conjunction with AI, as it could be argued whether a natural person was close enough to the invention to claim credit.[33]

Transparency and algorithmic bias

Over the past several years, US lawmakers have proposed pieces of legislation that seek to regulate AI, with a focus on pursuing transparency, accountability and 'explainability' in the face of emerging risks such as harmful bias and other unintended outcomes. 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

[30] The AI in Government Act is comprised of corresponding bills introduced in the Senate and House introduced on 8 May 2019 which would establish an 'AI Center of Excellence' within the General Services Administration. The AI Center of Excellence would assist the implementation of AI in federal government agencies and provide guidance to agencies on implementing AI while protecting civil liberties and identifying and mitigating discriminatory bias or other unintended consequences of AI. See HR 2575, 116th Cong (2019); S. 1363, 116th Cong (2019).

[31] Laura Peter (Deputy Director of the USPTO), Remarks Delivered at Trust, but Verify: Informational Challenges Surrounding AI-Enabled Clinical Decision Software (23 January 2020), available at https://www.uspto.gov/about-us/news-updates/remarks-deputy-director-peter-trust-verify-informational-challenges.

[32] See USPTO Decision on Petition In Re Application No. 16/524,350, available at https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf?utm_campaign=subscriptioncenter&utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=. See also Jon Porter, 'US Patent Office Rules that Artificial Intelligence Cannot Be a Legal Inventor', The Verge (29 April 2020), available at https://www.theverge.com/2020/4/29/21241251/artificial-intelligence-inventor-united-states-patent-trademark-office-intellectual-property.

[33] Jon Porter, 'US Patent Office Rules that Artificial Intelligence Cannot Be a Legal Inventor', The Verge (29 April 2020), available at https://www.theverge.com/2020/4/29/21241251/artificial-intelligence-inventor-united-states-patent-trademark-office-intellectual-property.

human activity online'.[34] 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, which has not progressed, 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.

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.'[35] 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. 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 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'.[36] The bill has not progressed but represent 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.

[34] 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.

[35] 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).

[36] 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.

On 31 October 2019, a bipartisan group of senators introduced the Filter Bubble Transparency Act.[37] The bill would require large-scale internet platforms to provide greater transparency to consumers by providing clear notice on the use, and enabling consumers to opt out, of personalised content curated by 'opaque' algorithms so that they can 'engage with a platform without being manipulated by algorithms driven by user-specific data' and 'simply opt out of the filter bubble.'[38] 'Filter bubble' refers to a zone of potential manipulation that exists within algorithms that curate or rank content in internet platforms based on user-specific data. The proposed legislation covers 'any public-facing website, internet application, or mobile application,' such as social network sites, video-sharing services, search engines and content aggregation services, and generally would prohibit the use of opaque algorithms without notice to the user.[39] Like the Algorithmic Accountability Act, the bill is squarely targeted at 'Big Tech' platforms – it would not apply to platforms wholly owned, controlled and operated by a person that did not employ more than 500 employees in the past six months, averaged less than $50 million in annual gross receipts and annually collects or processes personal data of less than a million individuals.[40]

However, there still are no presently enacted federal regulations that specifically apply to AI technology. While a number of bills have been introduced, many of them are contradictory or at odds with each other in their requirements, and the covid-19 pandemic and upcoming election has obviously changed much of the focus of federal lawmakers. As we head into 2021 and what will hopefully be a return to something more closely resembling what we previously viewed as 'normal,' it will be interesting to see whether the momentum toward AI regulation returns in Congress.

By contrast, state legislatures have now passed several laws directly regulating AI. California passed a bill in September 2018, the 'Bolstering Online Transparency Act',[41] 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.

[37] Filter Bubble Transparency Act, S. 2763, 116th Cong (2019). This Act would be the first substantive federal bill aimed at regulating algorithmic control of content on internet platforms.

[38] Marsha Blackburn, US Senator for Tennessee, 'Blackburn Joins Thune on Bipartisan Bill to Increase Internet Platform Transparency & Provide Consumers with Greater Control Over Digital Content', (31 October 2019), https://www.blackburn.senate.gov/blackburn-joins-thune-bipartisan-bill-increase-internet-platform-transparency-provide-consumers.

[39] S. 2763, 116th Cong (2019).

[40] S. 2763, 116th Cong (2019). New Jersey introduced similar legislation in May 2019. New Jersey Algorithmic Accountability Act, AB 5430, 218th Leg, 2019 Reg Sess (NJ 2019).

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

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.[42] 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 the John S. McCain National Defense Authorization Act for 2019 (the 2019 NDAA),[43] 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.[44] 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.[45] 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,[46] the JAIC will work with the Defense Advanced Research Projects Agency (DARPA),[47]

[42] 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.

[43] https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

[44] id.

[45] See Cronk, Terri Moon, 'DOD Unveils Its Artificial Intelligence Strategy' (12 February 2019), available 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.

[46] 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).

[47] 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

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.[48]

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.[49] 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.[50] 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.[51]

Several recent proposed bills at the federal level seek to increase funding and develop AI innovation in the United States defence sector. On 16 June 2020, Senators Rob Portman (R-OH) and Martin Heinrich (D-NM), the co-founders of the Senate Artificial Intelligence Caucus, introduced the bipartisan Artificial Intelligence for the Armed Forces Act which, if enacted, would further strengthen the Department of Defense's AI capacity by increasing the number of AI and cyber professionals in the department. The bill would require the defence secretary to develop a training and certification programme, and issue guidance on how the Pentagon could make better use of existing hire authorities to recruit AI talent.[52] For example, the Securing American Leadership in Science and Technology Act of 2020 (SALTA),[53] introduced in January 2020, would focus on 'invest[ing] in basic scientific research and support technology innovation for the economic and national security of the United States', which could encourage AI development, including for national security, in spite of challenges

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).

[48] 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

[49] 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.

[50] 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.

[51] 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.

[52] Artificial Intelligence for the Armed Forces Act, S. 3965, 116th Cong (2020).

[53] Securing American Leadership in Science and Technology Act, HR 5685, 116th Cong (2020).

discussed in the 'Labour' section below. Finally, in July 2020, the House passed the National Defense Authorization Act for Fiscal Year 2021, which directs the US Comptroller General to provide Congress with an assessment of DoD's resources, capabilities and plans regarding AI, and mandates the development of standard data formats and cooperative agreements for data sharing within DoD.[54]

Healthcare

Unsurprisingly, the use of AI in healthcare draws some of the most exciting prospects and deepest trepidation, given potential risks. As of yet, there are few regulations directed at AI in healthcare specifically, but covid-19 has introduced additional complications relating to healthcare treatment and delivery options that may affect AI, and regulators acknowledge that existing frameworks for medical device approval are not well-suited to AI-related technologies.

Recent legislation – partly resulting from covid-related data collections – may limit the extent to which companies can use AI to deal with the business challenges posed by the coronavirus. Specifically, restrictions on the use of facial recognition technology and personal health data may restrict the ways that technology can be used to track the spread and impact of the virus. Employers have begun using thermal scans to admit employees into their workplaces and this technology can use a facial scan of the employee as part of the process.[55] Owners of large residential properties are considering the use of facial recognition technology to control and monitor the entrances to their buildings and prevent unauthorised entrants who might carry the coronavirus.[56] These practices could expose companies to significant legal risk in jurisdictions like Illinois, which requires that private entities provide notice and obtain written consent from employees or members of the public before collecting their biometric data, even for fleeting or temporary purposes like a facial recognition scan.[57] The Illinois Supreme Court has ruled a plaintiff need not show actual harm beyond a violation of his or her rights under the act, so private companies could face costly class actions able to pursue damages between $1,000 and $5,000 per class member in addition to attorney's fees.[58] Several bills currently before Congress would impose similar affirmative consent requirements for the use of facial recognition technology at the federal level.[59]

[54] H.R. 6395, 116th Cong (2020).

[55] Natasha Singer, 'Employers Rush to Adopt Virus Screening. The Tools May Not Help Much,' *The New York Times* (14 May 2020), available at https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html.

[56] Chris Arsenault, 'Forgot your keys? Scan your face, says Canadian firm amid privacy concerns,' Reuters (16 April 2020), available at https://www.reuters.com/article/us-canada-tech-homes-feature-trfn/forgot-your-keys-scan-your-face-says-canadian-firm-amid-privacy-concerns-idUSKBN21O1ZT.

[57] 740 Ill Comp Stat Ann 14/15.

[58] *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (Ill. 2019).

[59] See Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong (2019); Ethical Use of Facial Recognition Act, S. 3284, 116th Cong (2020) (discussed further below); COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong (2020).

Furthermore, the Protecting Personal Health Data Act would create a national task force on health data protection and require the Department of Health and Human Services to promulgate regulations for health information not currently covered by the Health Insurance Portability and Accountability Act (HIPAA), but which may be collected in light of the pandemic and used by businesses implementing AI technology.[60] The Smartwatch Data Act would prohibit companies from transferring or selling health information from personal consumer devices without the consumer's informed consent, including wearables and trackers.[61] Some academic commentators have called for emergent medical data, or personal data that does not explicitly relate to health but that can be used to derive conclusions about the individual's health using AI technology, to be regulated more strictly to make the treatment of this information consistent with the regulations imposed by HIPAA.[62]

And data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) itself would be subject to its Privacy Rule,[63] which 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 action.[64] While there are innumerable ways AI could be used (including used pursuant to exceptions), such limitations on use can affect the ability to develop AI related to healthcare.[65]

Relating to medical devices specifically, the US Food and Drug Administration (FDA) has also offered its views on regulating the use of AI in a proposed 2019 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.

Its 'Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)' – offered that new framework for regulating health products using AI, and sought comment.[66] If AI-based SaMDs

[60] Protecting Personal Health Data Act, S. 1842, 116th Cong (2019).

[61] Stop Marketing And Revealing The Wearables And Trackers Consumer Health Data Act, S. 2885, 116th Cong (2019).

[62] Mason Marks, Emergent Medical Data: Health Information Inferred by Artificial Intelligence, 11 UC Irvine L Rev (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3554118.

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

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

[65] 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.

[66] See, US Food & Drug Administration, Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machin learning (AI/ML)-Based Software as a Medical Device (SaMD), available at https://www.fda.gov/media/122535/download. The paper introduces that one of the primary benefits of using AI in an

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 proposed 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.[67] 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 those that would require pre-market review, defining 'Good Machine Learning Practices', and in what ways might a manufacturer can 'demonstrate transparency'. There has been little update on this programme since that time.

Facial recognition, biometric surveillance and 'deepfake' 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.[68] Like other biometric data, data involving facial geometries and structures is often considered some of the most

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'. 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. 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.

[67] 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). 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/.

[68] 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, note 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/.

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 sound alarms about problems with the underlying technology as well as potential or actual misuse by governmental authorities. While most 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, particularly in light of covid-19 and a resurgence in social movements relating to racial justice, such as the Black Lives Matter movement.

Such racial justice movements have caused federal and state legislatures to reconsider the use of facial recognition technology by government and police departments and propose legislation that would ban the use of this technology by the police more generally. For example, the proposed George Floyd Justice in Policing Act of 2020 reform package contains two bills that would affect the use of AI technology and facial recognition. The Federal Police Camera and Accountability Act would require federal law enforcement officers to wear body cameras, but the bill explicitly prohibits federal police from equipping these cameras with facial recognition technology.[69] The Police CAMERA Act of 2020 would provide grants for state, local, and tribal police to implement body camera technology, but it bars these grants from being used on facial recognition technology and mandates that a study be completed within two years examining, among other topics, 'issues relating to the constitutional rights of individuals on whom facial recognition technology is used.'[70] The Ethical Use of Facial Recognition Act – proposed in February 2020 – would prohibit any federal officer, employee, or contractor from using facial recognition in large part without a warrant until a congressional commission recommends rules to ethically govern such use.[71] And the National Biometric Information Privacy Act – introduced in August 2020 – would be the most comprehensive, as it is modelled after Illinois's Biometric Information Privacy Act, and includes a requirement to obtain consent from individuals prior to collecting or disclosing their biometric information, a private right of action (including with the potential for liquidated damages), and security provisions.[72]

In June 2020, the California legislature, under pressure from the ACLU and other civil rights groups, rejected a bill that would have expanded the use of facial recognition technology by state and local governments.[73] That bill would have allowed government entities to use facial recognition technology to identify individuals believed to have committed

[69] Federal Police Camera and Accountability Act, HR 7120, 116th Cong (2020).

[70] Police Creating Accountability by Making Effective Recording Available Act of 2020, HR 7120, 116th Cong (2020).

[71] Ethical Use of Facial Recognition Act, S. 3284, 116th Cong (2020) https://www.congress.gov/bill/116th-congress/senate-bill/3284.

[72] National Biometric Information Privacy Act, S. ____, 116th Cong (2020), available at https://www.merkley.senate.gov/imo/media/doc/20.08.04%20National%20Biometric%20Information%20Privacy%20Act.pdf'

[73] Thomas Macaulay, 'California blocks bill that could've led to a facial recognition police-state,' The Next Web (4 June 2020), available at https://thenextweb.com/neural/2020/06/04/california-blocks-bill-that-couldve-led-to-a-facial-recognition-police-state/.

a serious criminal offence.[74] As a safeguard, the bill provided for third-party controllers to test whether the facial recognition technology exhibits any bias across subpopulations and allowed members of the public to request that their image be deleted from the government database. Other states are similarly addressing facial recognition, including Maryland, which passed a bill banning the use of 'a facial recognition service for the purpose of creating a facial template during an applicant's interview for employment', unless the interviewee signs a waiver,[75] and Washington, which approved a bill curbing government use of facial recognition, requiring bias testing and training, and transparency regarding use.[76]

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.[77] Only the Illinois Biometric Information Privacy Act provides for a private right of action as a means of enforcement.[78] In addition, the California Consumer Privacy Act extends its protections to an individual's biometric information, including that used in facial recognition technology.[79] 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.[80]

[74] AB-2261, 2019–20 Reg Sess (Cal 2020).

[75] HB 1202, Reg Sess (Md 2020).

[76] SB 6280, Reg Sess (Wash 2020).

[77] See Illinois 'Biometric Information Privacy Act', 740 ILCS 14/1 (PA 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'.

[78] 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).

[79] 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).

[80] https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states; eg, New York SHIELD Act, S. 110 Gen Assemb (2020).

Further, responses from businesses may turn out to be a substantial factor in deterring use of AI in a way that might perpetuate bias or infringe on civil liberties. A number of prominent technology companies have voiced their strong support for the Black Lives Matter movement, including IBM, which announced that it would discontinue its facial recognition products over concerns about bias in the technology and its possible infringement on civil liberties.[81]

More recently, 'deepfakes' – the output of generative adversarial networks, software systems designed to be trained with authentic inputs (eg, photographs) to generate similar, but artificial, outputs (deepfakes) – have also emerged as a high-risk use case. The Identifying Outputs of Generative Adversarial Networks (IOGAN) Act was introduced in the House in September 2019 and, if enacted, would direct the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to support research on the authenticity of manipulated or synthesised media and spur the development of standards.[82]

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[83] in September 2017, but its companion bill (the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act),[84] 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.[85]

Since late 2019, lawmakers have pushed to coalesce around new draft legislation regulating AVs. On 11 February 2020, the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, held a hearing entitled 'Autonomous Vehicles: Promises and Challenges of Evolving Automotive Technologies'.[86] At the hearing, witnesses expressed concerns that because of the lack of federal regulation, the US is falling behind in both the competitive landscape and in establishing comprehensive safety standards.[87] The

[81] Emily Birnbaum, 'How the Democrats' police reform bill would regulate facial recognition,' Protocol (8 June 2020), available at https://www.protocol.com/police-facial-recognition-legislation.

[82] H.R. 4355, 116th Cong (2019).

[83] HR 3388, 115th Cong (2017).

[84] 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.

[85] 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.

[86] House Committee on Energy and Commerce, Re: Hearing on 'Autonomous Vehicles: Promises and Challenges of Evolving Automotive Technologies' (7 February 2020), available at https://docs.house.gov/meetings/IF/IF17/20200211/110513/HHRG-116-IF17-20200211-SD002.pdf.

[87] The Hill, 'House lawmakers close to draft bill on self-driving cars' (11 February 2020), available at https://thehill.com/policy/technology/482628-house-lawmakers-close-to-draft-bill-on-self-driving-cars; Automotive

House Panel released a bipartisan draft bill shortly after the hearing, including a previously unreleased section on cybersecurity requirements.[88] The short window for feedback on the draft bill closed on 21 February 2020, and the legislation has not yet been introduced at the time of writing.[89]

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 January 2020, the DoT published updated guidance for the regulation of the autonomous vehicle industry, 'Ensuring American Leadership in Automated Vehicle Technologies' or 'AV 4.0.'[90] The guidance builds on the AV 3.0 guidance released in October 2018, which introduced guiding principles for AV innovation for all surface transportation modes, and described the DoT's strategy to address existing barriers to potential safety benefits and progress.[91] AV 4.0 includes 10 principles to protect consumers, promote markets and ensure a standardised federal approach to AVs. In line with previous guidance, the report promises to address legitimate public concerns about safety, security and privacy without hampering innovation, relying strongly on the industry self-regulating. However, the report also reiterates traditional disclosure and compliance standards that companies leveraging emerging technology should continue to follow.

In March 2020, the NHTSA issued its first-ever Notice of Proposed Rulemaking 'to improve safety and update rules that no longer make sense such as requiring manual driving controls on autonomous vehicles.'[92] The Notice aims to 'help streamline manufacturers' certification processes, reduce certification costs and minimize the need for future NHTSA interpretation or exemption requests.' For example, the proposed regulation would apply front passenger seat protection standards to the traditional driver's seat of an AV, rather than safety requirements that are specific to the driver's seat. Nothing in the Notice would make changes to existing occupant protection requirements for traditional vehicles with manual controls.[93]

News, 'Groups call on U.S. lawmakers to develop "meaningful legislation" for AVs' (11 February 2020), available at https://www.autonews.com/mobility-report/groups-call-us-lawmakers-develop-meaningful-legislation-avs.

[88] Previously released draft bill includes sections on federal, state and local roles, exemptions, rulemakings, FAST Act testing expansion, advisory committees and definitions, https://www.mema.org/draft-bipartisan-driverless-car-bill-offered-house-panel.

[89] Jessica Wehrman, Draft of Bipartisan Driverless Car Bill Offered by House Panel, Roll Call (13 February 2020), available at: https://www.rollcall.com/2020/02/13/draft-of-bipartisan-driverless-car-bill-offered-by-house-panel/.

[90] US Dep't of Transp, Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0 (January 2020), available at https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf.

[91] US Dep't 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.

[92] US Dep't of Transp, NHTSA Issues First-Ever Proposal to Modernize Occupant Protection Safety Standards for Vehicles Without Manual Controls, available at https://www.nhtsa.gov/press-releases/adapt-safety-requirements-ads-vehicles-without-manual-controls.

[93] 49 CFR 571 (2020), available at https://www.federalregister.gov/documents/2020/03/30/2020-05886/occupant-protection-for-automated-driving-systems.

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,[94] NHTSA announced that it was seeking comments about the possibility of removing 'regulatory barriers' relating to the introduction of automated vehicles in the United States.[95] 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.[96] 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

[94] 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.

[95] 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). The public comment period has closed, and 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). Meanwhile, regulators granted the first exception from FMVSSs to Nuro, a self-driving delivery vehicle startup, in February 2020. The exemption is conditional on Nuro's compliance with mandatory reporting and community outreach requirements. See https://www.nhtsa.gov/press-releases/nuro-exemption-low-speed-driverless-vehicle; https://www.theverge.com/2020/2/6/21125358/nuro-self-driving-delivery-robot-r2-fmvss-exemption.

[96] 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). See 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. On 27 March 2020, Governor Inslee signed HB 2676 into law, which established minimum requirements for AV testing in Washington. The requirements include liability insurance, advance notification to local and state law enforcement, and annual incident reporting. Notably absent is a provision regarding the presence of a human operator. See 2020 Wash Sess Laws, Ch 182. Pennsylvania, which last year passed legislation creating a commission on 'highly automated vehicles', has proposed a bill that would authorise the use of an autonomous shuttle vehicle on a route approved by the Pennsylvania Department of Transportation. HB 1078, 2019–2020 Reg Sess (Pa 2019). (The PA proposal comes from the 2019 Annual Update).

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.[97] California is generally 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.[98] 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.[99] In the California legislature, two new bills related to AVs have been introduced: SB 59[100] would establish a working group on autonomous passenger vehicle policy development while SB 336[101] would require transit operators to ensure certain automated transit vehicles are staffed by employees (both bills remain in committee at the time of writing). 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.[102] However, some US states have established provisions for liability in the event of a crash.[103]

Also at the local level, some states expressly forbid local governments from prohibiting pilot programmes within the state (eg, Oklahoma,[104] 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).[105]

[97] 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/.

[98] 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.

[99] 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.

[100] SB 59, 2019–2020 Reg Sess (Cal 2019).

[101] SB 336, 2019–2020 Reg Sess (Cal 2019).

[102] 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.

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

[104] 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).

[105] 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

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), which took effect on 1 January 2020, the New York Privacy Act (which lost steam midway through 2019, but was referred again to the Consumer Affairs and Protection Committee) and the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act. 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.

Most of the recently proposed and pending state privacy bills would not regulate AI technologies directly, but may do so with respect to transparency and consumer rights with respect to the data use in such technologies.[106] For example, New York's reintroduced Privacy Act 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 particular circumstances, such as with authorisation from the government.[107] Here, 'profiling' is broadly defined as '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 analyze or predict 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 about the logic involved, and the significance and envisaged consequences of the profiling.' Companies using AI technologies may find solace in a potentially significant carve-out through the use of the term 'solely' though – as with GDPR – if there is human intervention at some point in the decision-making process, then the regulation is not invoked.[108] Washington's proposed Privacy Act, (which was widely expected to pass, but has now been proposed twice, and failed each time) included very similar provisions. While additional states may develop their own legislation consistent with this framework, many state proposals may also stay silent on automated processing issues specifically, similar to the CCPA.[109]

[106] See SF 2912 (Minn 2019) in Minnesota, and SB 5376, 66th Leg, Reg Session (Wash 2019) in Washington.

[107] New York Privacy Act, A8526/S5642, Reg Sess (NY 2020).

[108] 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').

[109] SB 6281, 66th Leg, Reg Session (Wash 2019), available at http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376.pdf.

In either case – whether the law has provisions specific to AI or not – broadly applicable privacy laws are often fundamentally at odds with AI, and likely to generate headaches for companies developing and using AI technologies.[110] Fundamentally, AI technologies require large datasets, and those datasets are likely to contain some elements of personal information. This may trigger an avalanche of requirements under privacy laws.[111] 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 still unclear how these exceptions will be applied, and whether an entity can use the exceptions as a broad permission to include data in the datasets. Further, consumers' right to transparency of what data is collected, how it is used, and where it originates, may also 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. The uncertainty of this law's effect is compounded by the fact that the California Attorney General's office has just begun enforcement, amendments to the CCPA continue to be proposed and a ballot initiative for California voters in November could overhaul the CCPA.[112]

[110] 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.

[111] 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.

[112] 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/. The California Privacy Rights Act (CPRA) obtained enough signatures to place it on the California ballot for voters in November. While the CPRA would impose additional obligations on businesses, it also extends the business-to-business and employment-related data exemptions. Geoffrey A Fowler, 'The Technology 202: Privacy advocates battle each other over whether California's Proposition 24 better protects consumers', Washington Post.

Other recent decisions and laws similarly may affect the ability to use data freely as may be required for AI development. The New York SHIELD Act took effect 21 March 2020, and amends the state's data breach notification law to impose additional data security and breach notification requirements on covered businesses to protect New York residents, including to ensure safeguards from their vendors as well. And companies previously permitted to transfer data – eg, for AI programmes – from the EU in light of the US-EU Privacy Shield are now facing additional hurdles in light of the Schrems II decision invalidating that mechanism. With more data comes more vulnerability, making AI companies particularly at risk of litigation for cybersecurity incidents and non-compliance with security and data transfer requirements.

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 the potential of bias (smaller datasets, 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'.

This wave of proposed privacy-related federal and state regulation is likely to continue As a result, companies developing and using AI are certain to be focused on these issues in the coming months, and will be tackling how to balance these requirements with further development of their technologies.[113]

Discrimination

While the federal discrimination laws the United States Equal Employment Opportunity Commission (EEOC) enforces[114] – and their guidelines – have not changed, AI is recognised as a new medium for such discrimination.

Indeed, senators and agencies – including the EEOC itself – are pushing to ensure that AI technology is held accountable to prevent discrimination based on bias. For example, the EEOC is reportedly investigating claims of algorithms used in hiring, promotion and

[113] Various federal bills are also likely to affect AI companies, including the Consumer Data Privacy and Security Act of 2020 (CDPSA), S. 3456 116th Cong (2020). The CDPSA proposes a comprehensive data privacy framework that incorporates concepts from CCPA and GDPR, and covers obligations with respect to consent, transparency, and legitimate means for processing data. The Consumer Online Privacy Rights Act (COPRA) proposed in December 2019, also a comprehensive data protection law, specifically puts obligations on algorithmic decision-making, including annual impact assessments. COPRA, S. 2968 116th Cong (2019). These could both hinder the collection and use of information for building AI algorithms.

[114] 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).

other job decisions in a manner that discriminated against certain groups of individuals.[115] And US senators have been putting increasing pressure on agencies over the last couple of years to ensure they are doing their part to sufficiently investigate companies' use of AI in decision-making.[116]

The concerns raised are not theoretical, but based on an already realised dilemma, as various human resources and financial lending tools have fallen susceptible to inadvertent biases.[117]

Various racial justice movements, such as Black Lives Matter, have also caused federal and state legislatures to reconsider the use of facial recognition technology by government and police departments, as discussed further above.

[115] Chris Opfer and Ben Penn, 'Punching In: Workplace Bias Police Look at Hiring Algorithms', Bloomberg Law (28 October 2019).

[116] 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. 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). The letter cites various studies showing that facial recognition algorithms are significantly less accurate for darker-skinned individuals, and discusses legal scholars' views on how such algorithms may 'violate workplace anti-discrimination laws, exacerbating employment 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. 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. Further, in late 2019, senators sent letters to the FTC and Centers for Medicare and Medicaid Services questioning their efforts to investigate healthcare companies regarding biased decision-making, including relating to prioritisation of healthcare. See eg, Tom Simonite, 'Senators Protest a Health Algorithm Biased Against Black People', WIRED, (03 December 2019) https://www.wired.com/story/senators-protest-health-algorithm-biased-against-black-people/. 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'. 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.

[117] See, eg, Jeffrey Dastin, 'Amazon scraps secret AI'. The tool has since been decommissioned. See, eg, Tom Simonite, 'Senators Protest a Health Algorithm Biased Against Black People', WIRED, (3 December 2019) (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').

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. We may also see additional legislative proposals that seek to directly regulate algorithmic bias.

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 datasets for use in the development of machine learning systems. Such breakups could make the United States less competitive in its AI race with some of its geopolitical rivals as well, as the broken up companies will have access to smaller datasets, which will hinder AI innovation, and companies from other countries, such as China, are less likely to be subject to antitrust action.[118]

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.'[119] The DOJ indicated that it intends to continue its investigation of Alphabet's alleged anticompetitive practices during the pandemic, and the Attorney General plans to reach a decision on whether to bring antitrust actions against large technology firms during the summer of 2020.[120] The Federal Trade Commission continues to investigate online platforms,[121] and the House Judiciary Committee opened a bipartisan investigation into competition in digital markets, which includes holding hearings and subpoenaing

[118] Dakota Foster, 'Antitrust Investigations have Deep Implications for AI and National Security,' The Brookings Institute (2 June 2020), available at https://www.brookings.edu/techstream/antitrust-investigations-have-deep-implications-for-ai-and-national-security/. See also Nitisha Tiku, 'Big Tech: Breaking Us Up Will Only Help China,' Wired (23 May 2019), available at https://www.wired.com/story/big-tech-breaking-will-only-help-china/.

[119] 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.

[120] Sadie Gurman, 'Barr Strives to Keep Justice Moving Amid Coronavirus Crisis,' The Wall Street Journal (23 March 2020), available at https://www.wsj.com/articles/barr-strives-to-keep-justice-moving-amid-coronavirus-crisis-11584955802.

[121] 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; Federal Trade Commission, 'FTC to Examine Past Acquisitions by Large Technology Companies', (11 February 2020), https://www.ftc.gov/news-events/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies

documents.[122] Indeed, the House Judiciary antitrust subcommittee held an almost six-hour virtual hearing in July 2020 to question leaders of the most prominent technology companies.[123] 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.[124] 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.[125]

Labour

2020 will be marked by the covid-19 pandemic in many regards, including relating to unprecedented restrictions on travel and immigration. Given these limitations, and US tensions with China, companies developing AI may find it more difficult to recruit and retain top talent necessary for successful programmes.

Fallout from covid-19 and geopolitical concerns has led to a significant decrease in the ability of skilled workers to enter the US. In response to record unemployment numbers caused by the coronavirus pandemic, the Trump administration announced that it would largely suspend the issuance of new H-1B and some other non-immigrant visas until 31 December 2020, preventing new skilled workers from entering the country to work for the rest of this calendar year.[126] The administration has also extended a suspension of the issuance of employment-based green cards until the end of 2020, including those reserved for professionals with advanced degrees, which could reduce the number of new green cards issued in 2020 by one-third.[127] And since 2018, the State Department has restricted student

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

[123] Danielle Abril, 'Facebook and Amazon grilled over history of aggressive competitive practices at antitrust congressional hearing,' (29 July 2020).

[124] 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.

[125] 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.

[126] Suspension of Entry of Immigrants and Nonimmigrants Who Present a Risk to the United States Labor Market During the Economic Recovery Following the 2019 Novel Coronavirus Outbreak, 85 Fed Reg 38,263 (25 June 2020).

[127] id. (extending Suspension of Entry of Immigrants Who Present a Risk to the United States Labor Market During the Economic Recovery Following the 2019 Novel Coronavirus Outbreak, 85 Fed Reg 23,441 (27 April 2020)); Daniel Costa, 'Trump executive order to suspend immigration would reduce green cards by nearly one-third if extended for a full year,' Economic Policy Institute Working Economics Blog (23 April 2020), available at https://www.epi.org/blog/trump-executive-order-to-suspend-immigration-would-reduce-green-cards-by-nearly-one-third-if-extended-for-a-full-year/.

visas for Chinese graduate students seeking to pursue degrees in 'sensitive subjects,' requiring these students to renew their visa every year, instead of the prior practice of granting five-year visas.[128] In June 2020, the administration announced that it would bar the entry of any Chinese graduate student or researcher who previously served in the People's Liberation Army or attended a university affiliated with it, owing to concerns about theft of sensitive intellectual property.[129]

These actions are particularly relevant because the United States' dominance in AI research has been sustained in part by the ability of American companies and universities to attract talent from abroad, particularly from China. A recent study of participants in a major AI conference found that 60 per cent of the presenters currently work in the US, but two-thirds of those researchers obtained their undergraduate degree outside of the US.[130] AI research is particularly affected by the human capital of the teams developing a company's product rather than the IP that the company owns: '[r]esearchers generally publish what they find, and anybody can use it. So what the industry is looking for is not intellectual property but the minds that conduct the research.'[131] Rising geopolitical tensions between the United States and China, as well as related immigration restrictions, could further constrict the flow of labour and prevent American universities and companies from recruiting top AI talent, which necessarily could curb the US's success in AI development.

Conclusion

Discussion around regulating AI technologies has continued to expand over the past year, resulting in additional proposals across sectors from local and federal legislatures. However, while few AI-specific laws were actually passed by legislative bodies, those that have passed, as well as pending regulations and policies, still 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 recently enacted privacy regulation, may have an unintentional disparate impact on AI technologies, given their need for data. While it is still too soon to know for certain, 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

[128] Jeffrey Mervis, 'More restrictive U.S. policy on Chinese graduate student visas raises alarm,' Science (11 June 2018), available at https://www.sciencemag.org/news/2018/06/more-restrictive-us-policy-chinese-graduate-student-visas-raises-alarm.

[129] Suspension of Entry as Non-immigrants of Certain Students and Researchers From the People's Republic of China, 85 Fed Reg 34,353 (4 June 2020).

[130] Marco Polo, 'The Global AI Talent Tracker', available at https://macropolo.org/digital-projects/the-global-ai-talent-tracker/.

[131] Paul Mozer and Cade Metz, 'A U.S. Secret Weapon in A.I.: Chinese Talent', *The New York Times* (9 June 2020), available at https://www.nytimes.com/2020/06/09/technology/china-ai-research-education.html.

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 have changed dramatically.

The authors would like to acknowledge and thank Nicholas Venable and Amanda Sansone for their assistance and contribution to this chapter.

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 litigation attorney whose practice focuses on technology-driven disputes and encompasses complex commercial and antitrust litigation, investigations by US and international enforcement authorities, and regulatory compliance. She has experience litigating a wide range of complex disputes, including cross-border cases, often involving cutting edge technologies such as electronic devices, computer software and AI-based systems. Her antitrust experience includes the defence of civil class action lawsuits and cartel investigations by the US Department of Justice (DOJ) and global antitrust enforcers in industries including consumer electronics, transportation, automobile parts, telecommunications and financial services.

Ms Waldmann also counsels technology-focused clients on regulatory compliance, corporate governance and product liability issues with respect to the developing body of law on emerging technologies, data privacy and the sharing economy. She has particular expertise in legal, ethical and policy developments surrounding artificial intelligence and automation, and advises companies navigating the evolving regulatory landscape for technologies such as autonomous and connected vehicles. She spearheads Gibson Dunn's Quarterly Artificial Intelligence and Automated Systems Legal Update, and speaks and writes on matters relating to AI and automation.

Ms Waldmann is a member of the State Bars of California and New York, and the bar of England and Wales.

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 978-1-83862-266-4