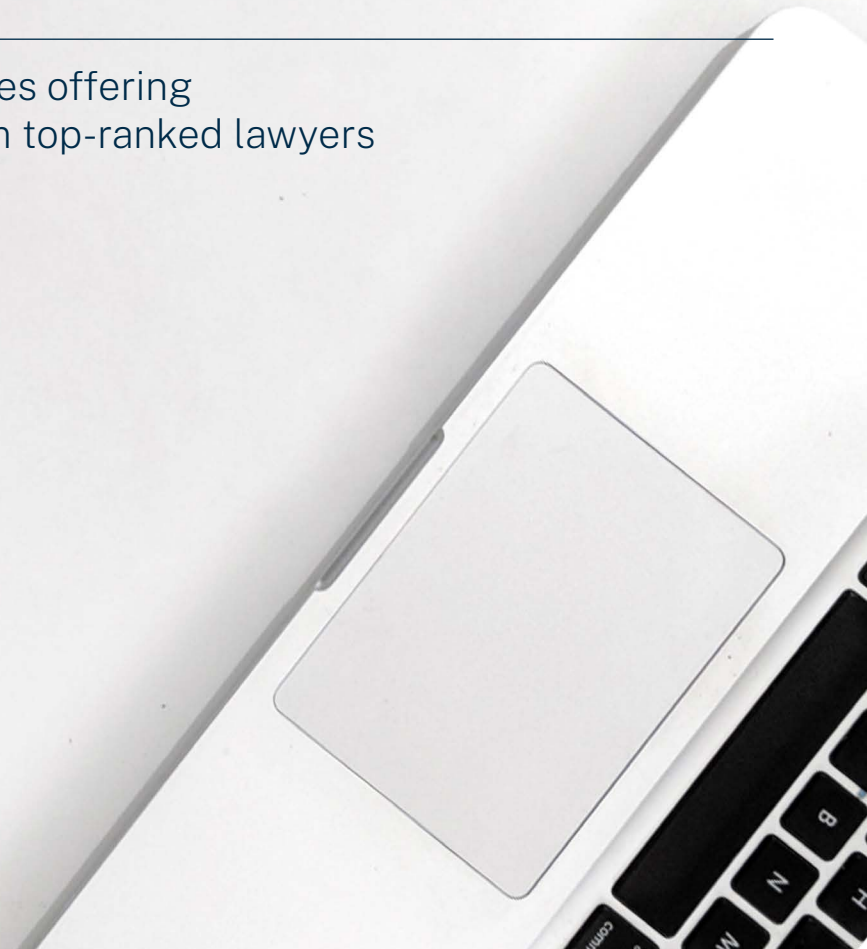
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers



Introduction
Alan Charles Raul
Sidley Austin LLP

INTRODUCTION

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Geneva, Hong Kong, Munich, Shanghai, Singapore, Sydney and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, tech, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, digital governance, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as the GDPR and CCPA; legislative and policy developments; and international data transfers.

Contributing Editor

Alan Charles Raul is the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on US and international privacy, cybersecurity and technology issues. Alan advises on global regulatory compliance, data breaches, and crisis management. He also focuses on issues concerning national security, constitutional and administrative law. He handles enforcement and public policy issues involving the FTC, State Attorneys General, SEC, DOJ, FBI, DHS/CISA, the intelligence community, as well as other federal, state, and international agencies. Alan previously served in government as vice chairman of the Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, General Counsel of the US Department of Agriculture, and Associate Counsel to the President. Alan serves as a lecturer on Law at Harvard Law School, where he teaches courses on Digital Governance: Privacy and Technology Trade-offs and Cybersecurity Risks, Rules and Responsibilities. He is a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center, and the Council on Foreign Relations. He serves as Chairman of the governing Board of Directors of the Future of Privacy Forum.

INTRODUCTION

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Sidley Austin LLP

One South Dearborn
Chicago
Illinois
USA
IL 60603

Tel: +1 312 853 7000
Fax: +1 312 853 7036
Web: www.sidley.com

Global Approach to AI Policy: Who, and What Framework, Will Emerge as the World's Leader in AI Regulation

The future of privacy and data protection regulation around the world could soon be swamped by governance concerns over, as well as great enthusiasm for, artificial intelligence. Governments are increasingly focused on digital technology broadly, and not just personal information narrowly.

The deployment of sophisticated AI is challenging this global regulatory status quo, much in the same way it is having a transformative effect on the technology sector. For example, while many experts in the field have wondered whether advances in AI are compatible with the onerous privacy dictates of the GDPR, given the enormous data sets required for training and machine learning, some astute observers, such as Theodore Christakis, ask about the other side of the policy equation too: in the contest between the enormous benefits advanced AI offers society and the innovation-inhibiting impact of EU regulation, can the GDPR survive the allure of generative AI, notwithstanding the vast amount of data it demands?

The deployment of revolutionary large language models such as OpenAI's GPT series has catalysed a flurry of AI policymaking across the globe over the past year as leaders attempt to grapple with both the present and existential risks posed by powerful predictive systems. However, the question of who – and what framework – will emerge as the world's leader in AI regulation is not clear, given the uncertainty of exactly how advanced AI works, what it is capable of today, and what it will be able to do tomorrow. These kinds of open questions provide the United States with the opportunity, and perhaps the obligation, to assert leadership on the relevant global technology standards.

Indeed, it has become evident that either the United States has learned a lesson from its relative abstinence from global leadership on privacy policymaking, or AI is simply too important for America to stand on the international sidelines of AI governance. Alan Davidson, Assistant Secretary of Commerce for Communications and Information at the National Telecommunications and Information Administration, recently called President Biden's October 2023 AI executive order "the most ambitious government effort to date". He further remarked that a key difference between the American approach and

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

other efforts is that the executive order will allow officials to move more quickly as compared to comprehensive legislation, like the EU AI Act.

AI governance is further complicated because of the inescapably dual use of the technology; as hard as it will be to get a handle on commercial governance of AI, military applications will likely proceed on a separate track (potentially beyond conventional regulation).

Of course, the European Union appears to have forged ahead by reaching an agreement on a comprehensive AI Act, which regulates the development, use, import, and distribution of high-risk and limited-risk AI systems. But even there, negotiations were disrupted by the pace of technological change. The original text of the AI Act, proposed in 2021, did not account for the rise of so-called generative AI and, in particular, those foundational or general purpose models such as OpenAI's GPT series that can serve as a platform for other applications. European industry leaders began to urge officials to think more carefully before adopting suffocating regulations that could hamstring entrants in the sprint toward generative AI dominance. In any event, the European Parliament plenary vote on the final text of the EU AI Act will likely not occur until April.

As IAPP Research and Insights Director Joe Jones recently summarised, the AI Act's final text indicates that the obligations for high-risk systems enumerated in Annex III thereof, including for use in biometrics, critical infrastructure, education, employment, essential private and public services, law enforcement, immigration, and the administration of democratic processes, will not apply until 24 months after the Act comes into force. Obligations for those high-risk systems that form components of or are themselves products covered by the EU legislation listed in Annex II of the Act, and are required to undergo conformity assessments before being placed on the market, will not apply until 36 months after the Act comes into force. American agencies, by contrast, must meet a variety of substantive deadlines imposed by the Biden executive order before the end of 2024.

In another recent announcement regarding the creation of the US AI Safety Institute Consortium, which includes over 200 leading AI stakeholders, key Biden administration members highlighted the importance of US leadership. Secretary of Commerce Gina Raimondo noted, "[t]hrough President Biden's landmark Executive Order, we will ensure America is at the front of the pack" when it comes to setting AI safety standards and protecting the AI innovation ecosystem. Bruce Reed, White House Deputy Chief of Staff, further commented that "[t]o keep pace with AI, we have to move fast and make sure everyone – from the government to the private sector to academia – is rowing in the same direction. Thanks to President Biden's landmark Executive Order, the AI Safety Consortium provides a critical forum for all of us to work together to seize the promise and manage the risks posed by AI".

The plethora of federal initiatives adopted at the direction of the Biden executive order supports the conclusion that the United States intends to run ahead of the field on AI governance, analogous to its leadership on cybersecurity rules and governance. The White House recently confirmed that every 90-day deadline set forth by the order has been met. Notably, "developers of the most powerful AI systems" are already required "to report vital information" to the Department of Commerce (ie, the order is self-executing in this regard), including the results of safety testing. Nine agencies have submitted risk assessments

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

to the Department of Homeland Security regarding the use of AI in critical infrastructure.

The intense level of agency engagement called for by President Biden led the order to be viewed by some in Congress and industry as too powerful, triggering a "campaign to take [it] down," or "defang the industry-facing sections". Nevertheless, the United States appears to be forging ahead with asserting influence over governance standards for frontier AI models both domestically and abroad.

The UK, in contrast to the EU's characteristically precautionary and prescriptive posture, had already announced a pro-innovation approach to AI in March 2023. On 12 February 2024, the Department for Science, Innovation, and Technology, followed up this policy with a long-anticipated response to the March 2023 White Paper to build out an approach to AI governance that is "is strongly pro-innovation and pro-safety". The February publication further examined the case for "new responsibilities for developers of highly capable general-purpose AI systems" with an eye towards a "more international approach to safety, where we collaborate with partners to ensure [frontier] AI systems are safe before they are released".

Reflecting the importance of this internationalist approach, the UK hosted a global AI Safety Summit at Bletchley Park. The impetus for the summit was to focus world leaders' attention on the need for co-operation regarding the systemic risks that powerful AI could pose for global society at least as much as on the international competition to innovate. Building on the momentum of the Biden executive order, however, the United States did not take a back seat at the summit and instead exerted its influence over the direction of the talks. For example, Vice President Kamala Harris's remarks upon arriving in the UK for the Bletchley Park summit signalled the Biden administration's intent to lead on all dimensions of AI, including international policy. She noted that American domestic AI policies, in development even before generative AI, are intended to "serve as a model for global policy, understanding that AI developed in one nation can impact the lives and livelihoods of billions of people around the world".

US global policy leadership on AI will likely play out based primarily on the Biden executive order issued just before the Bletchley Park summit, as well as on the other key developments discussed below. What is also clear, though, is that this incipient, but muscular, US leadership on AI governance is being conceived with what appears to be a multilateral mindset. This bodes well for the possibility of moving toward meaningful convergence on standards for the world's most powerful "safety impacting" and "rights impacting" AI systems.

The Biden Administration's Executive Order on AI

Issued on 30 October 2023, the Biden administration's executive order on the "safe, secure, and trustworthy development and use of artificial intelligence" is one of the most significant federal efforts to regulate – or otherwise govern – information technology in modern history. Though it is not a self-contained, comprehensive piece of legislation such as the EU AI Act, the order has the immediate effect of directing federal agency resources toward assessing and addressing AI risk. As discussed above, the EU AI Act, by contrast, is not likely to come into full effect for the next several years.

The depth of President Biden's commitment to the project is reflected by the order's assign-

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

ment of critical responsibilities for execution to some of the administration's most effective "go-to-to-get-it-done" administration officials, such as White House Deputy Chief of Staff for Policy Bruce Reed, who led the order's development, along with Secretary of Commerce Gina Raimondo. Secretary Raimondo, a Democratic policy "rock star", also played a key role in the development and execution of the CHIPS and Science Act. She is now similarly tasked with implementing and overseeing certain key requirements in the AI executive order, including the unprecedented Defense Production Act (DPA) reporting and testing obligations imposed on the developers of the most powerful AI systems. Intense focus and co-ordination will be essential to carrying out a nearly overwhelming executive order that runs the gamut on AI-related risk, canvassing national security, cybersecurity, biosecurity, intellectual property, labour, antitrust, education, healthcare, privacy, consumer protection, and American leadership abroad.

Global Leadership at the Bletchley AI Safety Summit, in Washington, and by the G7

Two days after the release of the Biden AI executive order, Vice President Harris traveled to the UK to attend the AI Safety Summit. On the eve of the summit, she delivered a speech at the American Embassy in London to outline American leadership on the issue, including the capacity of the United States to address the concrete and present risks of AI. The vice president took the opportunity to announce the joinder of 30 countries (not including China, as of 12 January) to the US-led "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy", and also the launch of the US AI Safety Institute (AISI), a body similar to the UK AI Safety Institute, which will create standards to test the safety of AI models for public use.

The Bletchley summit appeared to be a diplomatic success, given that participating countries – which included not only leading democratic nations but also, most notably, China – signed the first international declaration to co-operate on AI safety. Nevertheless, one of the key elements of the declaration is transparency. In the context of an internationalist approach, transparency rests on voluntary commitments from private firms. As discussed, previous actions by the Biden administration had already secured such voluntary commitments from leading AI developers. The executive order goes one step further by directing the secretary of commerce to require government reporting requirements. The United States has therefore positioned itself as willing to exercise the "hard" power of the DPA to achieve leadership in the field of AI regulation that might otherwise be limited to so-called soft power.

The executive order explicitly calls for the United States to "lead the way" for global progress on AI and promote "responsible AI safety and security principles and actions with other nations, including our competitors". The White House fact sheet released with the order describes the administration's extensive global engagement already on AI governance, including with Japan regarding the Group of Seven's AI Code of Conduct, with the UK on its Safety Summit, and with India, the United Nations, and numerous others. Accordingly, the order expressly directs the secretary of state to engage in global leadership, including by "lead[ing] efforts to establish a strong international framework for managing the risks and harnessing the benefits of AI". And it likewise tasks the secretary of commerce to lead a co-ordinated initiative with key allies and international partners to develop consensus standards for AI.

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Mandating Government Reporting and Red-Team Testing Requirements in the Interest of National Security

The AI executive order takes the position that the safe and trustworthy development of AI is a matter of national security. This posture is both true and legally relevant given that American constitutional law affords the executive considerable deference on matters of national defense and security. One of the most significant elements of the order, Section 4.2(a), directs the secretary of commerce to require "[c]ompanies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records" relating to a series of topics, including training and development, ownership of model weights, and the results of mandatory red-team testing. Companies that acquire, develop, or possess large-scale computing clusters are obligated to report the existence and locations of such clusters and the total computing power available in each cluster.

The order sets forth the proposed statutory basis for the Section 4.2(a) reporting requirement, citing the broadly powerful Defense Production Act (DPA). The fact sheet released by the White House on 29 January 2024 confirms that the president's invocation of the DPA has compelled certain developers to report "vital information," including the results of safety testing, to the federal government. Therefore, Section 4.2(a) is self-executing, and no further action on the part of the Secretary of Commerce appears necessary.

The importance of global co-operation on AI standards is evident when one considers other actions taken by the Department of Commerce under the executive order. To implement Section 4.2(c), and to address the risks associated with the ability of malicious foreign actors to "engage in certain AI training runs" on US "large-scale computing infrastructure", the Department of Commerce recently issued a Notice of Proposed Rulemaking that would impose government reporting requirements on all US providers of Infrastructure-as-a-Service (IaaS) products. These requirements include, amongst other things, providing notice to the department whenever the IaaS provider has "knowledge" of a "transaction by, for, or on behalf of a foreign person which results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."

Alongside providing useful information to the US government, these requirements may pose challenges for US infrastructure providers regarding how to report such information in a manner that respects existing privacy commitments and relevant law. They may generate frustration amongst allied governments if information is collected on domestic champions without further co-ordination. It may be the case that the US government will need to engage in discussion with partner governments and others to develop a more durable agreement.

Overall, the impact of the US government's leadership on AI so far – with the executive order, AI Safety Institute, the White House AI Bill of Rights, NIST's AI Risk Management Framework, and voluntary commitments by leading AI companies – is world leading. At the same time, as noted at the outset of this piece, the intensity of the new order has caused a backlash from some who view its regulatory mandates as overreaching, unauthorised, and unwarranted.

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Nevertheless, the impacts of these governance elements in the United States will be widespread in both government and civil society. And with the spectre of the Defense Production Act over the development of the most powerful AI systems, there may be an effective fail-safe at the ready. These American AI policy initiatives are certainly substantive and impressive, and they could well serve as models for our international partners and for the private sector at home.

This piece was adapted and updated from an article originally published on Lawfare. Mr Raul also wishes to acknowledge the contribution of his Lawfare co-author Alexandra Muskha.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com