President Biden's Executive Order on AI shows privacy is foundational to responsible AI

Businesses that want to succeed and remain in the AI market must bake privacy into their AI systems. Privacy professionals are well-positioned to help them succeed. By **Abigail Dubiniecki**.

A mixture of excitement and trepidation around Artificial Intelligence (AI) has hit a fever pitch now that generative AI[1] has moved from the sphere of scientific imagination to the everyday lives of consumers and small businesses. Some legislators are struggling to craft legislation that balances innovation and responsibility[2] across the spectrum of AI,[3] while others like the UK opt for self-regulation with guardrails.[4]

Yet DPAs aren't waiting for an AI rulebook. They're using existing privacy and data protection regimes to reign in harmful AI practices, including with generative AI.[5] In keeping with this trend, privacy plays a key role in US President Joe Biden's administration's sweeping 30 October *Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence*[6] (the EO on AI). It will have cascading effects that will impact the private sector.

Business leaders face growing pressure to adopt AI quickly and worry about consequences later.[7] But Biden's EO on AI is the latest reminder that AI businesses who chose to ignore privacy in their race to be first-to-market may not remain on the market for long.

The impact on the private sector

An Executive Order (EO) is a legally-binding directive from the US President regarding the management of operations of the federal government. The members of the executive branch and federal agencies specified in an EO are bound by the rules that EOs create. EOs can have far-reaching impact beyond the US Federal government. For instance, an EO permitting interception of electronic communications helped topple both the Safe Harbor and Privacy Shield frameworks for EU-US data transfers in *Schrems I* and *II*, creating significant burdens for privacy professionals advising clients with overseas business. In contrast, the EO on AI should give privacy professionals a boost because of the strong emphasis it places on privacy, data protection, and other areas that fall squarely within privacy office jurisdiction.

Here are five ways the EO on AI will raise the standards for AI privacy in the private sector:

1. First-mover advantage: The EU was on track to set the global standard for AI with the EU AI Act, just as it had for data protection with the GDPR. The EO on AI now arguably puts the US in that enviable position, according to Dr. Gabriela Zanfir-Fortuna, Vice President for Global Privacy for Future of Privacy Forum (FPF). It creates a legally binding definition of "artificial intelligence" and it gives the US credibility in assuming a leading role in global cooperation on trustworthy AI. Dr. Zanfir-Fortuna suggests the EO on AI may create a "Washington effect" comparable to the Brussels effect created by the GDPR. She notes that the EO requires the Secretary of State to publish an "AI in Global Development Playbook" which will apply the *NIST AI Risk Management Framework* principles to non-US contexts to create a "Global Research Agenda". This harks back to the EU's adequacy regime for non-EU recipients of EU personal data.[8]

Debbie "the Data Diva" Reynolds agrees.[9] As a Global Data Privacy and Protection Expert and Strategist, she notes that Washington has sent a clear signal to the private sector regarding its expectations for AI offerings. Within a year it will have solid evidence showing it is possible to innovate responsibly, emboldening other jurisdictions to follow suit. This will raise the bar for all businesses seeking to integrate AI.

2. Procurement and contracting; research and development: Reynolds notes that the EO on AI sets clear expectations on AI for the private sector. The Federal government is the largest employer in the US and has significant purchasing power.

Indeed, the EO tasks the Labor Secretary with publishing best practices for fair use of AI in the employment context, in consultation with unions and employees. The draft Office of Management and Budget policy (the OMB Policy) tabled further to the EO on AI applies stringent minimum standards to AI use for "rights-impacting" activities, such as pre-employment screening, hiring, termination, performance pay and other contentious areas. Algorithmic Impact Assessments (AIAs), real-world pre-deployment performance testing; human review; transparency obligations, and more will be mandatory.

The OMB Policy will require newly appointed Chief AI Officers (CAIOs) of each major federal agency to review existing AI and proposed AI integrations that are "rights-impacting" against a set of high minimum standards. They must cease using any that fail to meet those standards by 1 August 2024. To make this assessment, CAIOs will be required to review extensive AI provider documentation (such as model cards, datasheets for datasets, etc.), which not all providers keep.

Professor Renée Sieber and Ana Brandusescu, Ph.D. (candidate) specialize in public governance of AI. They caution that anything short of "hard law" – legislative and judicial authority to punish non-compliance – may be insufficient. Mechanisms that can slow, prevent or even sunset potentially harmful AI systems are required.

However, Dr. Zanfir-Fortuna notes that even though the EO is not legislation,

it is legally binding. Reynolds notes that these requirements will flow across complex AI supply chains, much as the data protection due diligence under the GDPR. Contract, not regulation, may be the biggest source of effective guardrails for AI, even for those with no direct contractual relationship to the Federal government.

3. Research and Development (R&D): The EO calls for the development and deployment of Privacy-Enhancing Technologies (PETs) (s.9) and offers a range of AI R&D opportunities such as test beds, datasets, computing power and expertise to promote innovation. "To develop and strengthen public-private partnerships for advancing innovation, commercialization, and risk-mitigation methods for AI, and to help promote safe, responsible, fair, privacy-protecting, and trustworthy AI systems" the EO on AI order the Director of the National Science Foundation to launch its National AI Research Resource (NAIRR) (s.5(2)(e)). The NAIRR will build privacy, civil rights and civil liberties considerations into all facets of its design and operations. Its Ethics Advisory Board will include privacy experts. The NAIRR is intended to serve as an "exemplar for how transparent and responsible AI R&D can be performed…". Stakeholders will require privacy training as a condition for access.[10]

4. Standards: Under the guiding principles of advancing equity and civil rights and consumer protection (ss. 2(d) and (e)), the EO on AI commits to building on the Blueprint for an AI Bill of Rights (the "AI Blueprint"), which makes privacy and fairness foundational to AI, and the AI Risk Management Framework of the National Institute for Science and Technology (the NIST AI RMF). It also commits to enforcing existing consumer protection laws and enacting safeguards against unintended bias, discrimination and infringements on privacy.

Meanwhile, the EO on AI encourages agencies to use all their powers to protect consumers, patients, passengers and students from fraud, discrimination and threats to privacy. It also establishes a task force to establish policies, frameworks and regulatory action to ensure responsible deployment of AI-enabled technologies in the health and human services sectors. It will require the use of equity-focused algorithmic assessment, model development and monitoring, and the incorporation of privacy standards in the full software development lifecycle. It applies similar approaches to AI in education and proposes the development of an "AI Toolkit" for educators to align with privacy regulations and develop education-specific guardrails (s.8).

NIST standards are respected around the world, and DPAs often recommend adherence to them. Meanwhile, the toolkits and standards will set a higher bar for a range of health and social sectors. This EO will provide further impetus to align, while increased enforcement of existing laws in the US will be added to that of UK and EU regulators to create significant market incentive to AI providers, as discussed below.

5. 'Naughty lists' and reputational risks: Companies that lose their eligibility for government contracts pursuant to the 1 August 2024 OMB Policy deadline will not only lose revenue and market share, they will also suffer a reputational hit that could freeze them out of other opportunities. Meanwhile, the AI safety program that tracks AI harms and algorithmic errors envisaged under s.8(b)(iv) of the EO on AI could have a "name and shaming" effect on those AI providers. At a minimum, it will force them to address issues such as bias, discrimination and performance.

Privacy important for trustworthy AI

Managing AI risk is not new for privacy professionals. They have assisted clients in ensuring automated decision-making, biometrics, Internet of Things and many other AI-powered processing activities are compliant with privacy and data protection laws.

Indeed, DPAs have dipped into their data protection toolkits to regulate AI. Italy's *Garante* made headlines when it issued a temporary ban and compliance orders to OpenAI which brought the most influential and transformative AI company to heel.[11] It recently opened an investigation into web scraping to train algorithms, and has hinted at enforcement action.[12] Other DPAs have followed suit with investigations into the technology,[13] while the EDPB has created a dedicated Chat-GPT task force.[14] The Kenyan DPA reigned in WorldCoin's iris scanning cryptocurrency offering.[15] Courts and regulators are increasingly using algorithmic disgorgement[16] as a remedy (or punishment) for AI models developed using ill-gotten data.

Well before generative AI was a mainstream concern, the Global Privacy Assembly (GPA) had adopted the foundational 2018 *Declaration on Ethics and Data Protection in Artificial Intelligence*,[17] which emphasized fairness, transparency and measures to mitigate discrimination risks and harmful bias. In October 2020, the GPA adopted the *Resolution on Accountability in the Development and Use of Artificial Intelligence*, urging AI developers to build accountability measures into their AI systems, and in October 2023, a resolution on generative AI systems[18].

Meanwhile, many international and regional instruments have emphasized the foundational role of privacy and data protection, notably:

- 193 countries have adopted the *UNESCO Recommendation on the Ethics of AI*, which lists as key principles issues that will be familiar to privacy professionals;[19]
- Over 50 governments have endorsed the *OECD / G20 AI Principles*, which recognize the important role of privacy and data protection in promoting human-centric AI;[20]
- The 2023 *Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems* signed at the recent G7 Summit builds on the OECD principles;[21]
- The EU's proposed AI Act builds on the GDPR. Yonah Welker, a Board Evaluator for the European Commission focused on social AI, robotics, learning and accessibility, notes that the *Digital Services Act* and the *Digital Markets Act* complement the EU AI Act, imposing transparency, explainability and accountability requirements for recommendation algorithms and prohibiting deceptive and manipulative algorithms;
- The African Union Commission has endorsed the *African Union*

(AU) Data Policy Framework, which includes a milestone towards adoption of the 2024 AU Artificial Intelligence Continental Strategy tailored to the African context. Its transversal approach incorporates privacy, data protection, data justice and data sovereignty.[22]

AI policy safeguards around the world build on data protection frameworks.[23]

Dr. Zanfir-Fortuna notes that modern data protection frameworks were created in response to concerns around automation and computing: "...the first chatbot, Eliza, was also developed in the mid '60s at MIT, by Professor Joseph Weizenbaum. In fact, Weizenbaum was also a member of the Committee in the United States that proposed the Fair Information Practice Principles in 1973, which are now the cornerstone of data protection frameworks. Therefore, it should not surprise anyone that the closest existing legal framework to deal with the challenges of AI proved to be data protection, through all these regulatory actions by DPAs."

DPOs are well-positioned

Dr. Zanfir-Fortuna is confident privacy professionals are well-positioned to advise on AI projects: "Essentially, they have created processes and channels of communication internally across functions focusing on data issues. All these are very important skills and competences, which make privacy professionals well suited to play a key role in enterprise-level AI governance." Reynolds echoes this sentiment.

A recent study that produced a Taxonomy of AI Failures illustrates how many AI harms can be traced to AI failures,[24] many of which can be mapped to several privacy requirements. For example, transparency and explainability obligations force organizations to understand how AI systems work and assess decision quality. Data minimization requires AI developers to use data that is relevant, necessary and adequate, while the accuracy principle may justify more, not less, quality data to increase statistical accuracy.[25]

Conclusion

Privacy professionals can leverage their privacy expertise to help businesses innovate responsibly and weather the regulatory storm. And thanks to DPAs such as Spain's AEPD, UK's ICO, France's CNIL and think tanks like the FPF, they have ample guidance to consult.

AUTHOR

Abigail Dubiniecki is an independent Privacy Consultant in Canada.
Email: legallyabigail@protonmail.com

REFERENCES

1 On generative AI, see generally www.cnil.fr/en/artificial-intelligence-action-plan-cnil and fpf.org/wp-content/uploads/2023/07/Generative-AI-Checklist.pdf.

2 The EU's AI Act was almost derailed by disagreements among member states over whether and how to regulate generative AI and foundation models. See www.euractiv.com/section/artificial-intelligence/news/eus-ai-act-negotiations-hit-the-brakes-over-foundation-models

3 See the Future of Privacy Forum infographic, The Spectrum of Artificial Intelligence, for the wide range of AI use cases and types available and in use: fpf.org/wp-content/uploads/2021/01/FPF_AIEcosystem_illo_03.pdf

4 The UK's PM Rishi Sunak has reaffirmed his government's preference for a "pro-innovation" approach that takes a softer touch toward regulation – for now: www.aisafetysummit.gov.uk/video. In contrast, an Artificial Intelligence (Regulation) Private Members Bill has recently been tabled in the House of Lords: www.privacylaws.com/news/bill-proposes-an-ai-authority.

5 See e.g. fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai.

6 www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

7 Some have chosen to remove AI ethics teams or oversight bodies, seen as impediments to innovation. See e.g. www.theverge.com/2023/3/13/23638823/microsoft-ethics-society-team-responsible-ai-layoffs and www.nytimes.com/2023/11/22/technology/openai-board-capitalists.html.

8 Via email, 20 November 2023.

9 Web interview, 20 November 2023. Reynolds hosts "The Data Diva" Talks Privacy Podcast.

10 See new.nsf.gov/news/nsf-partners-kick-nairr-pilot-program and www.nsf.gov/cise/national-ai.jsp.

11 iapp.org/news/a/chatgpt-resolves-garantes-data-protection-concerns.

12 www.dataguidance.com/news/italy-garante-investigates-webscraping-algorithm

13 *Supra*, note 5.

14 edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

15 techcrunch.com/2023/08/02/kenya-suspends-worldcoin-scans-over-security-privacy-and-financial-concerns.

16 See e.g. Goland, Joshua A., Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data (March 1, 2023). *Richmond Journal of Law and Technology*, Vol. XXIX, Issue 2 (2023), Available at SSRN: ssrn.com/abstract=4382254 or dx.doi.org/10.2139/ssrn.4382254.

17 globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf.

18 globalprivacyassembly.org/document-archive/adopted-resolutions/

19 www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

20 oecd.ai/en/wonk/documents/g20-ai-principles.

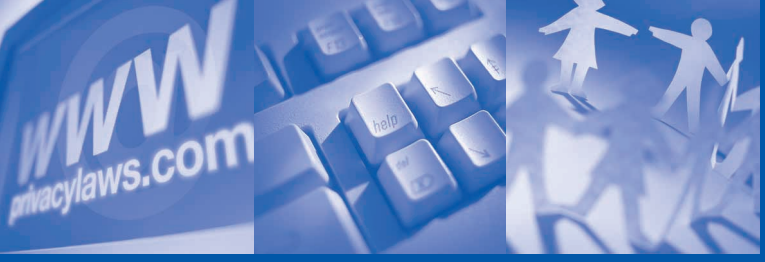
21 www.mofa.go.jp/files/100573473.pdf.

22 au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf.

23 *Ibid* at p. 3.

24 www.semanticscholar.org/reader/a38af38baeb1b5e25c089b699ab5072823ae6b4c.

25 For a list of helpful questions DPOs can ask as well as resources, see Abigail Dubiniecki and Ashantel Lachhani, 'Working with non-executive directors on AI privacy issues,' *PL&B UK Report*, September 2023, p. 14. See also Kingsmill, S. and Dubiniecki, A., 'Privacy in the New World of AI' regarding the importance of privacy, online: kpmg.com/us/en/articles/2023/privacy-world-ai.html



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Data protection enforcement trends in Germany

By **Julia Garbaciok** and **Katharina A. Weimer** of Fieldfisher.

In Germany there have been interesting recent decisions and trends across the country. In this article we discuss the latest news on e-marketing consent rules, and give an overview on recent developments in German employee data protection law, as well as a few highlights relating to data subjects' access rights requests.

Continued on p.3

Creating an AI governance framework: US and EU take steps to lead

The EU is finalising its AI Act while the US adopts a Presidential Executive Order on AI and creates an Artificial Intelligence Safety Institute. How are companies preparing? By **Laura Linkomies**.

The EU is still in the middle of the Trilogue process between the European Parliament, the European Council, and the European Commission. In October, they agreed on wording addressing important classification rules for high-risk artificial intelligence (AI) systems, but there are still other aspects to be finalised. There will be a certification regime for high-risk AI systems, and the Commission now

Continued on p.6

Issue 186 **DECEMBER 2023**

INTERNATIONAL report

ISSUE NO 186 DECEMBER 2023

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Julia Garbaciok and Katharina A. Weimer
Fieldfisher, Germany
Professor Graham Greenleaf
UNSW, Australia
Nana Botchorichvili
IDEA Avocats, France
David van Boven
Privacy Lawyer, the Netherlands
Patrick van Eecke, Loriane Sangaré-Vayssac and Enrique Capdevila
Cooley, Belgium
Yaron Dori, Megan Crowley and Diana Lee
Covington, US
Uche Val Obi San
Alliance Law Firm, Nigeria
Abigail Dubiniecki
Privacy Consultant, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Keeping up with AI is a challenge

There are so many privacy developments in AI governance. This issue will give you a good insight into some of the most recent news. The US Executive Order pushes the US to the lead in AI governance (p.1 and p.8) as the EU, with its complex decision-taking structure, has been delayed in adopting its AI Act. EU DPAs are alert and conduct their own investigations on AI but also unite at the European Data Protection Board to construct common positions. There is an important role for lawyers and DPOs now that market practices are developing. Privacy must be baked into products but also into organisations' AI governance, as our correspondent says.

But thoughtful public policy decisions are difficult to make when we do not fully understand the opportunities and risks with using AI, nor the impact on society as a whole.

Specifically working on privacy and new technologies is the International Working Group on Data Protection in Technology (the Berlin Group) which issues working papers on specific themes. The German-led group provided an update at the DPAs' Global Privacy Assembly in Bermuda, saying it works especially closely with the UK ICO and France's CNIL to develop future technology monitoring so that DPAs can issue privacy-friendly advice at an early stage of development of these technologies (www.bfdi.bund.de/EN/Fachthemen/Inhalte/Europa-Internationales/Berlin-Group.html).

In Bermuda, views were exchanged on the new EU-US Data Privacy Framework, which will inevitably face challenges (p.14), as well as enforcement cooperation, AI, risk based approaches and more (p.26).

We welcome your speaker offers in the first half of December for PL&B's 37th Annual Conference 1-3 July 2024 at St. John's College, Cambridge www.privacylaws.com/events-gateway/events/2024ic37/

As this is the last edition for 2023, I would like to thank you, our loyal readers, for your support and feedback (more needed though!). We are privileged to work with so many talented people, especially our *PL&B* Correspondents.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 7 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> "An indispensable resource for anyone who has a serious interest in privacy, combining latest news with thoughtful commentary and analysis."
>
> **Richard Cumbley, Partner, Linklaters**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the current Data Protection and Digital Information Bill, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.