POLSINELLI

Publications

November 16, 2023 • Updates

Unpacking the Executive Order on AI (for Data Privacy)

As we noted two weeks ago,[1] the Whitehouse has dipped its toe further into the generative artificial intelligence (AI) waters with the release of its Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO).[2] The EO maps how federal agencies and AI developers must deal with AI risks, including data privacy.

Data Privacy is Prevalent, not Dominant

For example, in Section 9 of the EO the federal government is directed to assess its use of

Related People

- Aaron M. Levine
- Elizabeth (Liz) Harding
- Gregory J. Leighton

Related Capabilities

- Artificial Intelligence & Machine Learning
- Privacy & Cybersecurity

Commercially Available Information (CAI), which anyone can buy from various data brokers. The concern is, CAI includes personally identifiable data (PII), therefore, the EO requires that more be done to upgrade standards regarding its collection, storage and processing.

To do this, a team of high-level operatives such as the Director of Office of Management and Budget and the Attorney General are required to create a request for information to be issued government-wide to assess potential updates to the E-Government Act of 2002, a statute promoting the use of electronic records which mandates improving privacy.

Among the E-Government Act's privacy measures are privacy impact assessments, privacy protections, and policies on government websites. For this reason, the EO also focuses on so-called Privacy Enhancing Technology (PETs), and it seems likely the government is going to explore implementing things like two-factor identification for its websites and data storages.

Section 8 of the EO discusses implementing privacy standards into the software development lifecycle of healthcare services. Also, the EO includes provisions directing the National Institute of Standards and Technology to advance research into PETs, including (interestingly enough) a provision to piggy-back on the UK's PET Prize Challenge and its results.[3]

Which leads to the observation that, despite being mentioned 38 times throughout the EO, references to data privacy are pale in comparison to the emphasis that the European Union has placed on it since implementation of the General Data Protection

Regulation (GDPR) in 2018. It follows then, that the EU would also take the lead with AI regulation.

The EU is Leading the Way, Again

The vehicle of the EU's ambition is its sweeping AI Act.[4] While the AI Act is not yet law, the EU has been working on its since 2017 when the European Council called for a "sense of urgency to address emerging trends including artificial intelligence …, while at the same time ensuring a high level of data protection, digital rights and ethical standards." The AI Act is likely to be passed sometime in 2024.

At a high-level, the AI Act is an extremely complex statute that incorporates and references numerous other EU regulatory regimes. It defines AI as "software that is developed with [several techniques, that] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."[5]

Beyond this broad definition of AI system, the AI Act divides relevant technologies into three categories:

1. Prohibited AI Systems. Prohibited systems include any kind of subliminal technique, systems that are designed to exploit age, physical or mental disabilities, social credit systems by public authorities and real time biometrics by law enforcement in public spaces (though many exceptions apply). Examples of such exceptions include targeted searches for missing children or the

prevention of a specific, substantial imminent terrorist threat.

2. High risk systems include applications where the AI system is intended to be used as a safety component of some other product, biometric identification systems, management of critical infrastructure, educational and training applications, HR systems, law enforcement, administration of justice and democratic process and access to private and public services and benefits, such as creditworthiness or emergency dispatch.

3. Unregulated, essentially, everything not prohibited or high-risk falls into the third, largely unregulated category.

Notably, providers and users of AI systems that are in countries outside the EU, where the *output* produced by the system is *used in the EU,* are covered by the Act.

As with the GDPR, enforcement penalties have the potential to be steep, with maximum fines of 20,000,000 EUR or 4% of annual revenue, whichever is greater.

As implementation of the AI Act gets closer, we will provide further details and updates. For other recent content addressing AI see *Chatbots: Select Legal Considerations for Businesses*,[6] and *Artificial Intelligence Has a NIST Framework for Cybersecurity Risk*,[7] and *Generative AI's 'Industry Standards' for Cybersecurity and Data Privacy Could be Here Sooner Rather than Later*.[8]

Save the Date

- December 7: Polsinelli will commence an AI webinar series, ‘Emerging Legal Concepts with Generative AI in 2024’. Register now.
- In the first quarter of 2024, lawyers from Polsinelli’s healthcare, intellectual property, labor and employment, and data privacy and cybersecurity groups will provide guidance on the legal issues relating to use and deployment of generative AI tools

---

[1] Hyperlink https://www.polsinelli.com/publications/unpacking-the-executive-order-on-ai-for-cybersecurity

[2] Hyperlink https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[3] Hyperlink https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[4] Hyperlink https://artificialintelligenceact.eu/the-act/.

[5] *Id.* at Art. 3 (1).

[6] Hyperlink https://www.polsinelli.com/matt-a-todd/publications/chatbots-select-legal-considerations-for-businesses

[7] Hyperlink https://www.polsinelli.com/leslie-f-spasser/publications/artificial-intelligence-has-a-nist-framework-for-cybersecurity-risk

[8] Hyperlink https://www.polsinelli.com/romaine-c-marshall/publications/generative-ais-industry-standards-for-cybersecurity-and-data-privacy-could-be-here-sooner-rather-than-later