Academia

The AI data challenge: How do we protect privacy and other fundamental rights in an AI-driven world?

Lee Tiedrich, Celine Caira, Yanic Benhamou
October 19, 2023 — 7 min read

Solving the AI data challenge supports the implementation of the OECD AI Principles

The rapid growth of generative artificial intelligence and other AI applications has great potential to enhance global prosperity, security, and social good. But to make this vision a reality, society must solve the AI data challenge as part of its broader efforts to operationalise the OECD AI Principles and ensure legal compliance.

AI typically relies on vast amounts of data for training and other purposes. Access to appropriate data for developing AI models can help advance the OECD AI Principles by reducing harmful AI bias and unfairness. It can also improve AI accuracy, reliability, and safety. Data cards and similar tools can also improve AI transparency and accountability by providing information on how models were trained and the data used.

Disinformation, manipulation, intellectual property infringement and privacy threats in a generative AI world loom large

Despite these benefits, significant challenges remain to responsibly unlock data for AI. Efforts to develop privacy-enhancing technologies, data governance, and other tools must continue. This includes creating widely embraced standards, like data cards, to evaluate AI training data's appropriateness for intended use cases. This can be said for narrow AI applications with specific uses and Large Language Models (LLMs) with many different purposes. More standard contract terms, common APIs, and other tools could facilitate greater voluntary and responsible AI data sharing.

Cybersecurity challenges also persist, as do concerns about protecting people's likeness. As spotlighted by growing disputes and a recent OECD survey of G7 members, the need to safeguard against disinformation, manipulation, and intellectual property infringement in a generative AI world also looms large. Responses from G7 members and the rise of enforcement actions and other disputes also underscore the urgency to protect privacy and other fundamental rights in a generative AI world. While privacy as a fundamental right is sacrosanct, questions remain on how best to uphold it.

AI and privacy experts explored these questions during the third AI2S2 Symposium in Geneva

To help find solutions, this topic was featured in a discussion at the third AI2S2 Symposium convened by the University of Geneva, the OECD, and the Global Partnership on AI (GPAI). The discussion began with a keynote address by Leonardo Cervera-Navas, the Secretary General of the European Data Protection Supervisor (EDPS), and an introduction by session co-convenor Celine Caira of the OECD. This was followed by a lively conversation among the other co-convenors and participants: Lee Tiedrich, Duke University (and Co-Chair of the GPAI Multi-Stakeholder Expert Working Group); Yanic Benhamou, Professor of Law, Digital Law Center at the University of Geneva Faculty of Law, Thomas Schneider, Director of International Relations at the Swiss Federal Office of Communications, Pam Dixon, Executive Director of the World Privacy Forum, and Laura Galindo-Romero, Privacy Policy Manager at Meta. In-person and virtual participants also shared their perspectives and questions.

During his keynote, the EDPS Secretary-General highlighted that society is at the beginning of a long AI journey and still faces many questions about what is to come. To help chart this journey, it is necessary to safeguard privacy and other fundamental rights in an AI-driven world. Here, we look at the EDPS Secretary General's remarks about protecting these rights and the panel's discussion about strategies for implementing this approach.

The perils for privacy and fundamental rights

If unchecked, generative AI and other AI technologies could seriously erode privacy and other fundamental rights. Already, significant amounts of personal data, including sensitive data, are being used to train and develop AI applications. Compounding the AI data challenge, data is being collected and processed in myriad ways. This includes data scraping or ingestion of publicly accessible data from third-party websites and social media properties. Data brokers also regularly monetise vast amounts of personal data, often harming individuals. Individuals frequently relinquish their data without necessarily understanding the consequences, using voice recognition, text-based writing tools, and other commonplace AI applications. Additionally, individuals have increased electronic monitoring in the workplace. Emotion detection and facial recognition applications continue to rise, too.

Unsurprisingly, the AI data challenge has sparked regulatory and enforcement actions in many countries. While privacy laws differ among jurisdictions, some common concerns have emerged. These include the lack of transparency, for instance, around data collection and usage. Additionally, individuals often cannot easily access, delete, correct, or otherwise control their personal data. Data minimisation and establishing sufficient justification for data collection have proven challenging, too. In a recent blog post, the FTC highlighted consumer concerns about AI, including its use of data.

The concerns also extend to data security. In a recent joint statement, 12 data protection authorities explained how data scraping presents cybersecurity risks and the obligations of social media companies and others to prevent unlawful data scraping.

The EDPS perspective

Secretary General Cervera-Navas presented the EDPS's perspectives in a keynote speech. In European Union tradition, AI policymaking must maintain a focus on individuals. Consistent with this approach, he proposed a three-pillar structure: 1) a human-centric regulatory framework, 2) robust enforcement, and 3) international standards and tools. International standards and tools can aid with regulatory compliance and enforcement. They can also foster greater international harmonisation, particularly when jurisdictions have different regulatory regimes.

The Secretary-General highlighted the work of the Geneva-based International Standards Organisation (ISO) and the US National Institute of Standards and Technology (NIST) in this area. He stressed AI's potential to advance human progress and cautioned that AI should not become a tool that generates "profits for a few or to the detriment of the fundamental rights of many."

Key takeaways

Much of the following discussion took inspiration from the Secretary General's three-pillar structure and other remarks. Panel participants shared several ideas on implementing the three pillars to protect privacy and other fundamental rights in an AI-driven world.

1. Inclusive dialogue

Since privacy and other fundamental rights impact everyone, the process for developing safeguards must involve the global community and diverse stakeholders, such as historically under-represented groups. The dialogue should also include experts from multiple disciplines to help ensure that technical and other profiles can widely operationalise legal and policy approaches in a compliant, ethical, and sustainable manner.

2. Common definitions

Even within the privacy and AI realms, a single term can have different meanings. Technical and non-technical experts often have different lexicons. Common definitions on an international level and across sectors can help support inclusive dialogue by bridging differences among jurisdictions and facilitating multi-disciplinary communications and collaborations. More progress in creating uniform definitions will bolster common understandings. These efforts can draw upon the excellent foundation of the OECD's Framework for the Classification of AI Systems and other important works.

3. Role of regulation, enforcement and other tools

Existing privacy frameworks have gaps in protecting individuals in an AI-driven world. For example, there are challenges in proving that fundamental rights have been violated and/or harm produced in a digital context. However, views among stakeholders continue to differ on the role of regulation in protecting privacy. While some prefer more regulation, others advocate for a heavier reliance on business codes of conduct, technical tools, contract terms, and other devices that are not legally binding. This often is referred to as a "soft law" approach.

Despite the differing views on the role of regulation, a consensus emerged on the importance of developing tools, including possibly through a "co-regulatory" process involving government and other stakeholders. Such tools can help increase cross-border harmonisation, particularly when jurisdictions have different regulatory pathways. For jurisdictions favouring a regulatory approach, tools can be referenced in or otherwise support regulations and enforcement. This aligns with the views expressed by EDPS Secretary General Cervera-Navas about the need for international standards and tools to support human-centric regulatory frameworks and their enforcement.

While more work needs to be done, a good foundation exists for developing AI standards and tools. This includes 1) the OECD's Due Diligence Guidelines for Responsible Business Conduct, 2) the OECD Catalogue of Tools and Metrics for Trustworthy AI, 3) NIST's AI Risk Management Framework, 4) ISO's Framework for AI Systems Using LLMs, and 5) GPAI projects, such as the report on AI Foundation Models and Detection Mechanisms. As noted above, developing common standards and tools requires multi-disciplinary input and engagement with diverse stakeholders.

4. Addressing data scraping

Data scraping for generative AI and other purposes has led to numerous enforcement and litigation actions across jurisdictions, raising privacy, intellectual property, and other concerns. The EDPS launched a task force on ChatGPT. Other government leaders continue to consider how to address data scraping, too.

These developments further underscore the need to continue exploring the development of tools to support the protection of privacy and other rights in an AI-driven world. Data scraping tools could include business codes of conduct, model contract terms, technical measures and education. These can support regulatory implementation and enforcement, complementing laws and policies.

5. Fostering innovation and regulatory harmonisation

While protecting privacy, safety, security, and other rights remains paramount, policies should also avoid unnecessarily deterring responsible AI innovation. This includes the important step of enabling responsible small and medium-sized enterprises (SMEs) to introduce new AI offerings and expand competition. Fostering innovation ranked high in the OECD survey of G7 members. International harmonisation — that includes widely available and accessible tools that can support regulatory compliance — may help unlock AI innovation and competition while maintaining privacy and other important protections.

Addressing the AI data challenge

Individuals stand to benefit from responsible generative AI and other data-driven technologies, including by improving their productivity, learning, healthcare, and environment and by making everyday tasks more enjoyable and efficient. But how can society provide and capitalise on AI technologies, given the vast amounts of data needed, and still protect privacy and other fundamental rights espoused in the OECD AI Principles?

The exponential growth of generative AI has escalated the urgency to address the AI data challenge and operationalise the OECD AI Principles more broadly. Actions aligning with Secretary General Cervera-Navas's three pillars will be essential while creating an environment where risks are appropriately mitigated and individuals benefit from AI. Privacy protection and human rights are critical to addressing the AI data challenge. However, to fully solve the AI data challenge, society must also tackle other issues, such as safeguarding against intellectual property infringement, manipulation, disinformation, cybersecurity attacks, workforce displacement, and other harms. Solving the AI data challenge requires an integrated approach that considers these objectives and upholds the OECD AI Principles.

Society is indeed on a long AI journey. The path it charts will determine how safely people will travel and how much benefit they will reap. Everyone can help chart this path, including by participating in the Global Challenge for Trust in the Age of Generative AI.

Lee Tiedrich
Duke University Science & Society
Distinguished Faculty Fellow in Ethical Technology
See all posts

Celine Caira
OECD
Economist / Policy Analyst – Expert Group on Compute & Climate
See all posts

Yanic Benhamou
Faculty of Law of the University of Geneva
Associate Professor of Digital Law
See profile

Related posts

Business
Lessons for businesses and regulators on implementing trustworthy AI
Reviewed at the OECD, seven practical lessons for businesses and regulators from seven case studies
April 30, 2021 — 6 min read