Shaping the future: A dynamic taxonomy for AI privacy risks

Henrique Fabretti Moraes
Maria Beatriz Previtali

schedule Jan 17, 2024
https://iapp.org/news/a/shaping-the-future-a-dynamic-taxonomy-for-ai-privacy-risks/

A well-known quote states when you name something, you gain power over it. Although this is true for so many fictional universes and fields of real-world knowledge, such a statement is especially applicable when talking about the interface between privacy and artificial intelligence.

While there is a consensus AI should be regulated, and there are increasing efforts in this sense — such as the highly anticipated EU AI Act — the fact is AI privacy risks remain uncharted waters, leaving both AI practitioners and privacy professionals with a feeling of unease. After all, since AI technologies are advancing faster than regulation, how should privacy pros approach AI privacy risks in a way that makes new products viable, while safeguarding data subjects' rights?

This is a complex question, but the first step toward a solution is naming things and mapping the surroundings. Of several recent efforts to systematize the risks that intersect privacy, data protection and AI, work conducted by a research group from Carnegie Mellon University and Oxford University in "Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks" caught our attention.

The researchers amassed a dataset of 321 fact-checked AI incidents from 2013 to 2023, available at the AI, Algorithmic, and Automation Incidents and Controversies Repository, focusing on those involving privacy issues.

The AI risks taxonomy is built from a well-established foundation: Daniel Solove's seminal 2006 paper, "A Taxonomy of Privacy." Instead of simply transposing all of Solove's 16 privacy risks to an AI-infused context, the authors first sought to assess how AI actually influences such risks, be it by exacerbating existing issues, creating new ones or simply not interacting with them at all.

By combining a regulation-insensitive approach with real-world, fact-checked incidents, the authors were able to curate a set of 12 distinct risks from Solove's original 16, avoiding speculative or theoretical scenarios.

This is a great starting point for privacy or AI governance professionals to build their risk assessment models to evaluate privacy risks on AI systems. To make this task easier, the following is a summary of the 12 risks:

- **Surveillance:** AI exacerbates surveillance risks by increasing the scale and ubiquity of personal data collection.
- **Identification:** AI technologies enable automated identity linking across various data sources, increasing risks related to personal identity exposure.
- **Aggregation:** AI combines various pieces of data about a person to make inferences, creating risks of privacy invasion.
- **Phrenology and physiognomy:** AI infers personality or social attributes from physical characteristics, a new risk category not in Solove's taxonomy.
- **Secondary use:** AI exacerbates use of personal data for purposes other than originally intended through repurposing data.
- **Exclusion:** AI makes failure to inform or give control to users over how their data is used worse through opaque data practices.
- **Insecurity:** AI's data requirements and storage practices risk of data leaks and improper access.
- **Exposure:** AI can reveal sensitive information, such as through generative AI techniques.
- **Distortion:** AI's ability to generate realistic but fake content heightens the spread of false or misleading information.
- **Disclosure:** AI can cause improper sharing of data when it infers additional sensitive information from raw data.
- **Increased Accessibility:** AI makes sensitive information more accessible to a wider audience than intended.
- **Intrusion:** AI technologies invade personal space or solitude, often through surveillance measures.

Lastly, it is important to remember the taxonomy of AI privacy risks is not static — it's a living framework that must evolve with the AI landscape. Effective governance requires continuous adaptation, informed by collaborative research and cross-sector dialogue. Balancing innovation with ethical standards and data protection is imperative.

This proactive and flexible approach, grounded in an evolving understanding of AI risks, is essential to safeguarding data subjects' rights as it aligns technological advancements with societal values. Such a strategy not only addresses current privacy concerns but also anticipates future challenges, ensuring resilience in an ever-advancing AI-driven world.