A Regulatory Roadmap to AI and Privacy

IAPP News (April 24, 2024)

By Daniel J. Solove

As AI is poised to take over the world, it is raising a number of problems, many involving privacy. These are catalogued in the recently posted article draft, "Artificial Intelligence and Privacy."[1] Understanding these issues and the overall relationship between AI and privacy is essential for determining how privacy law should regulate AI.

Current privacy regulations partly address AI issues. Legislation specifically targeting AI is emerging, with the European Union taking the lead with the AI Act, and U.S. states proposing new AI laws.

Are new laws needed to address AI's privacy problems? The answer is complicated. Existing privacy laws aren't well-designed to address AI's privacy problems. Although new AI laws can help, AI is making it glaringly clear that a privacy law rethink is long overdue.

Against AI exceptionalism

AI today is both old and new. The technologies branded as "AI" today are actually old technologies that are working more effectively given vast increases in data and computing power.

It is important to avoid "AI exceptionalism" — treating AI as if it were so unique that we are unable to see how its privacy problems are often outgrowths of existing privacy issues. The privacy problems associated with AI largely revolve around practices privacy laws have long dealt with, such as the collection and processing of personal data. To be effectively addressed, these privacy problems should be tackled holistically, not just in the context of AI. Rarely is there a magic line separating privacy issues in AI from those in the digital age generally.

AI can increase existing privacy problems, add dimensions and complexities to them, or remix them. Merely addressing AI is like trying to remove weeds without digging up

[1] Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 Fla. L. Rev. __ (forthcoming 2025).

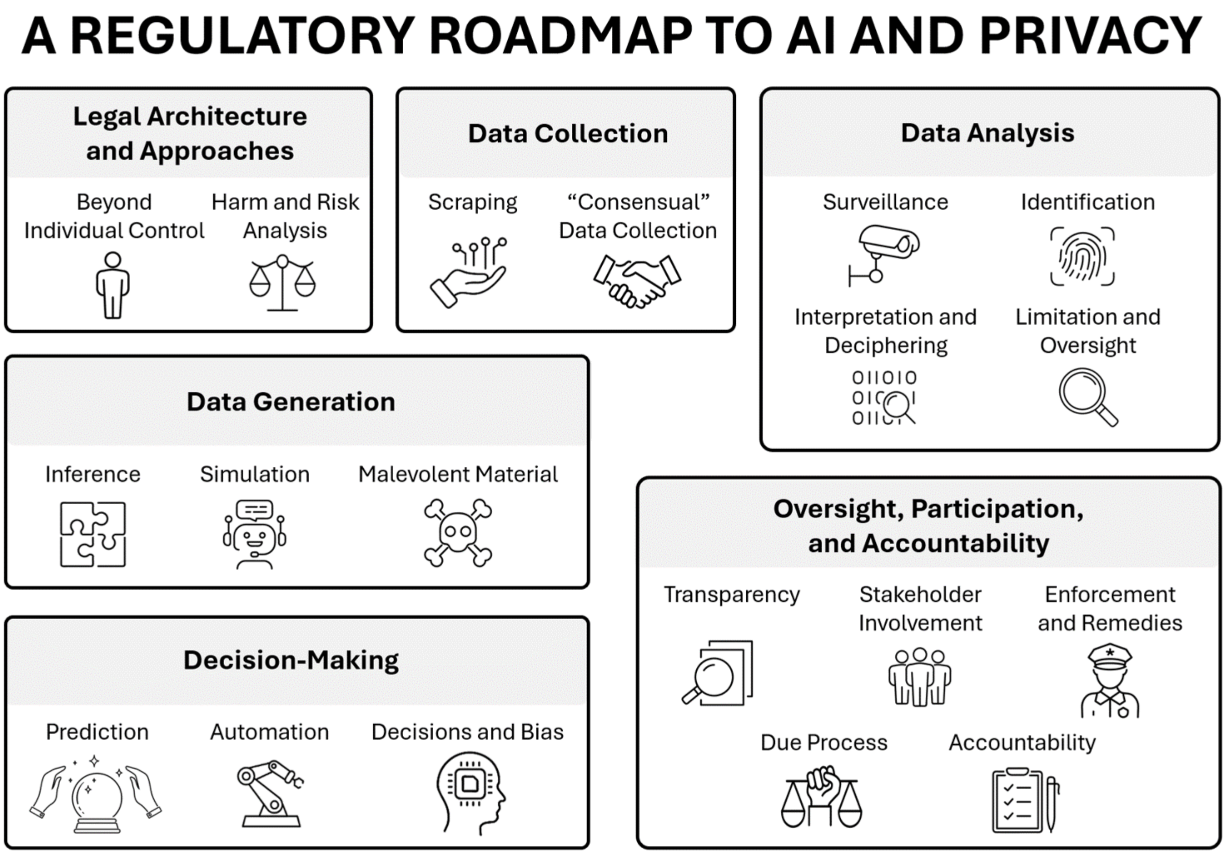
their roots.

In stark ways, AI is showing the flaws in existing privacy laws. Instead of seeing AI as a unique situation, AI should be viewed as an opportunity to change course with privacy law generally. To address AI's privacy problems, policymakers shouldn't just pass new AI laws; they should also fix existing privacy laws.

Guidance for the regulation of AI and privacy

Understanding the privacy challenges posed by AI is essential. A comprehensive overview is necessary to evaluate the effectiveness of current laws, identify their limitations and decide what modifications or new measures are required for adequate regulation.

"Artificial Intelligence and Privacy" develops a regulatory roadmap to AI and privacy, exploring the problems AI creates and the challenges it poses for the existing architecture of many privacy laws.



A REGULATORY ROADMAP TO AI AND PRIVACY

Legal Architecture and Approaches
- Beyond Individual Control
- Harm and Risk Analysis

Data Collection
- Scraping
- "Consensual" Data Collection

Data Analysis
- Surveillance
- Identification
- Interpretation and Deciphering
- Limitation and Oversight

Data Generation
- Inference
- Simulation
- Malevolent Material

Decision-Making
- Prediction
- Automation
- Decisions and Bias

Oversight, Participation, and Accountability
- Transparency
- Stakeholder Involvement
- Enforcement and Remedies
- Due Process
- Accountability

from Daniel J. Solove, *Artificial Intelligence and Privacy*, forthcoming 77 Florida L. Rev. __ (2025), https://ssrn.com/abstract=4713111

AI involves algorithms that ingest inputs and generate outputs. Both inputs and outputs lead to privacy problems. The gathering of inputs involves problems of data collection, while the production of outputs involves problems of data generation, decision-making and data analysis. AI challenges the very legal architecture and approaches of most privacy laws and poses vexing problems for oversight, participation and accountability.

Legal architecture and approaches

Existing privacy laws have long embraced approaches and strategies that are ill-suited for the digital age. AI exposes these problems quite clearly and emphatically.

Beyond individual control and self-management. Privacy regulation has traditionally emphasized a model of individual control referred to as "privacy self-management,"[2] but individuals are often unable to make informed decisions to manage their privacy. AI starkly highlights the inadequacies of the individual control model. The complexity and scale of AI exceed the capacity of individuals to grasp or evaluate its implications for their privacy. To ensure effective privacy protection, the law must put less onus on individuals to protect themselves and must mandate significant obligations on organizations to mitigate risks and harms and to ensure these entities are held accountable.

Harm and risk analysis. New AI laws are taking a harm and risk approach, which should be applauded. But there are challenges with the harm and risk approach that the law must address.[3] First, who should determine the harms and risks? The organizations that develop and use AI? A government agency? Second, how much should the law operate prior to the deployment of AI (ex ante) versus after AI tools have been released (ex post)? If the law is too ex ante, it could chill innovation. Harms and risk can sometimes be difficult to determine in advance. If the law is too ex post, it might fail to stop severe harms.

[2] I have explored these problems in many articles. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013); Daniel J. Solove, *The Limitations of Privacy Rights*, 98 Notre Dame L. Rev. 975 (2023); Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U. L. Rev. __ (forthcoming 2024).

[3] Margot Kaminski's article about risk regulation of AI is essential reading. Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. Rev. 1347 (2023).

Data collection

Data collection problems involve issues with AI's inputs. AI creates severe data collection problems because of its insatiable hunger for data.

Scraping. Much data used for AI is obtained by "scraping" — the automated gathering of data online. Scraping often violates most privacy principles found in legislation, industry codes or established norms. With scraping, third parties collect data without providing notice, obtaining consent, implementing safeguards, stating specific purposes, adhering to purpose limitations, practicing data minimization, respecting individual rights, observing data retention limitations, and much more.

"Consensual" data collection. In the mad scramble to gather data for AI, companies have quickly revised their privacy notices to bestow upon themselves the power to use people's data for AI.[4] Deeming people to have "consented" to this use is a fiction.

Data generation

Turning from inputs to outputs, AI not only ingests personal data but also generates personal data.

Inferences. Through inference, machine learning algorithms can produce new data that unexpectedly exposes personal details.[5] This blurs the distinction between data collection and processing, circumventing privacy protections and leaving individuals with little control over the data organizations can ascertain about them.

Simulation. AI's ability to simulate humans raises questions about whether to inform people that they are interacting with a simulation. Even if people know AI is a simulation, human verisimilitude provokes strong emotional responses in people that might be too manipulative.

Malevolent material. AI can also generate malevolent material, which can make it easier to deceive and manipulate people.

[4] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. Rev. 593 (2024).

[5] Alicia Solow-Niederman's terrific piece discusses this problem with great detail and insight. Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 Nw. L. Rev. 357, 361 (2022).

Decision-making

Another set of AI outputs involves the use of AI algorithms to make decisions about people.

Predictions. AI's capability to predict future behaviors can result in preemptive actions and judgments for actions not yet taken, undermining human autonomy, constraining individuals' freedom to determine their own futures. Algorithmic predictions tend to "fossilize" the past. Consequently, they can project existing inequalities and biases into the future. Such forecasts can turn into self-fulfilling prophecies, particularly when they trigger responses that solidify the expected results.[6]

Decisions and bias. Algorithms shift decision-making towards quantifiable metrics, often sidelining qualitative considerations. AI is hard to cleanse of bias because the data it feeds upon is riddled with it. Even if AI algorithms avoid discrimination based on legally restricted characteristics, the algorithms may use other characteristics to discriminate, such as baldness, weight and height. Thus, AI may give rise to new forms of discrimination.

Automation. AI automation shifts decision-making towards measurable factors, neglecting the nuanced, non-quantifiable aspects of individuals. Focusing on quantifiable data can skew decisions and impoverish them.[7] Additionally, bias embedded in AI can be ruthlessly systematic in ways far beyond human bias.

Data analysis

AI data analysis can dramatically increase the power of entities engaging in surveillance or data gathering about people.

Surveillance. AI technologies facilitate mass surveillance on a scale never before seen. Many societies already possess a robust surveillance infrastructure. However, the real power lies in data analysis. As noted by Bruce Schneier, AI will make surveillance data much more "searchable, and understandable, in bulk."[8] Thus, AI is poised to significantly exacerbate the detrimental impacts of surveillance.

[6] Hideyuki Matsumi & Daniel J. Solove, *The Prediction Society: Algorithms and the Problems of Forecasting the Future*, forthcoming 2025 U. Ill. L. Rev.

[7] Daniel J. Solove & Hideyuki Matsumi, *AI, Algorithms, and Awful Humans*, 92 Fordham L. Rev. 1923 (2024).

[8] Bruce Schneier, *The Internet Enabled Mass Surveillance. A.I. Will Enable Mass Spying*, Slate, Dec. 4, 2023.

Identification. AI enhances the ability to identify individuals through biometric information. This ease of identification boosts government power, creating risks of misuse. AI identification can better enable governments to pinpoint and apprehend those they deem undesirable.

Interpretation and deciphering. AI not only aids in managing government data but also significantly enhances the ability to interpret and understand this information. This shift in capability epitomizes how AI intensifies existing issues to a degree that fundamentally changes the landscape.

Limitation and oversight. Currently, the law grants the government considerable leeway to conduct surveillance and to collect and acquire data — often without adequate oversight or limitation. For example, in the U.S., the Fourth Amendment imposes minimal constraints on the duration for which the government can retain personal data and the methods it can use to analyze this data.

Oversight, participation and accountability

AI raises difficult challenges for regulatory oversight, stakeholder participation and accountability.

Transparency. AI introduces significant challenges to transparency due to the dynamic and often opaque nature of algorithms. Understanding these algorithms typically requires access to the training data, which is often neither accessible nor understandable to the general public and disclosing it could compromise privacy. The sheer volume of data involved is also overwhelming for individuals. Moreover, many AI algorithms continually adapt and learn from new data, making it essential for their assessment to be an ongoing process — a task that is impractical for most people to perform.

Due process. AI poses challenges to due process, as individuals frequently lack meaningful ways to challenge AI decisions.[9]

Accountability. Sufficient accountability for AI is often lacking. Effective regulatory frameworks should incorporate both internal and external accountability measures.

[9] Two classic works on this issue are: Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2007); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

Organizations must be held accountable with significant repercussions for any harm or risks they generate.

Stakeholder involvement. AI is being developed in a manner that excludes affected stakeholders, particularly those from underrepresented and marginalized communities.[10] There is a strong case to require developers of AI to incorporate feedback from a diverse group of stakeholders.

Enforcement and remedies. Regulatory enforcement struggles to keep pace with the immense rewards associated with developing successful AI technologies, resulting in unchecked risk-taking. Implementing measures like algorithmic destruction can be quite challenging.

The need for privacy law reform

AI impacts privacy in ways that often do not introduce entirely new problems, but instead modify and intensify existing ones. Current privacy laws are quite inadequate in addressing the challenges brought by AI. The outdated approaches that persist in most privacy laws are particularly unsuitable for managing AI's complexities.

With policymakers increasingly focusing on AI, this is a critical moment to address the longstanding issues and ineffective strategies of privacy law to ensure it effectively governs AI's impact on privacy.

* * *

This essay is a short overview of Daniel Solove's forthcoming article, Artificial Intelligence and Privacy, 77 Florida Law Review (forthcoming 2025). You can download the article for free here.

This essay was originally published at IAPP News.

Daniel J. Solove is the Eugene L. and Barbara A. Bernard Professor of Intellectual Property and Technology Law at the George Washington University Law School. He is also the founder of TeachPrivacy, a privacy and cybersecurity training company.

[10] Ngozi Okidegbe, *The Democratizing Potential of Algorithms?*, 53 Conn. L. Rev. 739 (2022).