

**Privacy Regulation Roundup – March 2024**

This Privacy Regulation Roundup summarizes the latest major global privacy regulatory developments, announcements, and changes. This report is updated on a monthly basis. For each relevant regulatory activity, you can find actionable Info-Tech analyst insights and links to useful Info-Tech research that can assist you with becoming compliant.

Contents

[CUPE Study of Bill C-27 Submitted to the SCIT, Calls for the AIDA to Be Redrafted 3](#_Toc161908804)

[Type: Announcement 3](#_Toc161908805)

[Announced: February 2024 3](#_Toc161908806)

[Advancing Neuroprivacy: Global Legislative Efforts to Safeguard Neural Data 4](#_Toc161908807)

[Type: Legislation 4](#_Toc161908808)

[Announced: February 2024 4](#_Toc161908809)

[European Commission to Establish an AI Office 5](#_Toc161908810)

[Type: Announcement 5](#_Toc161908811)

[Announced: February 2024 5](#_Toc161908812)

[President Biden Signs Executive Order on “Preventing Access to Americans’ Bulk Sensitive Data and United States Government-Related Data by Countries of Concern” 6](#_Toc161908813)

[Type: Executive Order 6](#_Toc161908814)

[Date: February 2024 6](#_Toc161908815)

[IP Addresses and Privacy Rights: A Legal Shift 7](#_Toc161908816)

[Type: Court Decision 7](#_Toc161908817)

[Date: March 2024 7](#_Toc161908818)

# CUPE Study of Bill C-27 Submitted to the SCIT, Calls for the AIDA to Be Redrafted

**Type:** Announcement

**Announced:** February 2024

**Summary:** The increasing prevalence of AI brings both transformative potential and serious risks to the workplace. The recent submission from the Canadian Union of Public Employees (CUPE) to the Standing Committee on Industry and Technology (SCIT) rightly emphasizes the lack of a robust regulatory framework for AI in Canada, particularly in the Artificial Intelligence and Data Act (AIDA) within Bill C-27. Left unchecked, AI has the potential to exacerbate job insecurity, erode worker privacy and rights, and degrade the very nature of the public services that CUPE members provide.

Unregulated AI systems, driven by a relentless focus on efficiency, can perpetuate pre-existing biases and deepen social inequities. The use of AI in hiring, for example, may amplify discriminatory patterns within seemingly objective data sets. Moreover, without clear guidelines and oversight, AI tools introduced under the guise of productivity can lead to intrusive monitoring, further eroding both workplace privacy and worker autonomy.

CUPE’s advocacy is crucial in this evolving landscape. Its call for stronger worker protections within Bill C-27, including mandatory consultations with employees and unions before AI implementation, is a necessary step. It is through proactive participation in the legislative process and informed bargaining at the workplace level that we can build safeguards and ensure AI serves to enhance worker wellbeing and public services, not undermine them.

**Analyst Perspective:** Bill C-27’s current form poses significant risks to workers and public services due to its weak AI regulation. CUPE’s timely intervention spotlights how unregulated AI can degrade workers’ rights, privacy, and job security while also potentially harming the delivery of public services. The union’s push for stronger protections, including worker consultation and stricter oversight, aligns with concerns about AI perpetuating bias and amplifying inequality. Its advocacy highlights the urgency of balancing AI’s potential with robust safeguards to ensure it works for, not against, both workers and the communities they serve.

**Analyst:** [Carlos Rivera](https://www.infotech.com/profiles/carlos-rivera), Principal Advisory Director – Security & Privacy

**More Reading:**

* Source Material: [IAPP](https://iapp.org/news/a/canadian-public-employees-union-comes-out-against-aida/), [EU Commission](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206), [CUPE Study](https://cupe.ca/sites/default/files/submission_study_of_bill_c-27_digital_charter_implementation_act_2022_-_2024-01-29.pdf)
* Related Info-Tech Research:
  + [*AI Research Center*](https://www.infotech.com/research-centers/artificial-intelligence-research-center)
  + [*Build Your AI Strategic Roadmap*](https://www.infotech.com/research/ss/build-your-ai-strategic-roadmap)

# Advancing Neuroprivacy: Global Legislative Efforts to Safeguard Neural Data

**Type:** Legislation

**Announced:** February 2024

**Summary:** Legislators in Colorado and Minnesota are introducing bills to secure neural data gathered by devices that scan the brain. These devices, which include everything from sleep monitors to brain-computer interfaces, are currently not federally regulated outside of medical settings. The Colorado bill aims to modify the state’s privacy law, while the Minnesota bill seeks to institute “cognitive liberty” with civil and criminal penalties for misuse. There is a critical need for industry standards and federal supervision to prevent potential misuse of sensitive brain data. The Neurorights Foundation has had an impact on neuroprivacy laws in Chile and is collaborating with other nations and the UN to tackle the implications of neurotechnology. The growing domain of neurotechnology and the privacy issues it brings to the forefront emphasize the necessity of creating legal frameworks to protect cognitive liberty and prevent misuse of sensitive brain data as neurotechnology continues to evolve.

**Analyst Perspective:** The rapidly evolving progress of neurotechnology, including brain-scanning devices, has led lawmakers in Colorado and Minnesota to suggest legislation for the protection of neural data privacy. This proactive step into largely unexplored areas signifies a forward-thinking approach to consumer data privacy, addressing potential issues before the technology becomes pervasive. The proposed laws could have a significant impact on companies developing neurotechnology, such as Meta Platforms Inc., which is developing noninvasive products to assist individuals with speech loss. The lack of federal regulations outside the medical sphere highlights the need for preemptive industry standards before state or federal intervention. International efforts are also taking place, such as Chile’s trailblazing role in incorporating mental privacy and free will into its constitution. This global trend indicates that brain-related data might soon be classified as a unique category of sensitive data, requiring careful deliberation by both developers and legislators. The drive for neuroprivacy legislation, although still in its infancy, signifies a growing consciousness of the potential risks linked with neurotechnology. Success in states like Colorado could serve as a blueprint for others, potentially leading to federal action in the United States.

**Analyst:** [Horia Rosian](https://www.infotech.com/profiles/horia-rosian), Director – Cybersecurity & Privacy, Workshops

**More Reading:**

* Source Material: [IAPP](https://iapp.org/news/a/us-states-look-towards-privacy-safeguards-for-brain-scanning-technology/), [Bloomberg Law](https://news.bloomberglaw.com/privacy-and-data-security/brain-scanning-technology-spurs-state-moves-on-neural-privacy)
* Related Info-Tech Research:
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)
  + [*Build a Security Compliance Program*](https://www.infotech.com/research/ss/build-a-security-compliance-program)

# European Commission to Establish an AI Office

**Type:** Announcement

**Announced:** February 2024

**Summary:** The European Commission has announced the launch of the European AI Office to help the EU’s 27 members leverage AI safely and responsibly. The objective of this office, which was announced in February, is to support the development and use of AI with a safe and secure approach. The AI Office will also be seen as a center of excellence of AI across the EU in implementing its AI Act. The Act is the first-ever legal framework on AI in the world, and it aims to guarantee the safety and rights of EU citizens while also providing legal clarity to businesses that operate within the region. The AI Act will also aim to support different AI initiatives being implemented by member states and welcome collaboration with those states and industry experts through a dedicated working group. Some of the tasks of the AI Office will include supporting general-purpose AI rules such as developing tools, methodologies, and benchmarks for evaluating the capabilities of AI models, as well as setting up evaluation of models to assess their capabilities and investigate any infringements of rules. These initiatives are all contributing to the EU’s strategy to promote trustworthy AI, which will include collaboration with other institutions worldwide.

**Analyst Perspective:** With rampant evolution of AI technologies, organizations are looking for opportunities to build their AI strategies to garner the benefits of AI. However, innovative technology comes with potential risks that must be addressed. When leveraging these technologies, you need to ensure your organization benefits while also protecting customers. The development of an AI office within the EU depicts the first steps government agencies are taking to establish guidelines for how the technology can be used. The guidelines on how to implement the AI Act within each member state, along with the tools and methodologies being developed, will provide organizations operating in these regions with standards they have to comply with. This assures customers and citizens of the member states that organizations are developing AI with a safe approach that is overseen by their governing bodies.

Other nations are exploring the development of similar AI regulation approaches, such as the US government’s executive order on safe, secure, and trustworthy use of AI. Government agencies need to do their due diligence to guide organizations on the responsible use of AI. Many other nations might follow suit in establishing an AI office to promote and provide guidance on the use of AI within their country.

**Analyst:** [Ahmad Jowhar](https://www.infotech.com/profiles/ahmad-jowhar), Research Analyst – Security & Privacy

**More Reading:**

* Source Material: [European Commission](https://digital-strategy.ec.europa.eu/en/policies/ai-office), [IAPP](https://iapp.org/news/a/european-commission-establishes-european-ai-office/), [Global Compliance News](https://www.globalcompliancenews.com/2024/02/18/https-insightplus-bakermckenzie-com-bm-technology-media-telecommunications_1-europe-the-european-union-unveils-its-artificial-intelligence-office_1_06312024/), [The White House](https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/)
* Related Info-Tech Research:
  + [*AI Research Center*](https://www.infotech.com/research-centers/artificial-intelligence-research-center)
  + [*Build Your AI Strategic Roadmap*](https://www.infotech.com/research/ss/build-your-ai-strategic-roadmap)

# President Biden Signs Executive Order on “Preventing Access to Americans’ Bulk Sensitive Data and United States Government-Related Data by Countries of Concern”

**Type**: Executive Order

**Date:** February 2024

**Summary:** On February 28, 2024, an executive order was issued by President Biden with the aim of shielding the sensitive personal data of Americans from potential misuse by nations deemed as threats. The order prioritizes the protection of various types of data including genomic, biometric, health-related, geolocation, and financial data, as well as certain personal identifiers. The Department of Justice is tasked with formulating regulations to hinder large-scale data transfers to these nations and to secure sensitive data related to the government. A collaborative effort will be made by different departments to ensure that federal grants and contracts do not inadvertently provide these nations with access to sensitive health data. This executive order is a significant step toward ensuring American’s privacy and data security against foreign threats. It also signifies the United States’ dedication to tackling global data security issues, particularly in a world where data is constantly crossing borders. The order was issued in the context of escalating geopolitical tensions and growing worries about state-sponsored cyberattacks. By securing sensitive data, the US seeks to lessen the risks brought about by hostile nations looking to exploit weaknesses. Legal professionals foresee potential difficulties in defining the term “countries of concern” and in striking a balance between national security and individual rights. The constitutionality of the order and its effects on international relations may be subject to judicial review. In conclusion, while President Biden’s executive order demonstrates a forward-thinking approach to data security, its execution will necessitate careful maneuvering through intricate legal, diplomatic, and technological terrains.

**Analyst Perspective:** The executive order is a significant step toward the protection of personal data, mirroring the escalating concerns over data privacy and national security. It targets highly sensitive data such as personal identifiers and genomic, biometric, health, geolocation, and financial data that is susceptible to misuse. The Department of Justice will create regulations to prevent the large-scale transfer of data to countries of concern and to safeguard sensitive government-related data. The measures are designed to strike a balance between the free flow of data and privacy and security, without impeding consumer, economic, scientific, and trade relationships. Industries such as healthcare, biotechnology, and finance will need to adjust. Adherence to new regulations may necessitate improved cybersecurity measures, data localization, and risk assessments. The order highlights the importance of interagency collaboration. Diplomatic efforts will be key to aligning data protection standards worldwide, promoting cooperation while addressing potential conflicts. Achieving the right balance between data privacy and innovation continues to be a challenge, and policymakers must ensure that protective measures do not suppress technological progress or obstruct cross-border research. The order emphasizes the necessity for public awareness campaigns on data privacy; educating citizens on risks and best practices will better equip them to protect their personal information. This action underscores the significance of data protection in the digital age and the need for comprehensive privacy legislation.

**Analyst:** [Horia Rosian](https://www.infotech.com/profiles/horia-rosian), Director – Cybersecurity & Privacy, Workshops

**More Reading:**

* Source Material: [The White House](https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/)
* Related Info-Tech Research:
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)
  + [*Build a Security Compliance Program*](https://www.infotech.com/research/ss/build-a-security-compliance-program)

# IP Addresses and Privacy Rights: A Legal Shift

**Type:** Court Decision

**Date:** March 2024

**Summary:** The Supreme Court of Canada recently issued a significant privacy ruling. According to the decision in R v. Bykovets, police must now obtain a warrant or court order before requesting IP addresses from organizations. The ruling is a result of police seeking IP addresses from a third-party payment processing company during fraud investigation. The court recognized that individuals have a reasonable expectation of privacy for their IP addresses, which are essential for internet access and link online activities to user identities. As such, requesting an IP address without proper authorization violates individual privacy rights. The court decision overturned previous rulings and ordered a new trial for the defendant.

Critics argue that this ruling could impede law enforcement efforts against cybercrime and create practical challenges in the digital age. They claim that it could compromise internet security by complicating matters for businesses and presenting hurdles for police investigations, raising questions about whether the same level of privacy should apply online as in the physical world.

The approach taken by the majority in the Supreme Court decision acknowledges the interconnected nature of data on the web. While IP addresses may not individually divulge much, when combined with other data, they can be quite revealing. This ruling extends the Canadian Charter of Rights and Freedoms protection to IP addresses, impacting law enforcement protocols and prompting organizations to reconsider how they share information with authorities.

**Analyst Perspective:** The recent ruling represents a significant change in how IP addresses are treated within privacy laws. This shift has implications beyond IP addresses, potentially affecting other digital data like location information. Private organizations must take precautions when sharing information with state-based entities and must safeguard relevant records. Organizations that track IP addresses need to ensure their practices align with privacy laws and regulations, possibly adjusting their data collection and handling procedures accordingly.

Additionally, this ruling may impact targeted advertising practices. Organizations might need to rely more on alternative methods, such as contextual advertising based on website content, rather than user-specific data like IP addresses. Obtaining explicit consent from individuals before tracking their IP addresses for advertising or marketing purposes, having clear and accessible privacy policies explaining IP address usage, and allowing users to opt out of tracking may become more important.

Furthermore, individuals now have a recognized expectation of privacy regarding their IP addresses. Organizations tracking these addresses must prioritize data security measures to prevent unauthorized access, breaches, and misuse. This decision sets a precedent across Canada, extending to the Personal Information Privacy and Electronic Documents Act (PIPEDA) and potentially impacting various sectors and activities.

**Analyst:** [Safayat Moahamad](https://www.infotech.com/profiles/safayat-moahamad), Research Director – Security & Privacy

**More Reading:**

* Source Material: [Supreme Court of Canada](https://www.scc-csc.ca/case-dossier/cb/2024/40269-eng.aspx), [McCarthy Tetrault](https://www.mccarthy.ca/en/insights/blogs/techlex/supreme-court-canada-rules-ip-addresses-attract-reasonable-expectation-privacy)
* Related Info-Tech Research:
  + [*Discover and Classify Your Data*](https://www.infotech.com/research/ss/discover-and-classify-your-data)
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Build a Security Compliance Program*](https://www.infotech.com/research/ss/build-a-security-compliance-program)