Final Report to the AI Strategy Task Force
Submitted by: Taylor Owen[1]

As part of the Federal Government's AI Strategy Task Force I was asked to provide input on the theme of Safe AI & Public Trust. Given the broad nature of this topic, I have chosen to focus this report on what I believe are core imperatives of democratic governance: ensuring that AI systems and other digital technologies used by Canadians are safe, contribute to the health of our democratic society, and are governed in ways that sustain public confidence. In what follows, I recommend a series of policies to achieve these goals organized into three priority areas (Citizen Safety, Information Ecosystem Integrity, and Democratic Legitimacy), most of which could be implemented through two existing federal governance frameworks:

- An amended version of the *Online Harms Act* that includes AI platforms within its scope;
- An amended version of the *Consumer Privacy Protection Act*.

By leveraging these frameworks, the Canadian government could ground its approach to AI governance in best international practices, move swiftly to ensure that Canadians are protected from immediate harms that AI systems pose,[2] and facilitate safe AI innovation and adoption.[3] Given low levels of trust in AI amongst Canadians,[4] legitimate concerns about its safety, and genuine uncertainty over how it will affect our economy and society, effective governance is imperative to solidifying Canadians' collective confidence in a future of Canada that is increasingly reliant on and intertwined with AI development, research, and implementation. Without this confidence, a sovereign AI innovation and adoption agenda is fraught with risk that undermines the government's investments in AI and the public's trust that it will do so responsibly.

The research centre I founded at McGill University seeks to better understand these complex systems, and to help citizens and their democratic governments maximize the benefits and minimize the harms posed by digital technologies, including AI. Through academic and policy research, years of public consultation, and close relationships with expert partners, we have built a deep empirical understanding of the impacts of the digital ecosystem on Canadians, and the policy mechanisms that advance a uniquely Canadian mix of public priorities for digital governance. This memo's perspectives grow out of that work, while also drawing from other

---

[1] Beaverbrook Chair in Media, Ethics and Communication in the Max Bell School of Public Policy, and Founding Director of the Centre for Media, Technology and Democracy, McGill University. This memo was written in collaboration with Helen A. Hayes, Associate Director, Policy, Centre for Media, Technology and Democracy.
[2] These harms, outlined below, include individual harms like race and gender-based stereotyping and collective harms, including the amplification of mis- and dis-information.
[3] Canada's G7 presidency in 2025 presents a unique opportunity to translate international commitments—such as the G7 Leaders' Statement on AI for Prosperity—into concrete domestic policies that meet the highest standards for safety and democratic values.
[4] According to KPMG's Trust, attitudes and use of artificial intelligence: A global study 2025, Canada ranks among the lowest globally in perceived trustworthiness of AI systems, with only 46% of respondents expressing trust. Similarly, Telus' Human-centric AI, perspectives on trust and the future of AI report finds that 70% of Canadians believe AI poses serious risks that society is not adequately prepared to address, and, notably, that only 1% of Canadians trust AI to operate independently.

expert scholars and civil society organizations; investigations into AI systems by international regulators; and statements and policy commitments made by governments around the world.

In summary, my opinion is that:

1. AI systems are increasingly embedded in Canadians' daily lives, shaping what we see,[5] the work we do,[6] the decisions we make,[7] and the services we access.[8] These systems mediate how citizens access information,[9] engage with public institutions,[10] and make decisions that shape their social and economic lives. This adoption is moving at a historically unprecedented rate.
2. For some, AI tools, particularly generative, conversational, and agentic systems, can enhance creativity,[11] facilitate learning,[12] and provide accessible forms of interaction or self-expression.[13]
3. For many others, AI systems pose significant risks and harms. Empirical studies have documented instances where AI chatbots, for example, fail to respond appropriately to users experiencing mental health crises,[14] reinforce cognitive distortions through mirroring language,[15] and cultivate a false sense of emotional reciprocity.[16] Beyond individual wellbeing, AI systems have also been shown to amplify mis- and dis-information,[17] enable non-consensual image generation[18] and impersonation,[19] perpetuate race- and gender-based stereotyping and inequalities,[20] and manipulate users through data-driven optimization for engagement.[21]
4. Public concern about AI in Canada is widespread and deeply held: only 32% of Canadians believe that the benefits of AI outweigh the risks,[22] 89% worry about their privacy,[23] 78% fear that AI will spread false information during elections,[24] and 70% are concerned about their children accessing AI chatbots.[25] In the 2025 election, polling we conducted at the

[5] Guess et al. 2023; Cinelli et al. 2021
[6] KPMG 2025.
[7] Levy et al. 2021; Lang 2021; Sumer 2024
[8] Pham et al. 2024; Ashraf et al. 2024; Sollapur et al. 2024
[9] Brown et al. 2024; Edelson et al. 2025
[10] Frangoudes et al. 2021; Senadheera et al. 2024
[11] Agboola and Yassin 2025; Chandrasekara et al. 2024
[12] Chiu and Rospigliosi 2025; Aluko et al. 2025
[13] Chemnad and Othman 2024; Penuela et al. 2024
[14] De Freitas et al. 2023; Dergaa et al. 2024
[15] Alabad et al. 2024 ; Yankouskaya et al. 2025
[16] Zhang et al. 2025; Laestadius et al. 2022; Li and Zhang 2024
[17] Canadian Digital Media Research Network 2025; Wack et al. 2025
[18] Hawkins et al. 2025; Umbach et al. 2024
[19] Tariq et al. 2022; Jasserand 2024
[20] Scheuerman et al. 2020; Omiye, J. A. et al. 2023
[21] Du and Sen 2023; Roberts and David 2025
[22] KPMG 2025.
[23] Office of the Privacy Commissioner of Canada, 2025.
[24] Leger 2025.
[25] Leger 2025.

Centre found that one in four Canadians encountered fake news sites, and that 80% of Canadians were concerned about AI-generated, misleading content.[26]

5. These harms originate from the structural dynamics of AI systems, which are shaped by corporate and economic incentives that govern their design, deployment, and diffusion. These conditions are largely insulated from democratic oversight.
6. Without this oversight, Canadians' trust in AI systems will remain low. 88% of Canadians support stronger governance of AI systems,[27] 85% want government oversight to ensure ethical and safe use,[28] and 80% believe that there should be penalties for AI-generated dis-information.[29]
7. If technical solutions do not make AI more trustworthy or the public does not perceive AI to be trustworthy despite those technical solutions, then trust must instead be built in the democratic infrastructure that governs AI. So, Canada's democratic institutions need to be capable of holding AI companies to account if and when they are irresponsible.
8. Canada is not alone in this: governments around the world[30] are beginning to enact legislation that addresses the structures, design, and incentives of AI and other digital technologies. They recognise that digital sovereignty[31] demands not just infrastructure, but also governance. Canada can learn from these and other best practices.
9. International precedent has demonstrated that effective AI governance does not necessarily require generalized AI legislation (such as the previous government's *Artificial Intelligence and Data Act*), but can at least initially be achieved through a range of existing and targeted policy mechanisms.
10. In Canada, there are two existing governance frameworks that could be quickly implemented by Canada's federal government to address the root causes of AI harm and promote safer systems: 1) an amended and re-introduced version of the *Online Harms Act* that includes AI platforms within its scope; and, 2) an amended and re-introduced version of the *Consumer Privacy Protection Act.*
11. While these governance frameworks will require policy iteration and innovation over time and may at some point fall short and demand stand-alone AI regulation, it is imperative that the Canadian government build a foundation of AI policy capacity. Doing so will ensure the baseline democratic accountability that Canadians rightly demand, and provide the time for a next phase of public consultation and policy iteration and design.

---

[26] The Canadian Digital Media Research Network 2025.
[27] Telus 2025.
[28] Leger 2025.
[29] The Canadian Digital Media Research Network 2025.
[30] Across Europe, the democratic global south, and at the US state-level.
[31] Canada's digital ecosystem and infrastructures are largely determined by foreign platforms, rules, and shareholder value. This leaves Canadian institutions and citizens vulnerable to the incentives of powerful, unpredictable, and uncontrollable foreign forces, and threatens Canada's digital sovereignty.

Summary of Policy Recommendations and Implementation Tactics

	Citizen Safety	Info Ecosystem Integrity	Democratic Legitimacy
Amended and Re-introduced *Online Harms Act*	Digital Safety Commission (1.1)[32] Systemic Risk Governance (1.2)[33] Age-Appropriate Design (1.3)[34]	Monitoring and Data Sharing (2.2)[35]	Recourse Mechanisms (3.2)[36]
Amended and Re-introduced *Consumer Privacy Protection Act*		AI Identification and Provenance Disclosure (2.1)[37]	Data Portability, Interoperability, and Right to Deletion (3.1)[38] User Empowerment Support (3.2)[39]
Other Measures		Reliable Information Production (2.3)[40]	Mandated Consultation Mechanisms (3.3)[41]

[32] The Digital Safety Commission would have authority to: 1.1.1) regulate data access; 1.1.2) conduct algorithmic audits; and, 1.13) enforce compliance by issuing orders, penalties, and corrective action plans.
[33] This would include three duties to: 1.2.1) act responsibly; 1.2.2) protect children; and, 1.2.3) make certain content inaccessible. It should also minimize users' exposure to other forms of harmful content, including fraud and scam content.
[34] This requires heightened safety and design standards, overseen by the Digital Safety Commission, including: 1.3.1) child-impact assessments; 1.3.2) default high-privacy settings; and 1.3.3) crisis-response protocols for conversational systems.
[35] At a minimum, this includes: 2.2.1) mandated data inventories of AI system inputs and outputs; 2.2.2) secure researcher access frameworks for data on social media and consumer chatbot use and algorithmic design, facilitated by an independent monitoring or observatory body; and, 2.2.3) confidentiality-safe data enclaves for public-interest research.
[36] This would involve 3.2.1) establishing a statutory AI and Digital Safety Ombudsperson within the Digital Safety Commission.
[37] This should include: 2.2.1) visible labelling; 2.2.2) provenance metadata and digital watermarking; and, 2.2.3) source transparency requirements.
[38] This should include: 3.1.1) interoperable data standards; 3.1.2) user-initiated data mobility rights; 3.1.3) public disclosure of interoperability specifications, and, 3.1.4) mandated right to deletion for users.
[39] This include: 3.2.2) mandatory human review of consequential automated decisions; and, 3.2.3) public reporting obligations.
[40] The government could: 2.3.1) consider adapting existing journalistic support mechanism to, and develop new programs for, a broader range of journalistic content creators and reliable content generations forms; 2.3.2) support new sovereign, decentralized infrastructure for public interest media; and, 2.3.3) actively engage in domestic and international efforts to transition the journalism sector to a new AI-driven mediated information ecosystem.
[41] This could include: 3.3.1) standing citizens' assemblies or deliberative panels; 3.3.2) structured partnerships between civil society organizations and academic researchers; and 3.3.3) mandated and regularly held advisory councils.

Democratic Priority 1: Citizen Safety

One of the most fundamental obligations of a democratic government is to ensure the safety and security of its citizens.[42] As new AI technologies enter the Canadian market,[43] this responsibility extends to ensuring that they do not expose individuals or communities to preventable harms. On this measure, Canada has fallen short. While the decision to delay comprehensive AI legislation may reflect a desire for measured policy development, the absence of enforceable safety obligations has left Canadians under protected in a rapidly evolving digital marketplace.[44] The core challenge is not merely technological, but structural: AI systems are being designed, deployed, and monetized by private actors who bear little legal responsibility for the risks their systems create. Addressing this requires moving beyond voluntary ethics frameworks and industry self-regulation toward binding legal mechanisms that assign clear accountability and remedies. In order to protect Canadians from AI harms, the government should consider:

1.1 Independent Regulatory Authority. The asymmetry between global technology firms and national governments (both in technical capacity and access to information) makes independent regulatory authority not a procedural detail but a democratic necessity. Canada should create a single, empowered institution responsible for coordinating national digital governance (i.e., social media and consumer-facing AI) through new online harms legislation. This Digital Safety Commission[45] would have authority to: 1.1.1) mandate data access;[46] 1.1.2) conduct algorithmic audits;[47] and 1.1.3) enforce compliance by issuing orders, penalties, and corrective action plans.[48]

1.2 Systemic Risk Governance. The Digital Safety Commission, as proposed in Part 1 of the *Online Harms Act*, should adopt a systems-level duty of care for AI systems (once scoped in), which 1.2.1) obliges providers to assess and mitigate systemic risks before and after deployment (*duty to act responsibly)*;[49] 1.2.2) requires heightened protections for minors (*duty to protect*

[42] Anderljung et al. 2023; Coeckelbergh 2024
[43] Benchetrit 2025; Steven 2025
[44] Competition Bureau 2025; Du and Sen 2023
[45] In addition to the establishment of a Digital Safety Commission, it is also important for the Government of Canada to have a central digital governance coordinating capacity in order to overcome the soloing of digital polices between departments. In addition, it is critical that the Digital Safety Commission, the Office of the Privacy Commissioner of Canada and the Competition Bureau be empowered to share data and collaborate.
[46] This can be accomplished by applying sections 73-77 of Bill C-63, which provides mechanisms for a Commission to grant access to inventories and electronic data of the operators of social media services.
[47] The EU's Digital Services Act Article 37 requires very large online platforms to contract an independent auditor to assess compliance. In Canada, this function could be filled by a designated Commission, rather than left to independent auditors, such as the proposed Digital Safety Commission in Bill C-63.
[48] These powers are assigned to the Digital Safety Commission in Bill C-63.
[49] This can be accomplished by adapting Bill C-63, Section 54: operators "must implement measures that are adequate to mitigate the risk that users of the regulated service will be exposed to harmful content on the service." The EU's AI Act Article 51 further provides definitions and obligations for operators of general-purpose AI models that entail systemic risk.

children);[50] and, 1.2.3) mandates categorical removal of certain categories of content and updating of models,[51] including child sexual abuse material and non-consensual intimate images (*duty to make certain content inaccessible).*[52] Beyond this, systemic risk governance should also minimize users' exposure to other forms of harmful content, including fraud and scam content.[53]

1.3 Age-Appropriate Design. Democratic societies have distinct obligations to protect children and youth in digital environments.[54] Beyond content-based governance mechanisms, this requires heightened safety and design standards, overseen by the Digital Safety Commission, including: 1.3.1) child-impact assessments;[55] 1.3.2) default high-privacy settings;[56] and, 1.3.3) crisis-response protocols for conversational systems.[57]

Democratic Priority 2: Information Ecosystem Integrity

Democratic societies demand access to reliable information. AI is reshaping our information ecosystem in two ways: it is used to determine our personalised feeds of content,[58] and is increasingly creating content itself.[59] In the near future, the majority of what we see online may

[50] This can be accomplished by adapting Bill C-63, Section 65: "an operator must integrate into a regulated service that it operates any design features respecting the protection of children, such as age-appropriate design, that are provided by regulations." The EU's AI Act also obligates operators to identify and address unique vulnerabilities of minors on digital platforms. California Senate Bill 243 additionally requires special protections for minors using chatbot platforms. The UK's Online Safety Act includes specific provisions for child safety, such as requiring platforms to use effective age assurance to prevent children from accessing harmful content.

[51] Examples of this include: the EU's Digital Services Act requirement for platforms to remove or disable access to illegal content and easily enable users to flag such content; the UK's Online Safety Act requirement that platforms remove illegal content, including fraud, incitement of violence, and content that promotes suicide. Luccioni et al., 2022.

[52] This can be accomplished by adapting Bill C-63, Sections 67-71, which obligates operators of regulated service to remove content that "sexually victimizes a child or revictimizes a survivor or intimate content communicated without consent" within 24 hours of identification.

[53] This can be accomplished by adapting Bill C-63, Section 54: operators "must implement measures that are adequate to mitigate the risk that users of the regulated service will be exposed to harmful content on the service" and by adding online scams and fraud as a category of harm.

[54] The UN Committee on the Rights of the Child's General Comment No. 25 clarifies that Canada's obligation to protect children's rights applies in the digital world, which explicitly encompasses AI technologies; This further contributes to the global consensus that children's rights must be protected in the age of AI, as reflected in the UN High-Level Advisory Body on AI's 'Governing AI for Humanity', UN General Assembly resolution 78/187 on the Rights of the child in the digital environment, and UNICEF's Policy guidance on AI for children.

[55] These assessments should be designed around the "best interests of the child". See UNCRC General comment No. 25, paras. 23 and 38, the Canadian Department of Justice, Child Rights Impact Assessment tool and e-learning course, and UNICEF, Assessing child rights impacts in relation to the digital environment.

[56] This aligns with the Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight "Putting best interests of young people at the forefront of privacy and access to personal information"; the Roundtable of G7 Data Protection and Privacy Authorities Statement on AI and Children; and the Sweep Report 2024: Deceptive Design Patterns.

[57] Examples of this includes California Senate Bill 243, which obligates conversational AI platforms to maintain "a protocol for preventing the production of suicidal ideation, suicide, or self-harm content to the user" and issue crisis service provider referral notifications when needed.

[58] Brown et al. 2024; Edelson et al. 2025

[59] Wei and Tyson 2024; DiResta and Goldstein 2024

be both selected and created by AI.[60] This raises acute challenges for democratic societies, particularly regarding electoral integrity. AI systems can now produce and circulate synthetic political content,[61] impersonations,[62] and deepfakes at unprecedented speed. Ensuring the transparency of these systems and the reliability of content they prioritize and generate must be a priority for democratic societies. In order to ensure information ecosystem integrity, the government should consider:

2.1. AI Identification and Provenance Disclosure. Citizens should have the right to know when they are interacting with or consuming content produced by an AI system. This requires a multi-layered identification regime that mandates clear disclosure in both human and machine-readable formats. At a minimum, a re-introduced and amended *Consumer Privacy Protection Act* should include: 2.1.1) visible labelling;[63] 2.1.2) provenance metadata and digital watermarking;[64] and, 2.1.3) source transparency requirements, including training data.[65]

2.2 Monitoring and Data Sharing with Researchers and Civil Society. Addressing the power asymmetry between private platforms and the public, and ensuring that researchers, journalists, and civil society organizations can study the effects of AI systems, requires statutory mechanisms given to the Digital Safety Commission for data access, transparency, and independent oversight. At a minimum, this includes: 2.2.1) mandated data inventories of AI system inputs and outputs;[66] 2.2.2) secure researcher access frameworks for data on social media and consumer chatbot use and algorithmic design, facilitated by an independent monitoring or observatory body;[67] and 2.2.3) confidentiality-safe data enclaves for public-interest research.[68]

---

[60] Kreps and Kriner 2023; Birrer 2024

[61] Examples in Canada include the Kirkland Lake Bot Incident and the emergence of AI-generated ads masquerading as legitimate news sources during the 2025 Federal Election.

[62] Leong et al. 2024; Lyngaas 2025

[63] California's Senate Bill 243 requires that conversational AI systems issue periodic, in-context notifications to remind users that they are interacting with an automated agent, with heightened requirements for mental health and companion chatbots; South Korea's Artificial Intelligence (AI) Basic Act requires labelling or generative AI content.

[64] The EU's AI Act (article 50) establishes mandatory disclosure when users interact with an AI system and requires providers of generative AI to implement technical measures such as watermarking or metadata tagging that signal synthetic content.

[65] This can be achieved through the Consumer Privacy Protection Act or through the transparency provision of the Online Harms Act should AI systems be brought into scope. Other examples of legislation with AI transparency provisions include Australia's Data Availability and Transparency Act, the EU's AI Act, and Japan's Act on Improving and Fairness of Digital Platforms.

[66] The EU's AI Act (article 10) mandates developers of high-risk systems must maintain detailed records and evaluations of training and testing datasets.

[67] This can be achieved through Sections 73-74 of Bill C-63, which outlines access to electronic data by accredited researchers.

[68] This can be achieved by amending Part 1, Sections 73-74 of Bill C-63 or introducing a stand-alone Act to allow persons engaged in public interest research to request access to inventories of electronic data that are included in digital safety plans. Other examples of legislation with similar provisions include that EU AI Act's Article 57, which establishes "AI regulatory sandboxes" for controlled testing of AI and the EU's Digital Services Act Article 40 which obligates very large online platforms to provide vetted researchers with access to platform data for systemic-risk research under secure conditions.

2.3 Support for Reliable Information Production. As AI-generated content saturates digital spaces,[69] supply-side measures are essential to preserve and promote the production of reliable, evidence-based information in an increasingly AI mediated and created information ecosystem. Policies in this domain are less developed, however, the government could: 2.3.1) consider adapting existing journalistic support mechanism to, and develop new programs for, a broader range of journalistic content creators and reliable content generations forms;[70] 2.3.2) support new sovereign, decentralized infrastructure for public interest media; and, 2.3.3) actively engage in domestic and international efforts to transition the journalism sector to a new AI-driven mediated information ecosystem.[71]

Democratic Priority 3: Democratic Legitimacy

In a democratic society, citizens must have meaningful agency in determining the development and governance of the AI infrastructure that shapes their lives. Rebuilding democratic legitimacy in the age of AI therefore requires more than public consultation; it demands institutional pathways that are built for meaningful participation, agency and autonomy, and accountability. This includes mechanisms through which citizens can contest automated decisions,[72] assert control over their data,[73] and contribute to the governance of AI itself.[74] In order to ensure the democratic legitimacy of AI systems, the government should consider:

3.1 Data Portability, Interoperability, and Right to Deletion. Empowering citizens also means restoring their control over their personal data. In our current information economy, data mobility is not simply a matter of convenience, but is a structural determinant of citizens' autonomy.[75] Together, portability and interoperability provide the technical and legal architecture through which citizens can reclaim agency over their data[76] and reduce the concentration of informational power.[77] To do so, amendments to the *Consumer Privacy*

[69] Birrer 2024; Chen et al. 2025
[70] Such as the Local Journalism Initiative, the Online News Act and the Media Fund.
[71] Examples include: International Fund for Public Interest Media, Media Forward Fund, Public Media Bridge Fund.
[72] The EU's General Data Protection Regulation Article 22 grants individuals the right "not to be subject to a decision based solely on automated processing", and allows them to request human review and contest decisions. The EU's AI Act Article 86 further allows individuals affected by AI systems to lodge complaints with national authorities and receive information about how decisions were made.
[73] This can be accomplished by applying sections 62, 63, and 72 of Bill C-27, which requires organizations to disclose the use of individual data in automated decision systems, provide explanations of decisions with "significant impact" on individuals, and "disclose the personal information that it has collected from the individual to an organization designated by the individual" upon request.
[74] Examples of this include regular citizen assemblies on AI policy and the creation of public transparency registers to allow civil society to monitor incidents and risks.
[75] The EU's Digital Markets Act Article 6(64) explains that a "lack of interoperability allows gatekeepers that provide number-independent interpersonal communications services to benefit from strong network effects, which contributes to the weakening of contestability."
[76] Walker and Milne 2024; Crabtree and Mortier 2016
[77] Mantelero 2012; Rahman 2018; Zuboff 2015

Protection Act should include: 3.1.1) interoperable data standards;[78] 3.1.2) user-initiated data mobility rights including social graph data;[79] 3.1.3) public disclosure of interoperability specifications,[80] and, 1.1.4) a mandated right to deletion for users.[81]

3.2 Recourse Mechanisms and User Empowerment Support. Citizens must have clear and accessible avenues for redress when AI systems cause or exacerbate individual and collective harms. Establishing recourse mechanisms ensures procedural fairness by enabling users to challenge automated decisions, demand explanation, and seek remedies. The amended and re-introduced *Online Harms Act* should include: 3.2.1) a statutory AI and Digital Safety Ombudsperson[82] within the Digital Safety Commission, who is empowered to receive complaints, investigate harms, and provide users with informational resources, including literacy materials. The amended Consumer Privacy Protection Act should include: 3.2.2) mandatory human review of consequential automated decisions;[83] and, 3.2.3) public reporting obligations.[84]

3.3 Mandated Consultation Mechanisms. This will institutionalize democratic input into the design and oversight of AI policy. This could include: 3.3.1) standing citizens' assemblies or deliberative panels, composed of demographically representative participants;[85] 3.3.2) structured partnerships between civil society organizations and academic researchers to promote co-governance and value-chain governance;[86] and 3.3.3) mandated and regularly held advisory councils, such as with youth and Indigenous stakeholders.[87]

---

[78] The EU Digital Markets Act Article 6 mandates that gatekeeper operating systems provide "effective interoperability for third party services," and in all cases, "the gatekeeper and the requesting provider should ensure that interoperability does not undermine a high level of security and data protection in line with their obligations."
[79] This can be accomplished by applying and expanding section 72 of the CPPA in Bill C-27, which grants individuals the right to request an organization to disclose their data to another organization.
[80] An example of this includes the EU's Digital Markets Act Article 7, which requires companies to allow "reasonable requests for interoperability" by providing technical interfaces and relevant information required to interoperate.
[81] The "right to erasure" originates in the EU's General Data Protection Regulation Article 17. This grants data subjects the right to request the prompt deletion of personal data held about them by a business organization.
[82] This can be accomplished by applying and expanding the rights and duties afforded to the Digital Safety Ombudsperson proposed in Bill C-63, Sections 10-12.
[83] An example of this includes the EU's AI Act Article 14, which requires that high-risk AI systems be designed and developed in such a way that "they can be effectively overseen by natural persons,"
[84] This can be accomplished by applying and expanding section 62 of Bill C-27, which requires organizations to publicly disclose their data collection policies and account how automated decision systems are used for significant impact decisions, and section 62 of the Online Harms Act in Bill C-63, which requires operators to publish a digital safety plan online.
[85] Examples of these assemblies include Taiwan's standing Alignment Assemblies, The Centre for Media, Technology and Democracy's Youth Assembly on Digital Rights and Safety, and Germany's Artificial Intelligence and Citizens Councils.
[86] The United States has relied primarily on soft law and voluntary frameworks for AI governance, including NIST's AI Risk Management Framework (2023) and the White House's Blueprint for an AI Bill of Rights (2022), both which promote co-governance through extensive multi-stakeholder consultation.
[87] Examples of these councils include the IPC's Youth Advisory Council, The Digital Youth Advisory Committee, the OECD's Youthwise, and the Global Indigenous Data Alliance.