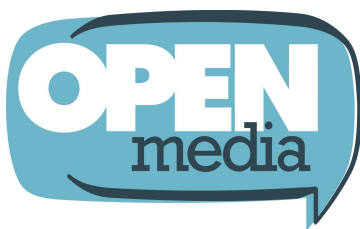




What Canadians Want from a Modernized Privacy Act

Key findings from OpenMedia's 2026 community survey

July 2026



OpenMedia is a grassroots community of 230,000 people in Canada that work together for an open, accessible and surveillance-free Internet. We work as a civic engagement platform that educates, engages, and empowers Internet users to advance democracy and digital rights across North America.

For more information, visit openmedia.org.

You can also find us on these social media platforms.

Bluesky | [@openmedia.org](https://bsky.app/@openmedia.org)

Mastodon | [@OpenMediaOrg](https://mastodon.social/@OpenMediaOrg)

Instagram | [@openmediaorg](https://www.instagram.com/openmediaorg)

LinkedIn | [OpenMedia.org](https://www.linkedin.com/company/OpenMedia.org)

Our Team

Matt Hatfield | Executive Director

Jenna Fung | Policy Engagement Manager

Table of Contents

Background	2
About the survey	3
What Canadians actually want	4
On data sharing between departments.	4
On AI decision-making.	4
On accountability.	4
Concerns behind the concerns	5
Digital sovereignty.	5
Government reliance on US digital services.	5
Key findings	6
Deep distrust of government is based on past systemic failures.	6
Data minimization and privacy by design are necessary.	7
Transparency and meaningful consent are top trust-builders.	9
Being informed isn't the same as being in control.	10
People reject/wish to heavily restrict AI in government.	11
Ongoing monitoring matters; self-oversight is not accountability.	13
Real accountability requires personal consequences.	14
Data sovereignty, but no backdoors and mass surveillance.	15
Political parties must not be exempt from privacy law	17
APPENDIX A: The Original Survey as Presented to Our Community	19
APPENDIX B: A Summary of the Survey Result	21

Background

Canada's [Privacy Act](#) hasn't had a meaningful update since the legislation was first enacted in 1983. At that time, government records were still stored on paper. The Internet hasn't gotten popular yet. There were no smartphones, no social media, and no AI hype. Fast forward to today, the amount of data the federal departments collect about Canadians has grown enormously. And so have the tools used to analyze it, share it, and act on it.

On April 2, 2026, the Treasury Board of Canada Secretariat announced a new formal [review of the Privacy Act](#). Along with the announcement, the government released a policy paper outlining [23 policy proposals](#) that are described as being about:

- Enabling better, more integrated services for Canadians;
- Strengthening privacy protections for the digital age;
- Updating the rules and oversight of the federal privacy system.

Specific proposals include formally recognizing privacy as a fundamental right in the Act, embed Indigenous data sovereignty directly into the Act, and give the Privacy Commissioner strengthened powers to hold departments accountable. There's also a proposal to establish a mandatory five-year review of the Privacy Act. Some of the proposals are genuinely promising, and reflect demands shared by [more than 4,000](#) OpenMedia community members in the previous consultation in [2021](#).

Unlike [past consultations](#), which focused on privacy principles in plain terms, the 2026 review takes what experts are calling a "[pragmatic](#)" approach. It combines discussions of privacy law with discussions of data infrastructure — the technical systems that determine how government data is actually built, stored, and shared. The result is a consultation that often requires the kind of specialist knowledge most Canadians simply don't have to engage with seriously.

About the survey

The 2026 review covers important issues that Canadians do have strong opinions on, including data sharing, AI accountability and establishing legal requirements with real consequences for ordinary Canadians' privacy rights. To empower a broad range of Canadians outside the policy world to engage with the review meaningfully, we went through all 23 current proposals and our past community engagement, and launched a 15-question [community survey](#) for all Canadians to share their preferences and values through. We gathered input for the survey from April 28 to June 15, 2026.

Our survey covers the issues that matter most to ordinary Canadians:

- How much do you trust the government with your data?
- What should govern how your data is shared?
- What rights should you have when AI is used to make decisions about you?
- What real accountability should look like when things go wrong?

We surveyed **4,688 community members** across Canada to understand what Canadians want from a modernized Act. We also gave every respondent the opportunity to provide a direct comment on what their answers meant, and what the survey did not touch on that they wanted our government to hear. The findings are consistent and striking.

* Trust is the central problem.

Only 7% of respondents mostly or fully trust the government to handle their personal data responsibly. Seventy percent have little to no trust at all. That distrust is not necessarily rooted in bad personal service experiences, but in structural problems people have seen repeatedly occur when government handles data. These include data being shared without people's knowledge (85.6%), a lack of transparency about how data is used (85.4%), concern about AI being used to make decisions about people (80.5%), and repeated data breaches (79.9%).

The community's asks are equally clear:

 **Meaningful consent** — Canadians want to know when their data is shared between institutions, and have a real ongoing say in how it's used.

 **Data minimization with technical safeguards** — Canadians believe only data that is strictly necessary should be collected and shared, protected by strong security controls throughout.

 **Real data ownership with independent oversight** — Canadians want personal control over what government holds about them, backed by independent audits that sit outside the institutions that directly handle that data.

What Canadians actually want

The survey didn't just surface Canadians' concerns about governments' practices. It surfaced a fairly detailed policy wish list.

1 On data sharing between departments.

Canadians want meaningful consent before their data moves (88.8%), strict limits on what's shared and why (88.7%), data minimization so only what's necessary gets shared (84.6%), and effective technical safeguards during transfer (86.2%).

The right to access your own data was the single highest-rated ask in the entire survey, at 96.9%. How? People want a personal portal where they can see exactly what's happening with their information (84.6%), the right to be notified when their data is shared (roughly 4 in 5 respondents), and independent audits proving the system works as promised (81.7%).

2 On AI decision-making.

When an AI system makes a decision about someone's eligibility, screening, and service access, 90.5% want a full explanation of how that decision was reached. 87.7% want a universal right to human review, and judicial recourse if something goes wrong (86.5%). Only 23.6%, the lowest result anywhere in the survey, think a system-level AI certification alone is sufficient oversight.

A significant portion of open-comment respondents went further, calling for AI to be excluded from government decision-making entirely. This puts the government's aggressive AI adoption strategy on a direct collision course with a large segment of the population it serves. The majority demanded transparency about when AI is used, and a human ultimately accountable for every consequential decision.

3 On accountability.

Too often, government is found to have violated the law, whether negligently or intentionally, and no serious consequences follow for those responsible. When it comes to privacy, Canadians want consequences with real teeth. Canadians want mandatory correction plans independently monitored (92.4%), criminal liability for serious and willful violations (88.6%), and personal consequences for the responsible officials (85%). On enforcement, 83.4% want oversight vested in a body genuinely independent of government. Only 3.2% want it kept inside the Treasury Board.

Concerns behind the concerns

In open survey comments and in our community townhall — Media Riff-Raff June 2026 Edition, where we presented our survey result — two additional themes we did not ask about in the questionnaire emerged repeatedly.

1 Digital sovereignty.

Community members raised, without prompting, the question of where Canadian data is physically housed, and who can access it under foreign laws like the US CLOUD Act. For many, encryption alone isn't a sufficient answer when the underlying infrastructure is owned or operated outside Canada. The ask was direct: sensitive Canadian data should be hosted and governed on Canadian soil.

2 Government reliance on US digital services.

Closely related, respondents raised concerns that essential public services shouldn't require Canadians to use American platforms to access them — and should be usable on open source or Canadian platforms, and even in analog formats, without depending on proprietary foreign ecosystems.

Both themes point to a gap in how the current policy conversation is framing the problem, and both are reflected in OpenMedia's formal submission to the Treasury Board of Canada Secretariat's 2026 review of the Privacy Act.

The detailed findings that follow explore each of these threads alongside the full survey data, community quotes, and the policy recommendations we are bringing forward inspired by 4,688 Canadians who responded.

Key findings

Distrust government with data	Data shared without knowledge	Want consent before sharing	Uncomfortable with data sharing among governmental departments	Want full AI explainability	Want mandatory correction
69.9%	85.6%	88.8%	68.3%	90.5%	92.4%
No trust or very little trust (Q1)	Shapes their distrust (Q2)	Top trust-builder (Q3)	Uncomfortable or very (Q4)	Highest AI rights pick (Q7)	Top breach consequence (Q12)

1 Deep distrust of government is based on past systemic failures.

Distrust is broad and systemic, which means modest service improvements alone will not address it. **Structural reform is what is demanded.**

When Canadians are asked *How much do you trust the federal government to handle your personal information responsibly?* (Q1), only 6.9% mostly or fully trust the government with their data. Critically, when we asked *What most shapes your level of trust (or distrust) in how the government handles your data?* (Q2), it reveals the distrust is driven by **structural concerns, not by bad personal service experiences**, which scored far lower at just 37%.

- Lack of transparency about what data is collected and how it's used (85.4%)
- Data shared without knowledge (85.6%)
- Use of AI to make decisions about people (80.6%)
- Data breaches and security incidents (80%)

"I really am not comfortable with all this, the government has had too many breaches in the past."

– A. Schultz, Alberta

"The current government's recent pivot to forcing AI into everything is what makes me distrustful of the government holding my data."

– J. Fraser, Ontario

"I believe that good governance requires the collection of data about citizens, and the trust that that data will be used in a responsible manner. Unfortunately, due to the loss of my own data in the Alberta elector list leak, and the federal government's apparent intent to use AI and also to share my

data with foreign governments, I have lost that trust. I require that trust to be rebuilt as the foundation for good governance."

– Mark R-H, Alberta

"Personally, I don't think the government should have any data about me without my specific authorization, including the AI collection and use of said data. The government cannot be trusted and never seems to be held accountable for any of their actions."

– G. McLeod, Ontario

POLICY RECOMMENDATIONS

- Recognize privacy as a fundamental right in the Act's purpose clause/preamble (government proposal 12), establishing it as a core democratic value rather than a procedural afterthought.
- Address structural issues that erode trust — including undisclosed data sharing, opaque collection, AI-driven decisions, and breach exposure — before expanding integrated data services, not alongside them.
- Ensure external, independent oversight (recommendation 6) and meaningful consequences for those who fail to protect the public's privacy (recommendation 7), as our community.
- Address gaps in privacy law domestically (recommendation 9), and ensure that foreign companies and government not subject to Canadian privacy law do not receive sensitive Canadian data (recommendation 8).

2 Data minimization and privacy by design are necessary.

When we asked Canadians what should be required if *a government department were to share your personal data with another department or level of government*, 84.6% selected **data minimization** (a strict limit on what data is shared and for what purpose); and 82.6% said **privacy by design**.

In open comments, **some community members argue for non-collection** (e.g. via edge computing) **as the best protection for privacy**. Others call for **automatic deletion timelines** and **privacy-by-design as a legal default**. This aligns with our community's unanimous support for **right to deletion**, where 92.9% expressed in Q14 when we asked them what rights they believe the Privacy Act should guarantee.

"In general, principles should be to keep the minimum amount of personally identifying data and/or data linked to individuals as possible... Data should be binned and anonymized whenever specific records are not required, particularly when data is being transmitted between different systems... The best protection for privacy is not collecting or storing unnecessary personal data in the first place"

– T. Armstrong, British Columbia

"Finally, the Act should mandate security-by-design standards drawn from established industry practice: end-to-end encryption for sensitive data in transit and at rest, mandatory breach-detection and response timelines, zero-trust access controls so employees access only what they need, and regular independent penetration testing of systems that hold personal data. These aren't novel ideas - they're table stakes in responsible tech - and there's no reason the government should be held to a lower bar."

– O. Voloshchenko, Ontario

"I think that wherever possible, data on me should only be stored as long as necessary, and once that window of necessity has passed it is promptly deleted. No matter how much I may trust the present administration, I cannot necessarily trust the next one, or the one after that."

– K. Redshaw, Ontario

"The more data in the database, the more likely it will be of interest to hackers, data thieves. This happens all the time. All the privacy legislation in the world isn't going to help if the system gets breached. Limiting database size, limiting what can be collected and stored, also protects our privacy. "

– J. Barnard, Alberta

POLICY RECOMMENDATIONS

- Adopt a peer-to-peer/federated data-sharing architecture (e.g. Estonia's X-Road model) so systems exchange "answers," not full data copies.
- Make privacy-by-design a legal default, and include automatic deletion timelines once data has served its purpose. — (government proposal 13 & 17).

3 Transparency and meaningful consent are top trust-builders.

We asked Canadians *what would increase your trust in how the federal government handles your personal data?* (Q3). The results show that **consent** (88.8%) and **transparency** (88.7%) are the **top trust-builders**. Some community members told us in the open comments what those words mean in practice: consent buried in fine print is not consent; a policy nobody can practically read is not transparency. Some spoke to the importance of actual choices as a precondition for consent; consent given as a precondition to practically access core services is not true consent. The framing aligns with the stand of 88.6% who said plain-language disclosure should be required when a government program collects or uses our personal data in Q11.

"Canadians should not have to fight to understand how their personal information is being collected, used, shared, stored, or analyzed by government systems"

– T. Parr, Ontario

"I would like full disclosure on what the government actually decides on all choices to do with my data and choices made for me by them. And not government speak mumbo jumbo wording, plain straight talk and language."

– A. Neiffer, Alberta

"CONSENT: in the current environment, we are often requested to read privacy, terms and conditions, and tick a box giving our consent. However, contrary to what this might appear, it is really not about protecting the citizen or client or getting their real consent. It's about protecting the government or the company. If something happens, they can turn around and say "Well, you ticked the consent box". In the end, if we want a service, be it from the government or from the private world, we have to give our consent, so it is a false, forced "consent". Furthermore, companies, more so than government, cover their back ends by making their privacy terms and conditions extremely long and difficult to understand which again is in order to protect themselves and force the citizen or client to tick the box to something they don't understand, but do so hoping that they won't be the person who gets harmed by the system. "

– C. Balaberda, Ontario

"The contemporary idea that the presence of a technology is somehow consent to its use is both pervasive and rotten. Our government MUST put people ahead of technology, and rights ahead of efficiency. It is better for the government to do the right thing slowly, than the wrong thing quickly. When information is exposed, it can not be taken back. The only time to get it right is the first time. "

– G. Jans, British Columbia

"The government should not coerce citizens into using digital services. No penalties should be imposed on those who choose traditional methods of communication or paper-based tax filing — participation in digital systems must remain a matter of personal choice, not obligation. "

– A. Kottova, British Columbia

POLICY RECOMMENDATIONS

- Ban blanket consent provision models to access fundamental services ("by using this service you agree to data sharing across government"); require consent to be specific, in most circumstances revocable, and tied to individual data categories.
- Make explanations and plain-language notices a default right, not something citizens must actively request (government proposal 5 & 6).
- Guarantee that there will always be a non-digital means of accessing essential government services.

4 Being informed isn't the same as being in control.

Question 6, *"if your data is shared or reused by the government, what tools or mechanisms should exist to give you visibility and control over your personal data held by the government?"*, shows a **meaningful gap between mechanisms for visibility and autonomy**: a personal portal (84.6%) and independent audits (81.7%) score far higher than a public registry (62%) — the lowest Q6 result.

People want **control over their own data**, and **independent expert verification that it is being handled as they are told**, more than generalized public transparency. This is reinforced in Q14, where a personal **right to access** (96.9%) and **right to correction** (96.4%) are the **two highest-scoring rights in the entire survey** — higher even than breach notice or human review. Our open comments strongly echo the framing of information self-determination and data ownership.

"I want the government to do the right thing and do it in the open. The government shouldn't be a black box. As an individual I must be able to see, review and correct the data held about me. Right now I have very little idea what information the government has associated with my name. "

– C. Prokopanko, Manitoba

"We should be able to monitor all information regarding ourselves..."

– M.C. Ducharme, Quebec

"Take a look at how different European jurisdictions work with the concept of open government, where an individual is always in control of their data. Estonia used to be a leader in this, but I don't know if that's still the case."

– T. Blampied, Ontario

"Individuals must have the right to know the source of any data used about them, and the right to correct errors BEFORE decisions are made."

– E. Allott, British Columbia

"Citizens should have access to a public registry listing all private tech companies offering services to the Government... Canadians should also be informed of all countries the Gov of Canada is sharing our data with"

– C. Perlain, Quebec

POLICY RECOMMENDATIONS

- Build a dedicated, personal data portal accessible to every Canadian that gives visibility into the data government departments hold them— distinct from and complementary to the centralized registry (government proposal 4), so people can see real-time, event-level access to their own data.
- Treat the registry as documenting institutional intent, not verified outcome; pair it with independent audits confirming actual compliance.
- Explore a zero-trust, single source retention approach to citizen data that minimizes multiple sources of potential vulnerable personal information within government.

5 People reject/wish to heavily restrict AI in government.

A strong plurality of Canadians are extremely skeptical of AI. **Only 23.6% chose system-level AI certification as sufficient** when an automated system makes a decision that affects them in Q8 (the single lowest result in the entire survey); while **majorities chose every other AI rights option**, e.g. Universal right to human review (87.7%), Judicial recourse (86.5%), and Rights-based threshold (80.1%). **Open comments go further**, with many **calling for outright bans** on generative AI and LLMs in decision-making. Strong objections to the use of AI in government for decision making was the single most common write-in comment in our survey, with many calling for tight limits on use, and some calling for a total moratorium.

"I wish that AI was not used in governmental decisions. I understand it may speed along certain processes, but AI as a whole is currently extremely faulty. It breaks a lot of my trust in the government to know AI is being used to handle decisions about my privacy and decisions that affect me personally."

– P. Reuben, Alberta

"AI should legally not be allowed to make any decisions about a person."

– T. Turner, Nova Scotia

"A machine can never be held accountable, therefore a computer must never make a management decision. IBM Training manual from 1979. I believe this applies even more strongly today than it did back then."

– M. Royal, Quebec

"I think we should have the right to refuse our data being fed into AI in the first place. I oppose the government giving any of my data to AI without my consent (and in general). I am a software developer; I know AI can be useful for some things. There are some things that are too important to be trusted at all to a system full of bias and hallucination—to me that includes anything our elected government does. "

– A. Méthot, Alberta

"In most industrialized countries, governments are taking steps to regulate artificial intelligence to limit or prevent its many negative effects and results (one of these being violation of privacy). Instead, Canada's government appears to be going all-in on adopting AI and using it for every possible purpose and function. Nothing good can come of such an approach, and it has to change. To the extent that AI is adopted at all by the government, its functions must be regulated, limited, and compartmentalized to prevent its negative effects and the degradation of public services, and to ensure that human labour and jobs are not replaced by advanced technologies."

– E. Janzen, Quebec

"AI can and could be used in certain circumstances and situations, but each case needs to be publicly announced or shown as beneficial before implementation. AI usage needs to be declared upfront and only with consent of users or those affected by it. AI physical data centres must have environmental impact assessments done long before any are built."

– E. Jilec, British Columbia

POLICY RECOMMENDATIONS

- Make providing ADS notice and explanation a guaranteed, linked sequence — not two disconnected, request-based provisions (government proposal 5 & 6).
- Establish human review of any automated decision as a guaranteed right (not institutional discretion) and provide an explicit path to judicial appeal for ADS decisions

that may impinge on fundamental rights (government proposal 8).

- Define the scope of "automated decision system" clearly in the Act with to prevent inconsistent application across institutions.
- Require proof of independent environmental review and best practices for AI data centres contracted, built, or subsidized by Canada's government.

6 Ongoing monitoring matters; self-oversight is not accountability.

Many respondents expressed trust in the government's good intentions; but good intentions are not enough. Instead, they asked for **continuous, living accountability**, and **independent verification** of how our government is managing our data. In Q11, "*When a government program collects or uses your personal data, what should be required before it goes ahead?*", **ongoing monitoring** after launch (86.2%), **Mandatory definition scope** (86.2%) – the law should spell out exactly what a mandatory privacy impact assessment must cover, not leave it to government regulatory policy or individual departments.

Government programs evolve after launch; effective privacy protections can erode or functionally disappear. For this reason, **people want oversight that keeps pace** (77.82%). Open comments reinforce this by calling for regular reviews, annual audits, and laws that update with technology rather than falling decades behind.

In Q9, "*How should the government be held accountable for the AI systems it uses?*", **independent audit** (87.4%) and **radical transparency** (85.5%) score strongly, while relying on open source standards (65.9%) or parliamentary oversight (66%) score notably lower — about 20 percentage points behind. This mirrors Q10, "*Who should be responsible for making sure the federal government follows privacy law?*", where **only 6.8% chose parliamentary oversight as the preferred accountability body**.

A clear picture emerges: respondents want **oversight that is genuinely independent of government** — not just outside the specific department being reviewed, but **outside the system that can be leaned on by the government in power entirely**.

"While I doubt the current government would do anything nefarious with my data, the same cannot be said of a future government."

– B. Bedard, Quebec

"Transparency and accountability throughout with oversight by strong independent bodies not tied to a party nor government in office."

– P. Berrevoets, British Columbia

"All oversight must be insulated from political interference and manipulation — Political party influence is the enemy!"

– D. Bunn, Nova Scotia

"Regulations within the law that allow for regular (annual or semi-annual) reviews and amendments that allow for continuous updates to keep pace with changing realities."

– P. Tarnowski, British Columbia

POLICY RECOMMENDATIONS

- Define the requirements of Privacy Impact Assessments content in statute, not policy, and require independent review of mandatory assessments outside the originating department (government proposal 3), ideally by the OPC.
- Mandate continuous, post-launch monitoring and/or regular reviews, rather than one-time, pre-launch approval.
- Vest oversight in a body genuinely independent of government — supporting either a new independent tribunal or a strengthened Privacy Commissioner (government proposal 19 & 20).

7 Real accountability requires personal consequences.

Powerful institutions struggle to hold themselves meaningfully to account. Yet providing some measure of clear responsibility and accountability for serious government failures was one of the most popular asks of our respondents. When we asked *When a government department breaks privacy law, what should happen?* (Q12), 92.4% of respondents demand a legally binding requirement to correct what went wrong, monitored for acceptability by an independent body, and 88.6% want **criminal liability in serious or willful cases**. A further 85% of respondents want **personal consequences for senior officials** who could reasonably have prevented the error (e.g. demotion, suspension or removal from office).

The much lower segment of respondents 58.9% who chose departmental fines (the lowest Q12 option by a significant margin) reflects a widespread objection that frequently appeared in our open comments: **fining a department is fining the taxpayer, not actually penalizing the error**. Meanwhile 76.9% in Q12 and 84.9% in Q13 want compensation paid directly to affected individuals, signalling these should be treated as entirely separate mechanisms.

"Equally important, government departments and employees who knowingly misuse personal data, exceed their legal authority, or fail to safeguard sensitive information should face appropriate legal, administrative, and financial consequences. Without clear accountability mechanisms, privacy protections risk becoming little more than promises on paper."

– S. Kroyd, British Columbia

"Those who break the law MUST have serious consequences like hefty fines (not paid by taxpayers), prison time, exposure"

– D. Burgess, British Columbia

"I'd just like to emphasize that real punishments for departments and specific officials who bend or break the rules would be a very welcome change. Myself and the people in my community are beyond tired of slaps on the wrist and apologies for things that would likely land a normal person in very serious trouble. They shouldn't be immune to heavy fines or jail time just because they are elected officials and it shouldn't take moving mountains to impose these penalties."

– E. Jelkovic, Ontario

POLICY RECOMMENDATIONS

- Add a plain criminal liability provision for willful or seriously negligent violations of privacy rights by public officials.
- Provide external independent review of serious but not willful lapses to ensure there are real consequences (demotion, suspension, removal) for officials who preside over such errors.
- Direct compensation to affected individuals rather than issue departmental fines.

8 Data sovereignty, but no backdoors and mass surveillance.

An exceedingly popular write-in concern was fear that Canada is, or will, permit sensitive personal data to be accessed by domestic or foreign law enforcement. Many raise it independently in open comments, citing possible Canadian ratification of the **US CLOUD Act**, its impact on **US government access to the US tech platforms** we are overwhelmingly reliant on, and our slowness to adapt to a rapidly changing **geopolitical climate**. These comments fit with the strong desire for limited data collection, minimal data sharing, and the 86.2% who want zero trust **technical safeguards** (encryption and security controls that prevent unauthorized access during sharing) documented elsewhere in our survey. The need for Canada to exercise genuine digital sovereignty - keeping our most sensitive data on Canadian servers,

using domestic or open-source code we can fully control – was a frequent refrain in the open comments.

Another point we did not ask about in the structured questions was Bill C-22; but this was frequently named by name across many responses in open comments. The 85.6% who cite "data shared without my knowledge" as their top trust-shaper in Q2, "*What most shapes your level of trust (or distrust) in how the government handles your data?*", connects to Bill C-22's deficiencies directly: respondents experience backdoor legislation as exactly that — sharing without knowledge or consent.

"Ensure that ALL government data, including, but not limited to, those in the control of crown corporations, about the Canadian people is hosted on Canadian owned servers INSIDE the country, NOT hosted on servers owned by foreign citizens, businesses, companies or governments."

"Canadian data and AI systems need to be stored only in Canada and not accessible to outside powers or individuals."

– T. Browne, British Columbia

"To strengthen data oversight, accountability, and long-term resilience, all levels of Canadian government federal, provincial, and municipal, should adopt a coordinated policy prioritizing open-source, self-hosted software solutions over proprietary, foreign-controlled platforms. This shift would reduce vendor lock-in, keep sensitive public data within Canadian legal and technical jurisdiction, and ensure systems remain transparent, independently auditable, and adaptable to domestic priorities. By treating public digital infrastructure as critical national infrastructure, not a leased commodity. Canada can mitigate geopolitical and supply-chain risks, lower recurring licensing costs, and align with European jurisdictions that have successfully migrated public services away from dominant commercial vendors. A principled transition toward open, sovereign technology is not merely an IT procurement choice; it is a foundational step toward trustworthy, accountable, and autonomous governance."

– J. Powlesland, British Columbia

"Metadata is not trivial, and the Privacy Act reform cannot be separated from legislation like Bill C-22... The Privacy Act should explicitly establish that metadata receives the same protection as content, not less..."

– J. Geiger, Ontario

"When using AI or automated tools, be mindful of who processes the data and where. Considering the government handles very confidential data, instances of those tools and AI models / engines should be hosted by the government on government-owned-and-controlled servers (eg. not in the cloud, like Microsoft Azure, AWS or any other cloud provider). Third parties should only be involved in providing said tools and models, as well as the necessary technical documentation, for the government to be able to install, operate, maintain and audit on their own, without the need of going through said third parties."

– G. Stébenne, Quebec

"I am VERY concerned about who owns the servers where Canadian data is stored. If the "cloud" or "server" is owned by a non-Canadian company, such as the US and the Cloud Act, Canadian data is not safe. This is very dangerous for Canadians and for Canadian security. Canadian information should be safe from any foreign countries' laws on servers. I hope my not too techy way of writing is understandable for you."

– C. Viereck, Quebec

POLICY RECOMMENDATIONS

- Require public disclosure of which institutions store/process data outside Canada, moving foreign-storage and access decisions from internal risk judgment to a transparent, auditable practice (government proposal 9).
- Steadily reduce dependence on proprietary foreign platforms (e.g. Microsoft) in the operation and access to government services; support open, non-proprietary systems, and preserve analog/paper alternatives.
- Invest in physical network infrastructure that can better transmit Canadian data from one Canadian destination to another, reducing so-called 'boomerang' routing (Canada-to-Canada traffic routing through the U.S.).
- Abandon or heavily amend Part 2 of Bill C-22.

9 Political parties must not be exempt from privacy law

A final point that we did not ask about, but which was raised consistently and across apparent political leanings in our open comments, was the need to place federal political parties under meaningful, external privacy law, beyond the current requirement to follow their own policies. Respondents frame it as a **basic consistency argument**: if the law applies to government, **it must apply to parties that form government**. We recognize that this will not likely be solved by reforming the Privacy Act; but it is precisely Canada's public versus private sector privacy separation that has allowed this awkward and unusual privacy exception to come into being.

"I, personally, trust that the government and the public service want to do the right thing. What I don't trust are the political parties. Their access to my personal information should be severely restricted and misuse incur a penalty for the persons responsible."

– K. Kulak, British Columbia

"No longer permit political parties to be exempt from privacy laws regarding the collection, retention and distribution of personal and/or private information."

– G. Sheppy, Ontario

"Political parties should be subject to oversight and accountability in exactly the same ways as government departments."

– R. Cook, Ontario

"I have serious doubts about the government's ability and sincerity to protect the privacy rights of citizens, given they have exempted their political parties from abiding by the law like anyone else would have to."

– G. Fraser, British Columbia

POLICY RECOMMENDATIONS

- Extend the same privacy obligations, oversight, and accountability mechanisms that apply to commercial private entities to political parties and nonprofits, closing the current legal exemption.

APPENDIX A: The Original Survey as Presented to Our Community

OpenMedia Survey: Tell Ottawa How to Fix the Privacy Act

OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.



FIX PRIVACY ACT TOGETHER

Take our survey >>



OpenMedia Survey: Tell Ottawa How to Fix the Privacy Act

Canada's Privacy Act hasn't had a meaningful update in over four decades. In that time, the amount of data the government collects about you has grown enormously — and so have the tools used to analyze it, share it, and act on it, with little say from you.

That's finally about to change! The government just announced a review to the law that governs the privacy practices of 250+ government institutions, from the RCMP to Service Canada.¹

OpenMedia has been fighting for **real oversight, accountability, and transparency** in how the government handles your data for years.² **Now we need your voice to get these rules updates right!**

Take our survey before June 15, 2026 (Monday) and we'll bring your answers directly to the government.

Fill out the form below to get started.

⚠️ **Note: This form does not autosave.**

First Name*

Last Name*

Your Email*

Province*

Alberta ▾

Postal Code*

Note: Your name and comments may be included in our submission to the 2026 Privacy Act Review. Your contact info will remain private and will only be used to send you progress updates.

Section A: You and your data

Before we get into the specifics, we want to understand where you're starting from — how you feel about the way the federal government handles your personal data today.

1. How much do you trust the federal government to handle your personal information responsibly?

(Choose one answer)

No trust at all ▾

2. What most shapes your level of trust (or distrust) in how the government handles your data?

(Select all that apply)

- ☐ Government data breaches and security incidents.
- ☐ Government use of AI to make decisions about people.
- ☐ Lack of transparency about what data is collected and how it's used.
- ☐ My data being shared without my knowledge.
- ☐ Positive or negative experiences with government services.
- ☐ The operations of the federal Privacy Commissioner, the independent watchdog that investigates breaches of the Privacy Act.
- ☐ None of the above.

3. What would increase your trust in how the federal government handles your personal data?

(Select all that apply)

- ☐ Enforcement — stronger laws with real consequences when rules are broken.
- ☐ Transparency — easy visibility into what data is collected and how it's used
- ☐ Consent — my approval required before my data is collected or shared.
- ☐ Control — the ability to access, correct, or delete my data at any time.
- ☐ Independent oversight — a strengthened body outside the government overseeing data practices.
- ☐ Accountability — a proven track record of responsible behaviour over time.
- ☐ None of the above.

Section B: Data sharing across government

Sharing data across government departments can make public services faster and more seamless. But it also carries real risks: it can happen without your knowledge, and for purposes you never agreed to. We want to know what principles should guide how your data is shared, and how you should be kept informed.

4. How comfortable are you with federal government departments sharing your personal data with each other to improve public services?

(Choose one answer)

Very comfortable — I trust all branches of government to handle my data responsibly. ▾

5. If a government department were to share your personal data with another department or level of government, what should be required?

(Select all that apply)

- ☐ Consent — my explicit consent before any sharing takes place.
- ☐ Oversight — an independent body overseeing and approving the sharing.
- ☐ Purpose limitation — a clear public interest or direct benefit to me as the reason for sharing.
- ☐ Data minimization — a strict limit on what data is shared and for what purpose.
- ☐ Public record — a transparent log of what was shared, with whom, and why.
- ☐ Technical safeguards — encryption and security controls that prevent unauthorized access during sharing.
- ☐ Privacy by design — systems built from the ground up to minimize data exposure, not just policies added after the fact.
- ☐ Auditability — technical logs that allow independent verification of how data was accessed and used.
- ☐ None of the above.

6. If your data is shared or reused by the government, what tools or mechanisms should exist to give you visibility and control over your personal data held by the government?

(Select all that apply)

- ☐ Personal portal — a secure online space where I can see, download, correct errors, and track who has accessed my data
- ☐ Direct notification — a personal notice sent to me whenever my data is shared or accessed.
- ☐ Public registry — a publicly accessible log of government data holdings and sharing practices.
- ☐ Independent audits — regular reviews by a body outside government, with findings published publicly.
- ☐ None of the above.

Section C: AI and automated decisions

Federal departments already use AI and automated systems to make decisions that affect your life — from benefit eligibility to immigration applications.³ These systems may be faster and more consistent, but they can also reflect bias, make errors, hallucinate, and operate in ways that are hard to understand or challenge. We want to know what rights and accountability measures matter most to you when it comes to government use of AI.

7. What should you have the right to know when an AI or automated system is used to make a decision about you?

(Select all that apply)

- ☐ Full explainability — a plain-language explanation of what data was used and how the conclusion was reached.
- ☐ Meaningful transparency — a general summary of how the system works, without every technical detail.
- ☐ Impact assessment — a formal review of the privacy risks of the AI system, conducted before it's used and made publicly available.
- ☐ Disclosure — that AI was involved in the decision that affected me.
- ☐ Outcome only — what decision was reached is sufficient; how it was reached is an internal matter.
- ☐ None of the above.

8. When an automated system makes a decision that affects you, what should you be able to do about it?

(Select all that apply)

- ☐ Universal right to human review — the right to request a human review for any automated decision.
- ☐ Rights-based threshold — the right to human review when a decision affects my access to services, benefits, or rights.
- ☐ Judicial recourse — the right to challenge the decision in court, with access to all data and reasoning used.
- ☐ System-level assurance — if the AI system is independently certified as fair and accurate, no individual recourse should be necessary.
- ☐ None of the above.

9. How should the government be held accountable for the AI systems it uses?

(Select all that apply)

- ☐ Radical transparency — mandatory public disclosure of all AI systems in use, including their purpose, data sources, and bias testing results.
- ☐ Independent audit — regular audits by a body outside government, with findings published openly.
- ☐ Open source — government AI code should be publicly available for independent scrutiny.
- ☐ Parliamentary oversight — internal reviews by a dedicated committee, reported annually to Parliament.
- ☐ Technical accountability — mandatory logging and monitoring of AI decisions, accessible to oversight bodies.
- ☐ None of the above.

Section D: Oversight and accountability

When the government mishandles your personal data, who holds them to account — and what actually happens? Right now, oversight of federal privacy practices sits largely within the government itself, and the consequences for breaking the rules are limited. We want to understand what accountability looks like to you.

10. Who should be responsible for making sure the federal government follows privacy law?

(Choose one answer)

Strengthen the Privacy Commissioner — give them the power to investigate proactively, order change, and impose penalties. ▾

11. When a government program collects or uses your personal data, what should be required before it goes ahead?

(Select all that apply)

- ☐ Mandatory scope — the law should spell out exactly what a privacy impact assessment must cover, not leave it to government policy.
- ☐ Formal risk assessment — a privacy impact assessment conducted before the program launches, not after.
- ☐ Plain language disclosure — a public summary of the assessment in language anyone can understand.
- ☐ Independent review — the assessment reviewed and approved by a body outside the department.
- ☐ Ongoing monitoring — regular reviews after launch to catch new risks as the program evolves.
- ☐ None of the above.

12. When a government department breaks privacy law, what should happen?

(Select all that apply)

- ☐ Fines — significant financial penalties imposed on the department.
- ☐ Compensation — money paid directly to the people whose data was mishandled.
- ☐ Mandatory correction — a legally binding plan to fix what went wrong, monitored independently.
- ☐ Public disclosure — the government must openly explain what happened, who was affected, and what is being done about it.
- ☐ Personal consequences — senior officials responsible face professional sanctions, such as demotion, suspension or removal from office.
- ☐ Criminal liability — in serious or willful cases, responsible officials could face criminal charges and potential imprisonment.
- ☐ None of the above.

13. If your personal data is exposed as a result, what should you be entitled to?*

(Select all that apply)

- ☐ Timely notification — a direct personal notice within a fixed deadline, such as 72 hours.
- ☐ Full disclosure — a clear explanation of what data was exposed, how, and what risks it creates for me.
- ☐ Compensation — financial remedy paid directly to me for any harm caused.
- ☐ Right to appeal — the ability to challenge how my case was handled and seek further remedy independently.
- ☐ None of the above.

Section E: Your vision for the Privacy Act

After everything you've considered, tell us what you think should be guaranteed, and anything the government should hear that we haven't asked about yet.

14. Which of these rights do you feel should be guaranteed in law?

(Select all that apply)

- ☐ Right to access — see what data the government holds about me, in plain language.
- ☐ Right to correction — correct inaccurate information and know if it affected a decision about me.
- ☐ Right to explanation — know when AI was involved in a decision that affected me.
- ☐ Right to human review — request a human, not an algorithm, to review a decision about me.
- ☐ Right to breach notice — be notified promptly if my data is exposed.
- ☐ Right to legal remedy — challenge government data practices in court with real consequences.
- ☐ Right to deletion — request that data no longer needed about me be deleted.
- ☐ None of the above.

15. Is there anything else you'd like the government to consider in this reform, or anything you feel hasn't been covered?

Submit your response

This campaign is hosted by OpenMedia. We will protect your privacy, and keep you informed about this campaign and others. Find OpenMedia's privacy policy [here](#).

Want to learn more?

The government is proposing major changes to the Privacy Act. To see what this review means for your privacy and your rights, [check out our explainer](#).

Stay ahead of the changes.

Policy discussions move fast. Join our community to get the latest updates and ensure you won't miss a beat! [Sign up now](#).

Sources

- Government of Canada launches review of the Privacy Act — [Treasury Board of Canada Secretariat](#)
- Survey Results: The Privacy Act in Canada — [OpenMedia](#)
- AI Strategy for the Federal Public Service 2025-2027: Overview — [Government of Canada](#)

If you haven't taken action, [click here](#).

Press: Matt Hatfield | Phone: +1 (888) 441-2640 ext. 0 | press@openmedia.org

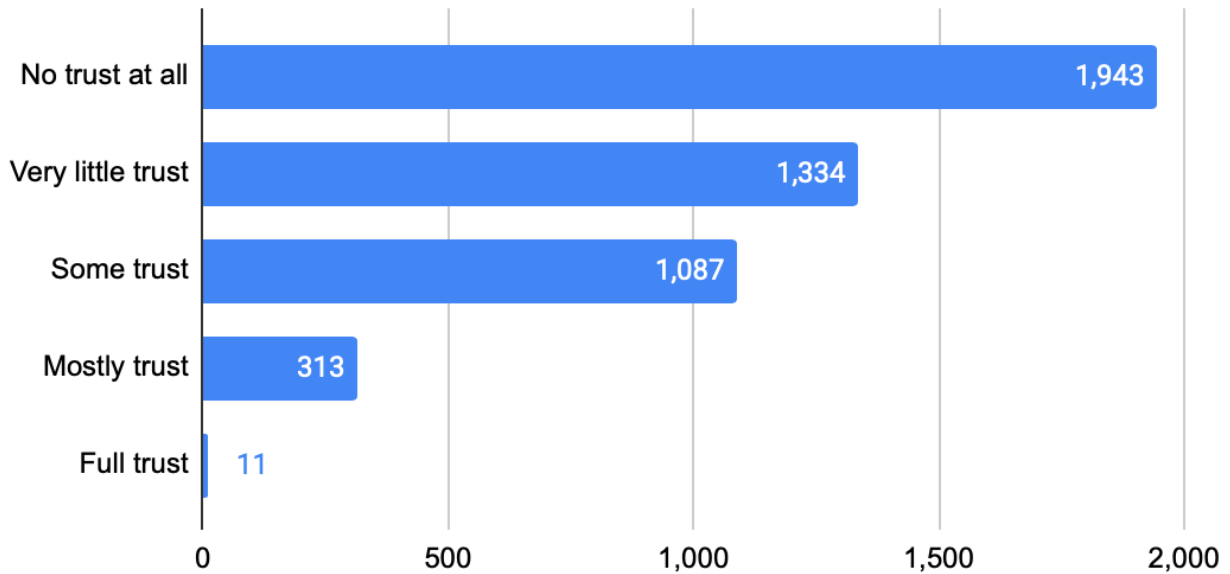
APPENDIX B: A Summary of the Survey Result

OpenMedia Survey: Tell Ottawa How to Fix the Privacy Act

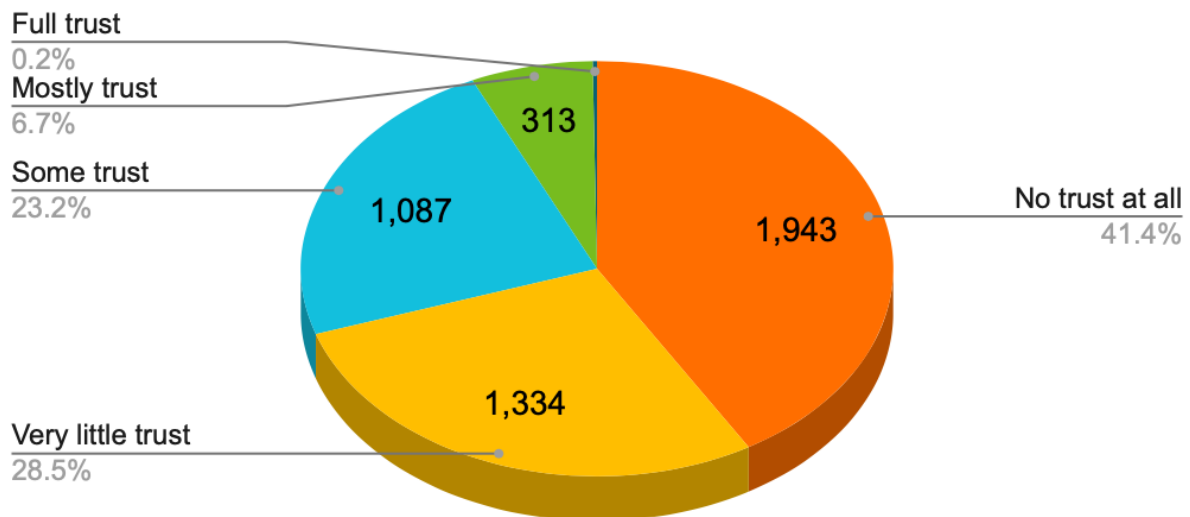
OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.



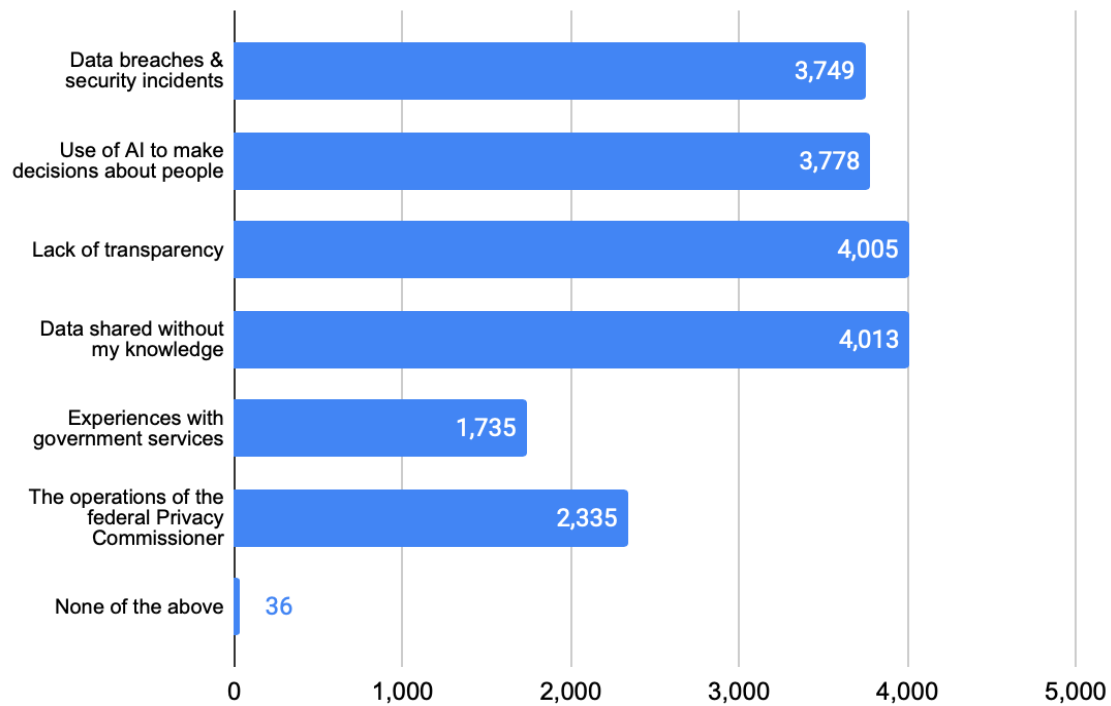
Q1. How much do you trust the federal government to handle your personal information responsibly?



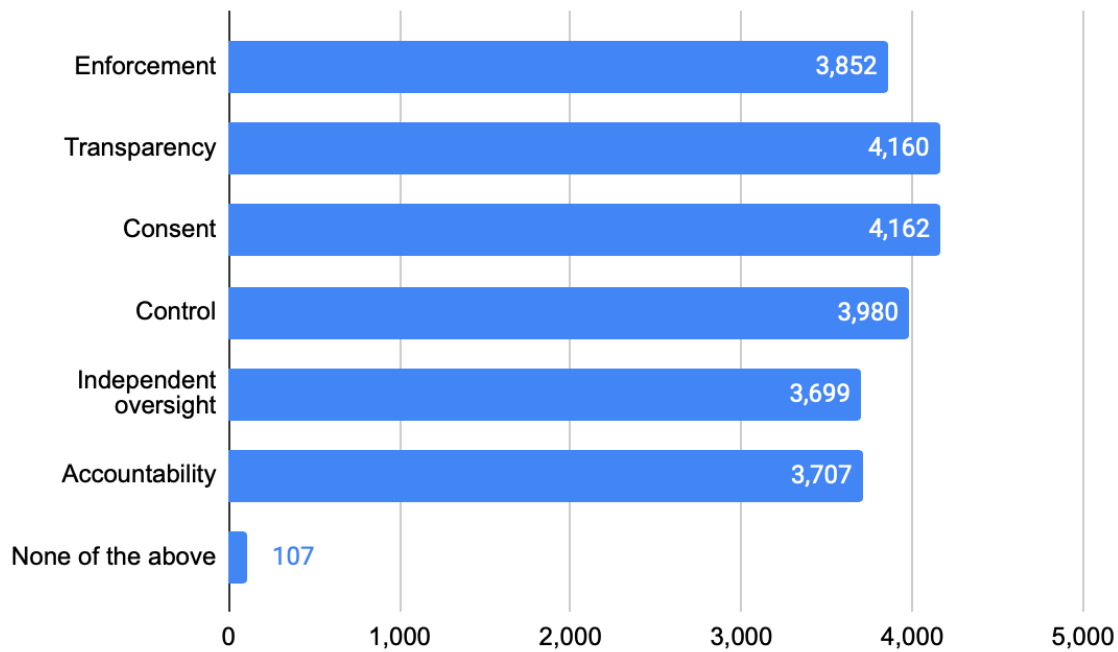
Q1. How much do you trust the federal government to handle your personal information responsibly?



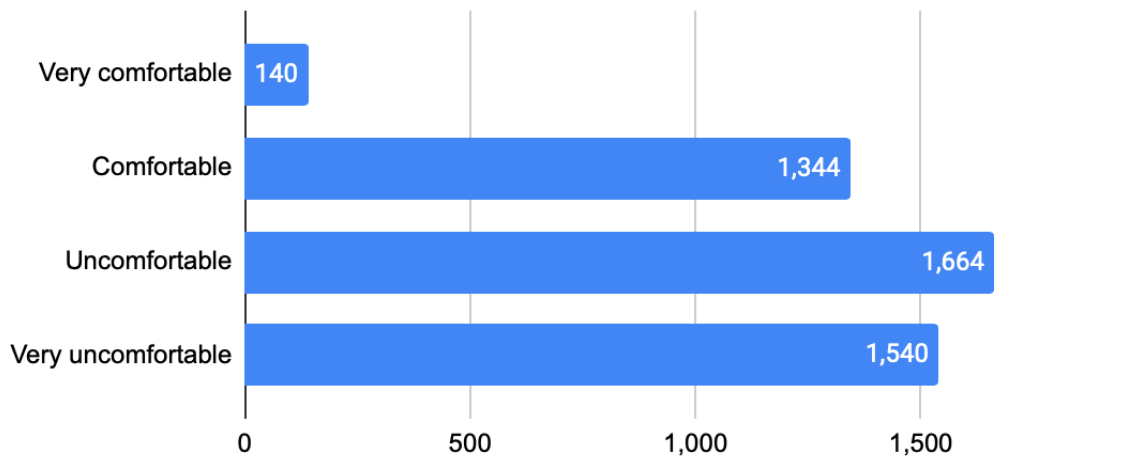
Q2. What most shapes your level of trust (or distrust) in how the government handles your data?



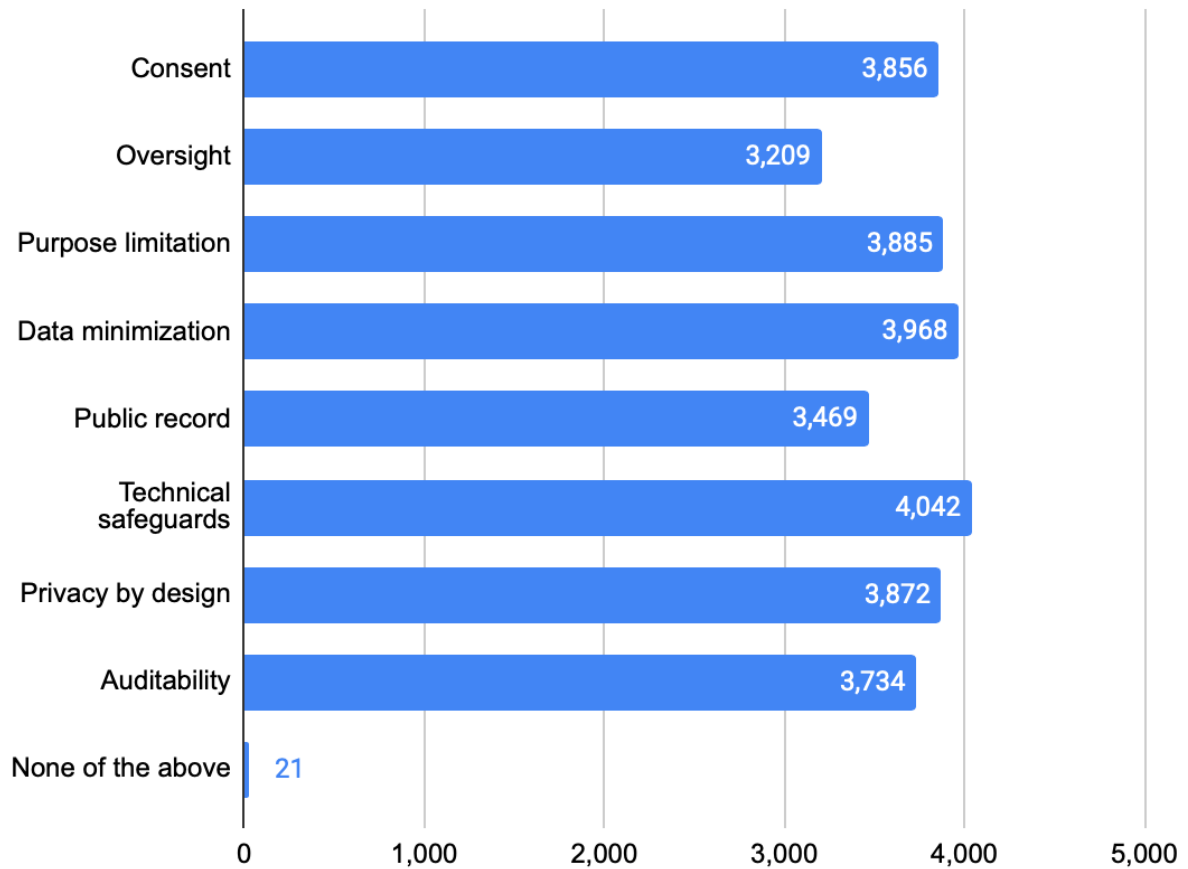
Q3. What would increase your trust in how the federal government handles your personal data?



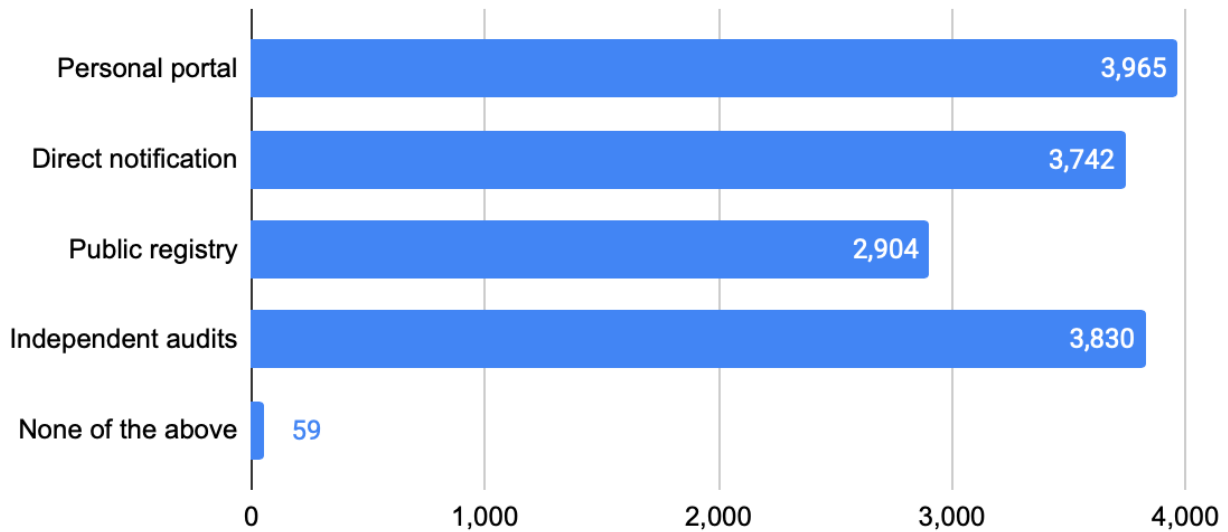
Q4. How comfortable are you with federal government departments sharing your personal data with each other to improve public services?



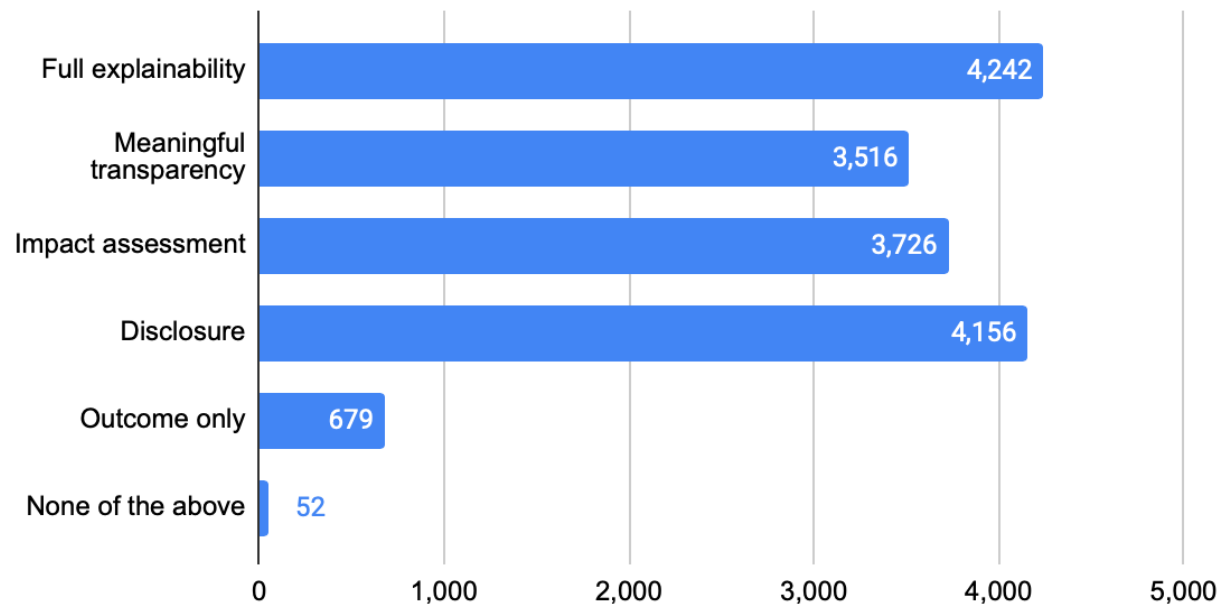
Q5. If a government department were to share your personal data with another department or level of government, what should be required?



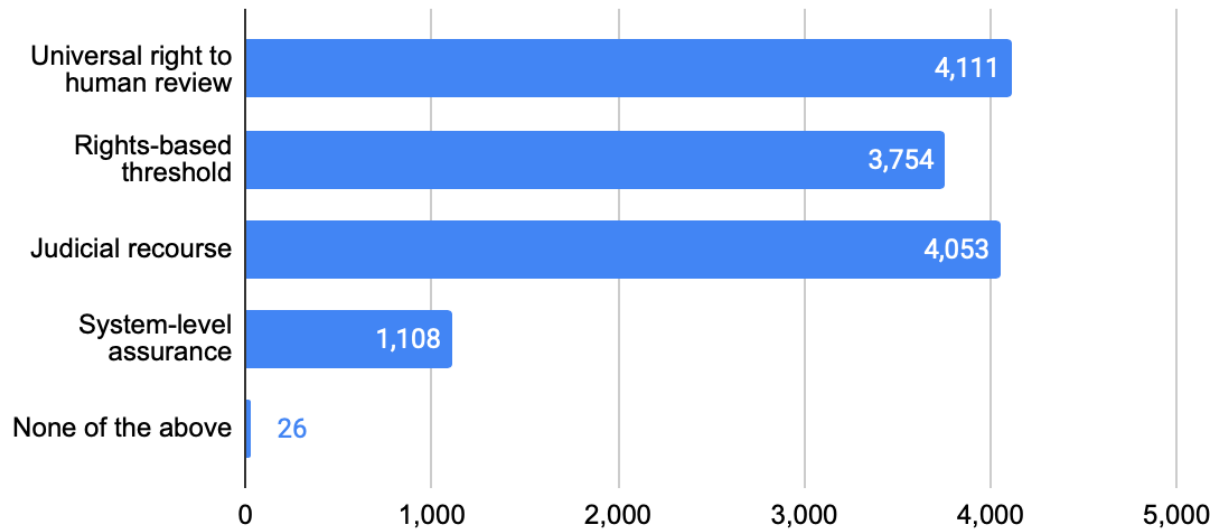
Q6. If your data is shared or reused by the government, what tools or mechanisms should exist to give you visibility and control over your personal data held by the government?



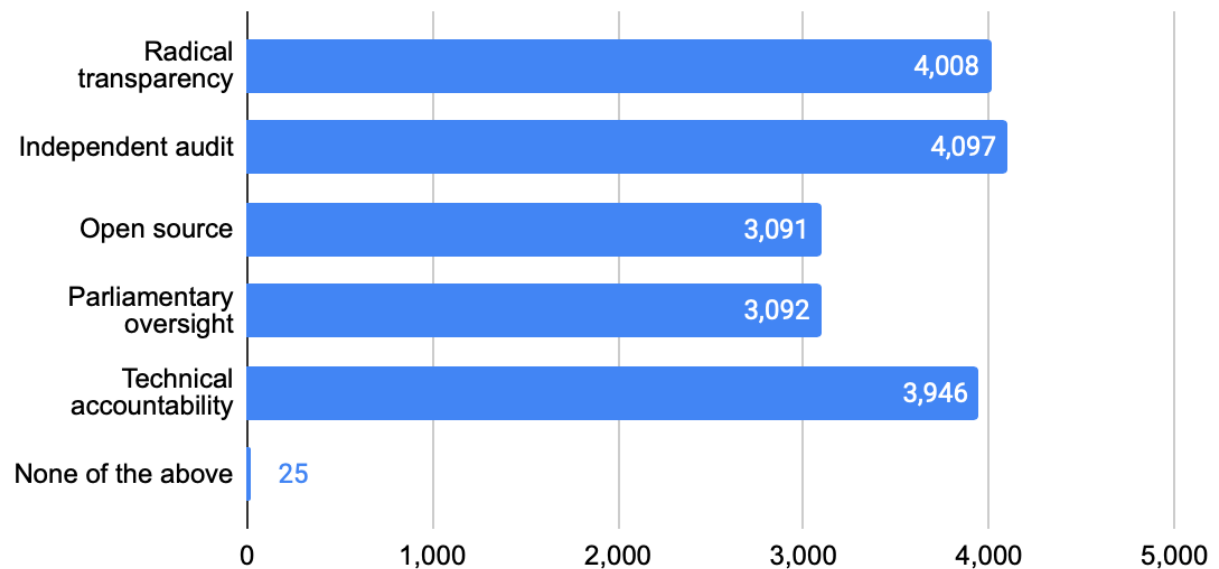
Q7. What should you have the right to know when an AI or automated system is used to make a decision about you?



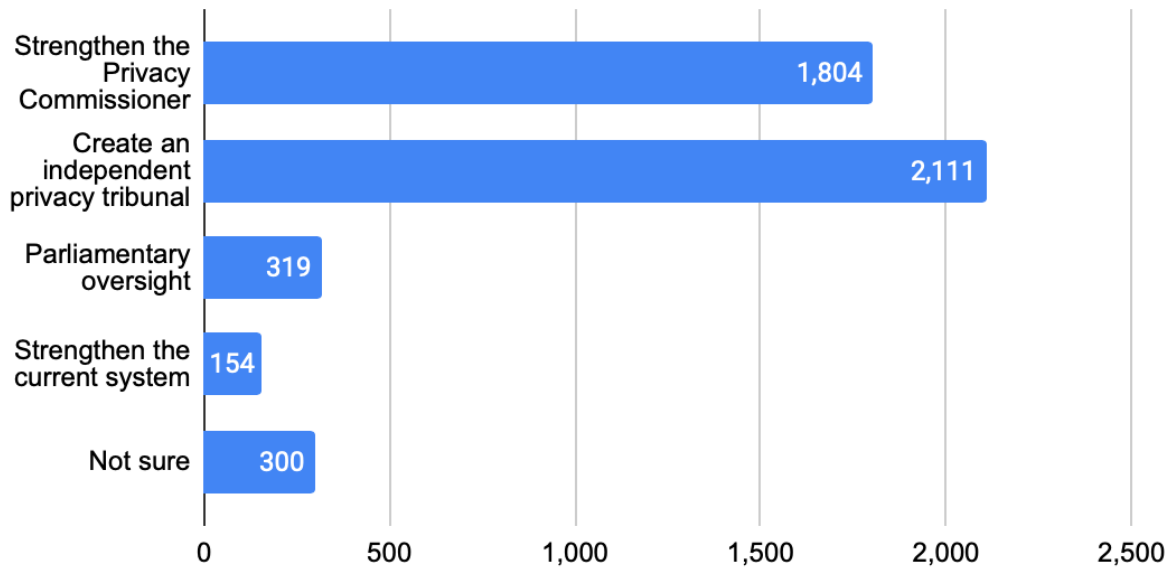
Q8. When an automated system makes a decision that affects you, what should you be able to do about it?



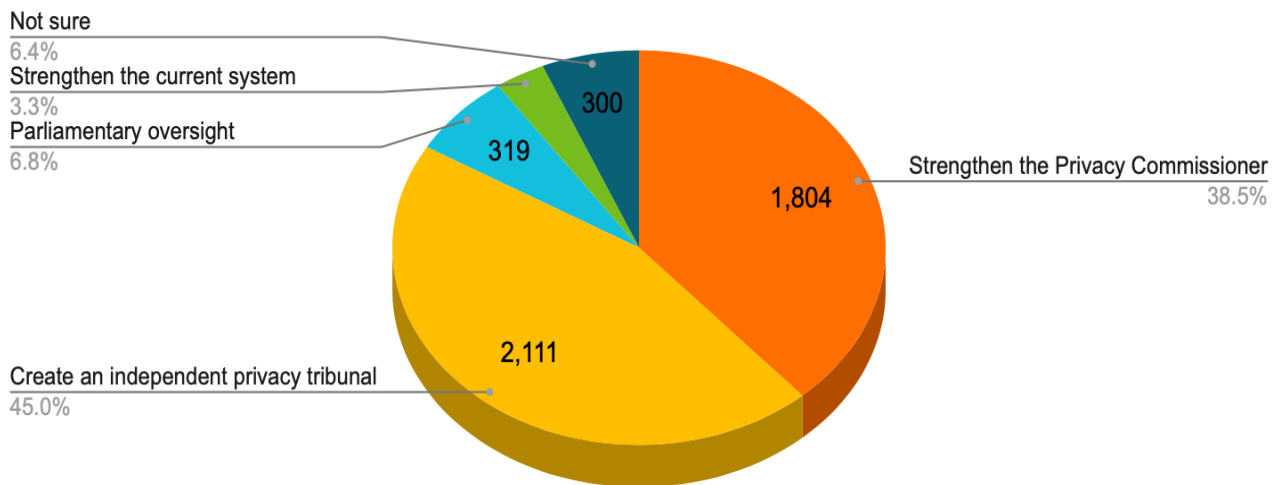
Q9. How should the government be held accountable for the AI systems it uses?



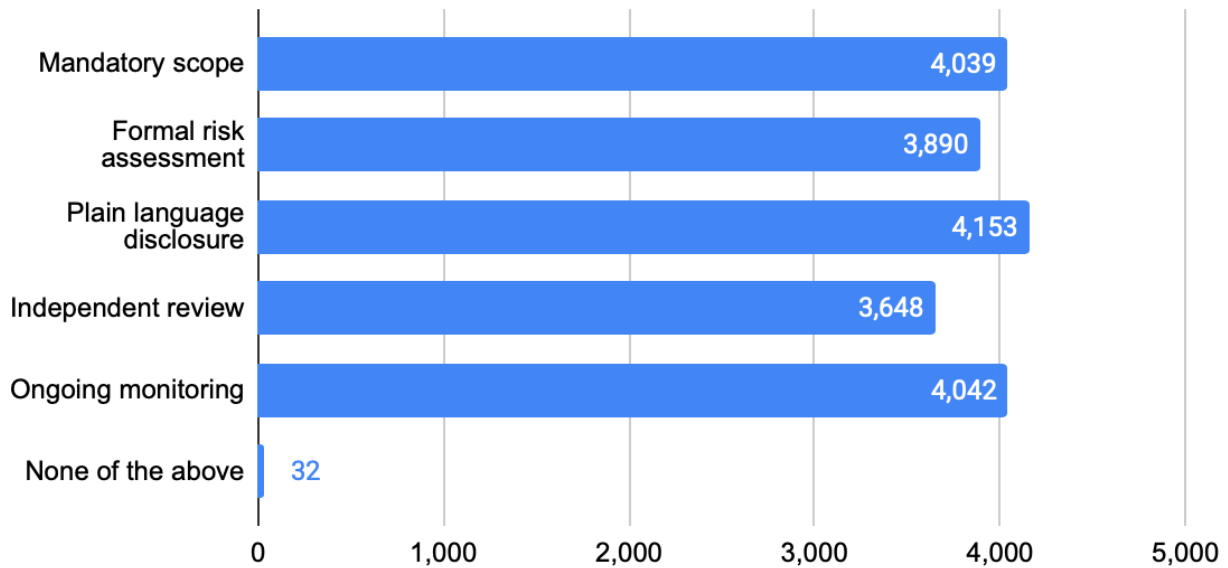
Q10. Who should be responsible for making sure the federal government follows privacy law?



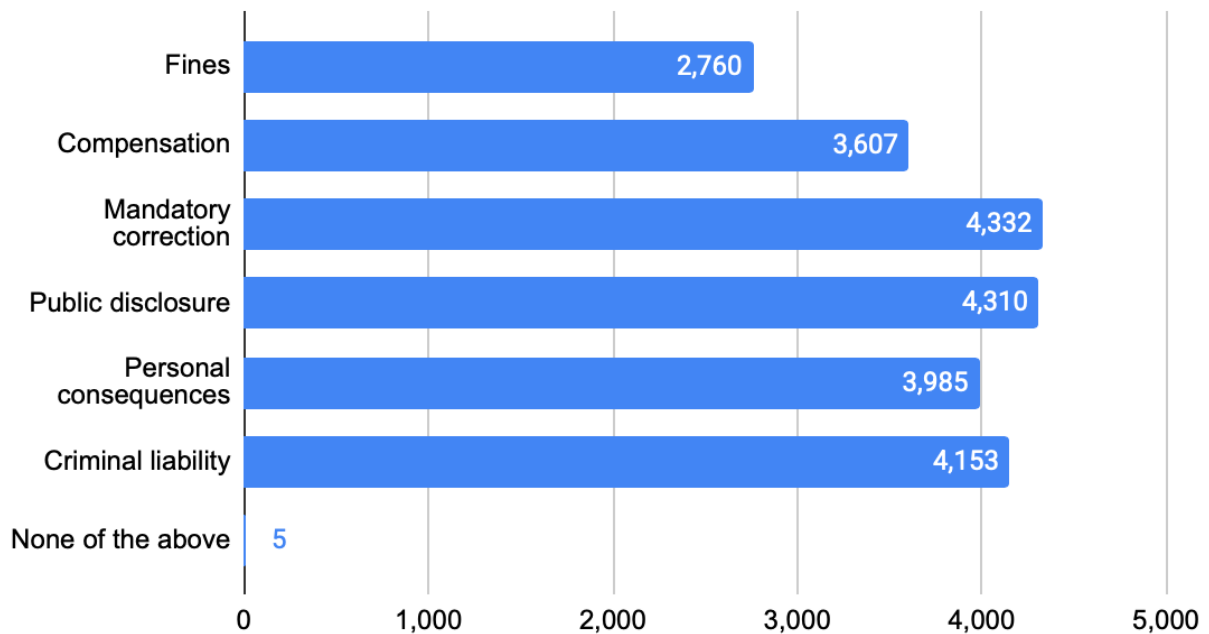
Q10. Who should be responsible for making sure the federal government follows privacy law?



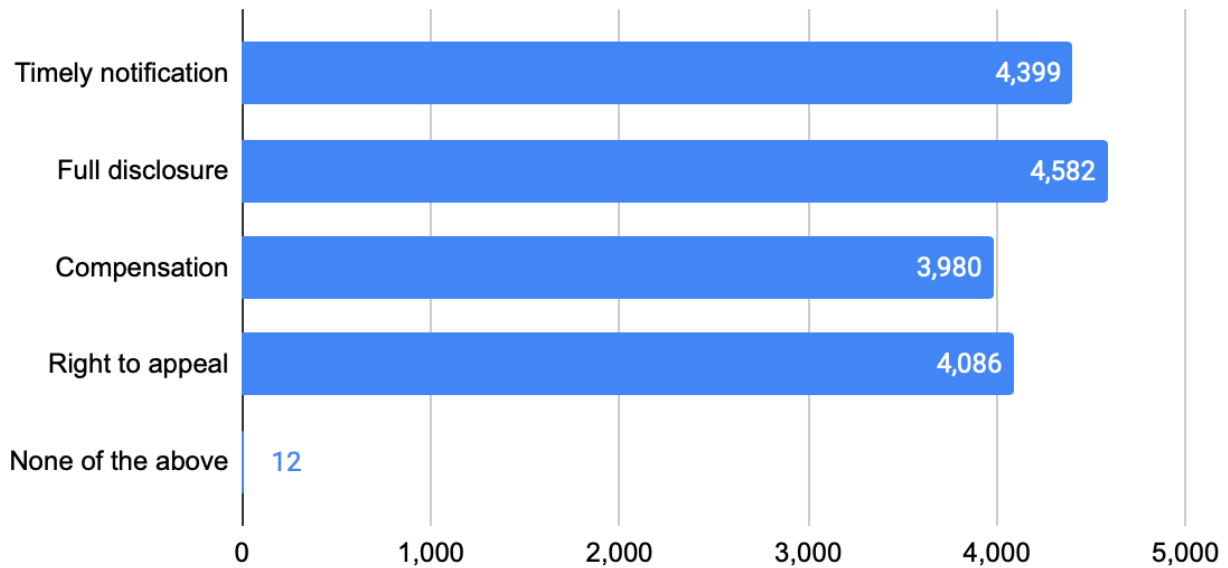
Q11. When a government program collects or uses your personal data, what should be required before it goes ahead?



Q12. When a government department breaks privacy law, what should happen?



Q13. If your personal data is exposed as a result, what should you be entitled to?



Q14. Which of these rights do you feel should be guaranteed in law?

