

July 13, 2026

Chair Brianne K. Nadeau
D.C. Council Committee on Public Works & Operations
1350 Pennsylvania Avenue, NW
Washington, DC 20004

Chair Nadeau and Members of the Committee:

Thank you for the opportunity to submit testimony concerning B26-0670, the DC Government Data Privacy and Protection Act of 2026. The Electronic Privacy Information Center, or EPIC, is an independent nonprofit research organization here in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC has long advocated for Americans' privacy and constitutional rights against government abuses.¹

EPIC applauds the D.C. Council's attention to safeguarding privacy rights and protecting against government abuses. In an era when governments are seeking to collect ever greater amounts of personal information, it is essential that there be meaningful guardrails in place to protect the public's privacy and constitutional rights. EPIC supports legislation that includes strong data minimization language, limits permissible disclosures, and addresses the risks posed by emerging technologies.

However, the collection and use of personal data by government agencies presents special risks that may differ in kind or degree from those posed by commercial surveillance practices, and it is important that the GDPPA fully account for those risks. Absent robust and enforceable safeguards, a government that collects personal data to register voters or administer public benefits may use that same data to carry out politically motivated investigations, intimidate dissenting voices, or fuel mass surveillance systems.

To that end, EPIC encourages the Committee to draw on ongoing efforts in Congress to strengthen the Privacy Act of 1974, the principal framework governing the protection of personal

¹ EPIC, *Comments of the Electronic Privacy Information Center to Congresswoman Lori Trahan* (Apr. 2025), <https://epic.org/documents/comments-of-epic-to-congresswoman-lori-trahan-on-efforts-to-reform-privacy-act-of-1974-and-protect-americans-data-from-government-abuse/>.

data held by federal agencies.² Decades of experience with the Privacy Act, both good and bad, underscore the importance of strictly limiting interagency disclosures of personal data, ensuring maximal transparency and accountability of data flows, and establishing enforcement mechanisms that are resilient to political turmoil. In particular, even the best privacy law is only as strong as it is enforceable, and EPIC strongly encourages the Committee to amend the language to include a private right of action.

I. The Council Should Maintain the Bill's Strong Provisions.

a. Data Minimization

When members of the public interact with the government, they reasonably expect that their data will be collected and used only for the limited purpose and duration necessary to provide the government service. While the legislation provides critical consumer rights, like the right to access, correct, delete, and opt out of harmful practices, a data minimization standard is a critical protection. It will hold government entities accountable for collecting personal information that is only necessary for government services. Any effort to weaken these standards would fail to meaningfully protect people's privacy rights.

b. Third Party Requirements for Data Requests

EPIC applauds the inclusion of language that ensures that third parties that receive personal data shall review the legal validity of any request to access that data, even from federal government agencies. This ensures that third parties are only disclosing this information pursuant a warrant or other valid legal process, and it only allows third parties to disclose the minimum amount of data to comply with the given request. Given the recent requests for collection of personal data from state and local governments, these are essential protections for D.C. residents.³ Businesses can be quick—even eager—to turn over personal information to government authorities, even when not legally required to do so. While government entities might have a sound basis to access this data, it is critical that the Committee adopt rigorous safeguards for such access. Additionally, the bill would require a third party to challenge the request in court if the entity has reason to believe the request is not legal. This critical language would ensure that disclosures are limited to necessary and lawful transfers of personal information.

II. The Committee Should Strengthen the Bill by Tailoring the Language to Known Abuses and Ensuring Strong Enforcement.

² *Id.*

³ Kabbas Azhar & Abigail Kunkler, *DOJ Wants Sensitive Voter Data But Can't Be Bothered to Protect It*, EPIC (Mar. 12, 2026), <https://epic.org/doj-wants-sensitive-voter-data-but-cant-be-bothered-to-protect-it/>.

a. Tailor Language to Government Data Use.

The DC Government Data Privacy and Protection Act uses similar language as in comprehensive consumer privacy laws and proposals across the country. However, this language may not be the best framework for regulating the collection and use of personal data by a sovereign government. For example, the bill tethers its data minimization provision to government products and services, yet many government activities do not fit neatly into these categories.

EPIC would encourage the Committee to draw lessons from the federal Privacy Act and recent efforts to amend that law.⁴ While the Privacy Act is far from perfect and needs updating,⁵ it is a crucial framework for limiting government power over people's personal information. EPIC would urge the Committee to look to the Privacy Act, and the proposed updates, and use both as a basis framework to strengthen this legislation.

b. Target Known Harms Around Sensitive Data Collection and Disclosure.

EPIC applauds the Committee for setting heightened protections for sensitive data (i.e., biometric data, health information, and protections for minors) to prevent collection, processing, or disclosure of this information unless it is strictly necessary. However, EPIC would urge the inclusion of "precise geolocation data" in the definition of "sensitive data." Location data can be incredibly revealing, including indicating whether someone visited an abortion clinic or attended a protest. Thus, collection and disclosure of this data by the government can be extremely concerning. All 24 states that have passed comprehensive privacy laws have included "precise geolocation data" in their definition of "sensitive data." A sample definition can be found in EPIC's model bill, the State Data Privacy Act.⁶

EPIC also appreciates the inclusion on a ban on the sale of sensitive data by government agencies. Sensitive personal information should never be sold to the highest bidder. However, the greatest harms from the sale of sensitive data are currently coming from businesses and third parties. The Committee should make clear that sensitive data that is provided to third-party vendors is never sold.

Additionally, the Committee should ban government agencies from buying personal information from third parties. This loophole has allowed government agencies to avoid obtaining a warrant before accessing personal information, leading to numerous privacy and civil liberties harms. The Committee should end this practice and protect their constituents' information.

⁴ EPIC, *The Privacy Act of 1974*, <https://epic.org/the-privacy-act-of-1974/>.

⁵ *Supra* note 2.

⁶ EPIC, *The State Data Privacy Act* (Apr. 2025), <https://epic.org/documents/the-state-data-privacy-act/>.

c. Include a Carefully Tailored Definition for Publicly Available Data.

Allowing agencies to collect significant amounts of publicly available data without a clear definition could create a major loophole for agencies and third parties. EPIC would encourage the Committee to define publicly available information in this legislation. A sample definition can be found in EPIC's model bill, the State Data Privacy Act.⁷

d. Maximize Transparency.

Agencies should be required to be transparent about information policies and practices with respect to both personal data and sensitive personal data. All notices about collection, use, processing, and disclosure should be in clear and accessible language so that a reasonable person can understand their meaning. Information on what rights individuals have and how to exercise those rights should be readily accessible, easy to understand, and simple to exercise. These notices should be fully accessible and useable for individuals with disabilities. Providing consumers these rights is extremely important, but these rights are only as strong as the knowledge consumers have that they exist and how they can use them. Without strong transparency standards, individuals will be unable to identify harms and violations and, thus, unable to vindicate their rights under this legislation.

EPIC urges the Committee to amend this legislation to require a public comment process before any changes to data flows can go into effect, like the Privacy Act's model of Systems of Records Notices (SORNs). This process would allow the public to weigh in on concerns or suggestions related to the agency's use of data before implementation. Like the Privacy Act, this public comment period should be publicly disclosed, accessible to the public, and available for responses for a set amount of time that allows the public to participate. All comments received by the agency should be considered before the agency adopts the announced change. The federal SORN process has been essential for the public to understand technology and data changes made by federal government agencies. It has also been a critical tool to hold federal agencies accountable for undisclosed data practices and changes. The Committee should adopt a similar framework for public input, transparency, and accountability.

e. Require Affirmative Consent from Individuals Before Using Information to Train AI Systems.

D.C. agencies have been using and developing AI systems in order to provide government services for years.⁸ These systems are using people's data in ways that impact individuals' work, benefits, housing, and interactions with law enforcement. Increasingly, governments are using

⁷ *Id.*

⁸ EPIC, *Screened & Scored in the District of Columbia* (Nov. 2022), <https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf>.

artificial intelligence to make critical decisions in these contexts. EPIC would urge the Committee to amend this legislation to require affirmative written consent before an affected individual's personal data may be used to train an AI model by either agencies or third parties. The affected individual would be anyone whose personal data the agency intends to use in the training of an AI model. AI systems are currently poorly regulated, and many individuals lack awareness that their information may be used to help develop and deploy these technologies. To reduce the burden for both agencies and third parties, the consent should be requested when the personal information is collected in the first place.

f. Strengthen Enforcement Provisions.

Robust enforcement is essential for effective privacy protection legislation. Strong enforcement by a government agency via Attorney General authority, or the creation of a state privacy agency, is a critical piece to include in any strong privacy law. EPIC commends the inclusion of the Office of the Attorney General (OAG) as an enforcer in this legislation. However, funds should be appropriated to ensure the OAG can meaningfully enforce the law.

However, the Committee should amend the language to also include a private right of action. Government enforcement is important, but the scope of data collection is too vast for only one entity to fully regulate. Individuals and groups of individuals who are impacted by the collection, use, and disclosure are in an excellent position to identify privacy issues and bring action to vindicate their rights. The inclusion of a private right to action is one of the most important tools the Council could give to their constituents to protect their privacy. The Privacy Act's private right of action has been a vital tool to hold government entities accountable for reckless and harmful data practices. Not only does the availability of a private right of action preserve government resources, it will ensure there are consequences for any violations.

The current proposal does provide individuals the right to information related to an agency's collection of personal data, the ability to correct inaccuracies, to delete personal data collected, and opt out of the disclosure or sale of personal data. However, the D.C. Council should go further. A private right of action should provide a range of injunctive remedies to allow individuals to fully vindicate their rights under the Act and to address any harmful agency data practices—ideally *before* they are implemented.

Privacy harms are, in many cases, irreparable. Once personal, sensitive information has been illegally accessed or disclosed, the harm cannot be fully undone and the individual cannot be made completely whole, even by damages. That is why individuals should have knowledge, and be able to consent to, any new data practice before they are implemented.

Private rights of action expand ability to enforce the law. Government enforcement agencies can be resource-depleted and vulnerable to political pressure. Many privacy laws across the country

include a private right to action, and these provisions have made it possible to hold entities accountable for privacy violations.⁹ Private enforcement ensures that data collectors have a strong incentive to meet their obligations under a privacy law. Consumers should be able to seek redress for privacy violations the same way they would for other violations of their consumer rights. We encourage the Council to adopt a private right of action.

III. Conclusion

EPIC again commends the D.C. Council for its commitment to safeguarding privacy rights and protecting against government abuses. However, EPIC strongly urges the Council to amend this law to better protect against existing and emerging threats. Specifically, the Council should amend the bill to 1) specifically target current government data practices, 2) protect against known harms from sensitive data use, 3) maximize transparency to constituents, 4) include language around using personal data to train AI systems, and 5) strengthen enforcement provisions.

While this bill is responsive to recent events that highlight the need for updated privacy protections, EPIC urges the Committee to adopt broader reforms. Additionally, EPIC encourages the Committee to ensure that relevant offices have the appropriate funding and expertise to effectively carry out the implementation of this law and safeguard privacy protections for decades to come.

Thank you for the opportunity to submit testimony on this important legislation. EPIC is happy to serve as a resource to the Committee on these issues.

Sincerely,

/s/ John Davisson

John Davisson
Deputy Director and Director of
Enforcement

/s/ Kara Williams

Kara Williams
EPIC Counsel

/s/ Ireland Lesley

Ireland Lesley
EPIC Law Clerk

⁹ Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 Wm. & Mary L. Rev. 1639 (2022), <https://scholarship.law.wm.edu/wmlr/vol63/iss5/5/>.