ACLU
AMERICAN CIVIL LIBERTIES UNION
Wisconsin

207 East Buffalo Street, Suite 325
Milwaukee, WI 53202
(414) 272-4032
aclu-wi.org

January 21, 2026

Chair Swearingen, Vice-Chair Green, and Honorable Members of the Assembly Committee on State Affairs:

The American Civil Liberties Union of Wisconsin appreciates the opportunity to provide testimony in opposition to Assembly Bill 172 in its current form.

For years, privacy, consumer rights, and civil rights advocates have called for meaningful privacy regulations that empower people to live their lives free from intrusive corporate surveillance and discrimination powered by technology. The ACLU of Wisconsin welcomes legislative efforts to address the growing harms caused by unchecked data collection and commercialization. However, while this bill gestures toward consumer rights, it ultimately falls short of providing meaningful privacy protections and risks cementing a weak, industry-friendly framework that does not meet the urgency of this moment.

Corporations have built a surveillance economy that seeks to collect as much information about a person as possible to turn a profit. They harvest data about what we do at home, what we do at work, what we buy, where we go, what doctors we see, our contacts with the criminal legal system, and more. In the United States, these companies face almost no real restrictions on the amount of personal information they can amass about us or the ways that they can exploit it. In the absence of protections, companies have compiled massive dossiers on each one of us containing staggering amounts of information. This information can identify us across our interactions with the world both online and off, within our homes and outside of them, creating the potential for private surveillance on a massive scale. That information can then be sold to data brokers or used to power surveillance-based advertising. Some of these uses have discriminatory impacts, as when companies exclude people from seeing advertisements for employment, housing, or credit on the basis of their race, gender, nationality, or other protected class status.

Privacy is not simply about personal preference or individual choice. It is about whether people can live their lives free from constant monitoring, profiling, and exploitation. When privacy erodes, the harm caused is not distributed evenly. Data is already being used to track reproductive health decisions, including through period trackers and location data tied to clinic visits. LGBTQ+ identities are inferred and monetized through online behavior. Immigrants are surveilled through commercially purchased data that allows law enforcement to bypass constitutional safeguards. Black and brown communities experience both physical over-policing and digital surveillance, with data brokers feeding information into systems that reinforce racial bias. Low-income people and people with disabilities are routinely subjected to algorithmic decision-making that determines access to jobs, housing, credit, and benefits.

Against that backdrop, this bill relies heavily on a notice-and-choice model that has repeatedly failed. Expecting people to read dense privacy policies, understand complex data ecosystems, and manage dozens of opt-out mechanisms is not realistic. Privacy cannot be protected through individual vigilance alone. It requires structural limits and enforceable rules.

There are several fundamental problems with this bill as currently drafted:

AB-172 does not meaningfully limit data collection and provides illusory protection for "sensitive data." Companies are largely free to collect vast amounts of personal data so long as they disclose it. That is not privacy protection. A strong law should require data minimization and purpose limitation. Companies should collect only what is necessary to provide the service a person actually asked for, and use it only for that purpose. Collecting data "just in case" or for future monetization is surveillance, not innovation. Further, the bill dis distinguishes between "personal data" and "sensitive data," and provides an additional right to opt out of the processing of "sensitive data." Sensitive data is defined as data that reveals race or ethnicity, religious beliefs, sexual orientation, citizenship/immigration status, and medical or mental health diagnoses. Although motivated by important concerns, this provision will leave people exposed to the very kinds of privacy violations that it seeks to avoid. Personal data that doesn't *expressly* reveal "sensitive" facts can also be highly sensitive, and when aggregated can reveal these sensitive characteristics even if individual data points do not. Indeed, the entire point of compiling massive stores of personal information by companies is to infer detailed information about people that any one piece of data does not reveal by itself. All personal information should receive robust protection.

AB-172 contains a limited opt-out, rather than strong opt-in consent requirement. The bill permits the collection, use, and sharing of personal information unless the consumer opts out, and only allows consumers to protect themselves by opting out of two categories of uses (targeted advertising and sale of data). That framework puts the burden on individual consumers to wade through dense terms of service with multiple services providers instead of on the companies profiting from data extraction. Opt-out should not be the primary safeguard. Opt-in should be the norm.

Additionally, the ability to opt out only from *sale* of personal information, but not *use* of that information, means that the data practices of the largest surveillance companies like Meta and Google will remain mostly untouched. That is because Meta and Google claim not to sell our personal information, but rather, they amass information about their own users and buy people's information from other companies, and then sell access to tools that make invasive use of that information. Only a strong and broad opt-in consent requirement can adequately protect people's privacy.

The bill does not provide a private right of action for violations. By granting exclusive enforcement authority to state agencies and denying a private right of action, the bill leaves individuals without a meaningful way to vindicate their rights. Agencies do not have the resources to investigate every case (or sometimes any case) where people's rights are violated. Rights without enforcement are not rights at all. If a company misuses your data, you should be able to seek relief in court. Further, the cure provision shields companies from accountability. Allowing companies to avoid penalties by quietly fixing violations after notice encourages noncompliance and treats privacy violations as a cost of doing business rather than a serious harm.

AB-172 broadly preempts local governments from enacting stronger protections. Counties and municipalities may first to respond to emerging privacy threats with local restrictions on biometric surveillance technologies, local digital antidiscrimination laws, and other important measures to protect people's privacy and civil rights. This preemption language would freeze Wisconsin at a low standard and block communities from protecting themselves.

AB-172 does not adequately address discrimination. Data-driven systems are already used to deny people opportunities based on opaque profiles and biased algorithms. At a minimum, there should be require auditing of automated systems for bias. A strong bill would also prohibit discriminatory uses of personal data in a manner that excludes people from opportunities such as housing, employment, education, and credit based on membership in a protected class.

Other states have passed similar laws modeled on the Virginia Consumer Data Protection Act, which has been widely criticized by privacy and civil rights advocates for prioritizing industry interests over people's rights. Wisconsin should not repeat those mistakes. Instead

This bill reflects an important acknowledgment that data privacy matters. But acknowledgment is not enough. Wisconsin has the opportunity to lead by enacting a law that truly limits data collection, centers civil rights, preserves local authority, and gives people real power over how their information is used. As written, this AB-172 does not meet that standard. We urge the committee to substantially strengthen it or to oppose it in its current form.