LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

AG Watch: Minn. Enters New Era Of Data Privacy Enforcement

By **Toni Michelle Jackson and Tiffany Aguiar** (April 8, 2026, 4:56 PM EDT)

This article is part of a regular column in which each installment features observations on one state's attorney general enforcement news and trends, and the compliance implications.


Toni Michelle Jackson


Tiffany Aguiar

The landscape of consumer data privacy enforcement in Minnesota has shifted materially. Until Jan. 31, the Minnesota Attorney General's Office was required to provide 30 days' notice of any believed violation before bringing a lawsuit — a notice period that sunsetted on that date.[1]

For businesses operating in Minnesota — or that collect data from Minnesota residents anywhere in the country — this is not a minor procedural change. It signals that the enforcement posture of the Minnesota Attorney General's Office under Attorney General Keith Ellison has entered a new phase under the Minnesota Consumer Data Privacy Act, or MCDPA.

Businesses that have not yet conducted a thorough compliance review should treat this moment as a call to action.

Defining the MCDPA

The **MCDPA** took effect six months ago, empowering Minnesota residents with key rights over their personal data. Under the law, residents have the right to access data that companies hold about them, have inaccurate data corrected, request deletion of their data, and opt out of the processing of their personal data for targeted advertising.

The law is not limited to Minnesota-based businesses — any company that collects or processes the personal data of Minnesota residents, regardless of where it is headquartered, falls within its scope if it meets applicable thresholds.

Since the MCDPA went into effect, the office sent hundreds of education letters and provided public compliance resources. With the end of the 30-day notice period, the attorney general can now investigate, conclude that a violation has occurred and file suit — all without any prior notice to the company. The Minnesota Attorney General's Office has strongly encouraged businesses within the scope of the MCDPA to review their practices to ensure compliance.

Ellison's Privacy Enforcement Record

Those inclined to view Ellison's MCDPA enforcement posture as untested should look no further than his office's track record.

In November 2022, he joined a bipartisan coalition of 40 attorneys general in reaching a $391.5 million multistate **settlement** with Google — the largest multistate privacy settlement ever reached by attorneys general — after finding that Google allegedly misled consumers about its location tracking practices since at least 2014, with Minnesota alone receiving $8.25 million.[2]

The Minnesota Attorney General's Office has also taken a strong enforcement stance on the impact of emerging technologies on children and teens. On Feb. 1, 2024, the office produced a report for the Minnesota Legislature on the effect that emerging technologies like social media platforms and artificial intelligence are having on young people, finding that these technologies often have a negative effect on the well-being of young people, and that product design choices facilitate these harms and calling for stronger privacy features to protect its users.[3]

And in January, Ellison released a consumer alert regarding the use of digital surveillance tools by the U.S. Department of Homeland Security, warning that Immigration and Customs Enforcement was utilizing advanced tools to identify and track people using data originally collected from online activity, phone apps, smart devices and vehicles, including information collected by data brokers, underscoring the office's commitment to consumer privacy concerns.[4]

Ellison is not a regulator who issues warnings as a formality — his record demonstrates that he is willing to tackle these issues individually and in coalition with peers across the country.

Key Obligations for Businesses

Consent for Sensitive Data

The MCDPA requires companies to secure consent before collecting certain sensitive data, including precise location data, data revealing mental or physical health conditions and data related to citizenship or immigration status.

Any business collecting health and wellness information — through apps, loyalty programs, wearables or other means — must ensure it has affirmative, documented consent before processing such data. A privacy policy disclosure buried in fine print is unlikely to satisfy this standard.

Honoring Consumer Rights Requests — Including the Right to Delete

In the first six months of MCDPA enforcement, the Minnesota Attorney General's Office received more than 200 complaints, and many involved consumers' attempts to exercise data rights under the law, including the right to delete.[5]

Companies must provide a secure and reliable means for consumers to submit rights requests — whether via a portal, email address or other format — that does not require the creation of a new account. Consumers who do not receive a response within 45 days are encouraged to file a complaint with the office, and businesses that miss the response window also face the possibility of direct enforcement action with no advance warning.

Universal Opt-Out Signal Compliance

The Minnesota Attorney General's Office has sent dozens of warning letters identifying problems with the responses to universal opt-out signals — signals sent by browsers or devices communicating a consumer's preference to ensure that their data is not sold or used for targeted advertising.

Going forward, businesses must take affirmative steps to ensure their technical infrastructure can detect and honor these signals. The failure to do so is the type of systemic deficiency that regulators tend to prioritize in enforcement.

Privacy Policy Accuracy

Privacy policy deficiencies were among the most common problems identified in the warning letters. Businesses should conduct a comprehensive and ongoing review of their privacy policies to ensure they accurately describe what data is collected, why it is collected, with whom it is shared and how consumers can exercise their rights.

Conclusion

The MCDPA is here. Ellison's Feb. 5 announcement made clear that the law is fully in effect and being actively enforced. The warning letters issued during the notice period generally resulted in quick corrections, but that corrective opportunity has expired.

Businesses that have not yet prioritized MCDPA compliance are operating with significant and escalating legal exposure — the combination of an active enforcement posture, a growing pipeline of consumer complaints, and the elimination of the 30-day notice requirement creates a risk environment that no covered business should ignore.

Toni Michelle Jackson is a partner and chair of the state attorneys general practice at Crowell & Moring LLP.

Tiffany Aguiar is counsel at the firm.

[1] https://www.ag.state.mn.us/Office/Communications/2026/02/05_MCDPA.asp.

[2] https://www.ag.state.mn.us/Office/Communications/2022/11/14_Google.asp.

[3] https://www.ag.state.mn.us/Office/Communications/2024/02/01_EmergingTechReport.asp.

[4] https://www.ag.state.mn.us/Office/Communications/2026/01/15_DHS_Digital-Surveillance.asp.

[5] https://www.ag.state.mn.us/Office/Communications/2026/02/05_MCDPA.asp.