



July 14, 2026

The Honorable Matt Meyer
Governor of Delaware
Tatnall Building
150 Martin Luther King Jr. Blvd. South
Dover, DE 19901

Re: HB 145- “An Act to Amend Title 11 of the Delaware Code Relating to Reverse Keyword Searches and Court Orders” (Veto Request)

Dear Governor Meyer,

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto of HB 145. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA supports policies that protect individual privacy while providing clear, workable rules for technology companies and law enforcement. Although this legislation is intended to limit reverse keyword searches, it ultimately establishes a legal framework that authorizes their use in certain felony investigations. In doing so, the bill misses an opportunity to provide the clear protections Delaware residents deserve.

The bill’s exceptions substantially broaden governmental authority.

While HB 145 prohibits reverse keyword warrants in most circumstances, it then creates exceptions allowing their use in felony investigations. Rather than establishing a clear rule, the legislation legitimizes the practice by expressly identifying when it may be used.

This exception all but invalidates the rule, as there is nothing to prevent law enforcement from opening a violent felony investigation solely to obtain authorization for a reverse keyword search and then shifting the investigation to a different offense. However, even if this loophole could be closed, the legislation is likely to generate disputes over the scope of the exceptions and the obligations they place on providers. A blanket prohibition on reverse keyword warrants would provide more certainty for courts, law enforcement, and technology companies alike, while reducing litigation over when and how these warrants may be used.

Reverse keyword warrants raise significant constitutional concerns.

Unlike traditional warrants, reverse keyword warrants do not begin with a known suspect or identified account. Instead, they require technology providers to identify individuals based solely on whether they searched for particular terms. Two days before the bill passed the Senate, the Supreme Court ruled in *Chatrue v. United States* that reverse searches must comply with the Fourth Amendment, holding that such searches “resemble[] other private materials—think of emails, documents, photographs, or calendars—that even if stored on Google’s servers, a user reasonably views as his own” and thus “reasonably expects to be



shielded from the ‘inquisitive eyes’ of the government.”¹ The same principle applies to the queries in online search tools that this legislation targets.

Note that a reverse keyword search cannot be constitutionally justified merely because an individual found through the search has committed one of the listed violent felonies. The Supreme Court has long held that “a search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from its success.”² For this reason, the law’s five-hit threshold is constitutionally dubious: law enforcement cannot repeatedly conduct unconstitutional searches until one of them yields the desired suspect.

Moreover, the bill risks sweeping in individuals who have no connection to criminal activity and whose search history may reflect lawful research, curiosity, journalism, education, or other protected activities. Protecting the privacy of innocent users has long been a bipartisan principle, and government searches should remain appropriately tailored and based on individualized suspicion.

This bill places technology companies in the middle of criminal investigations.

HB 145 also expands the role technology providers are expected to play in criminal investigations. Rather than responding to requests for information about a known account or user, providers may be required to conduct technical analyses to determine which users searched for particular terms, undermining their users’ privacy.

Moreover, the bill effectively asks private companies to perform investigative functions that extend well beyond the disclosure of existing account information, and often conflicts with their rights under federal law. For instance, the Stored Communications Act requires that the government reimburse the record provider for the records sought,³ but HB 145 makes no mention of such rights. Such contradictions create substantial uncertainty about how companies are expected to implement these requests.

The bill is based on technical assumptions that do not reflect industry practices.

The legislation further assumes that providers can readily conduct keyword searches through existing databases. In practice, most online services do not maintain systems designed to produce reverse keyword warrant results because there is little operational or commercial reason to create them.

As a result, responding to these requests is often far more complex than querying an existing database. Compliance may require companies to develop customized technical processes that vary considerably across services, increasing costs, creating implementation challenges, and producing inconsistent outcomes.

¹ *Chatrre v. United States*, No. 25-112 at *18 (June 29, 2026).

² *United States v. Di Re*, 332 U. S. 581, 595 (1948).

³ See 18 U.S.C. §§ 2701-2703 (2018).



*

*

*

*

*

For these reasons, CCIA respectfully urges you to veto HB 145. We welcome the opportunity to work with the General Assembly on legislation that provides meaningful privacy protections through a clear prohibition on reverse keyword warrants without exceptions that undermine those protections.

Sincerely,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association