ACLU
AMERICAN CIVIL LIBERTIES UNION
Wisconsin

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

September 5, 2023

Chair Wanggaard, Vice-Chair Jacque, and Honorable Members of the Senate Committee on Judiciary and Public Safety:

The American Civil Liberties Union of Wisconsin appreciates the opportunity to provide written testimony in opposition to Senate Bill 331. Put simply, SB 331 could provide an end-run around the Fourth Amendment's warrant requirement for a local prosecutor and law enforcement agency to intercept the constitutionally protected contents of someone's communications (ie. texts, direct messages, emails, phone calls) and location data by obtaining ex parte permission from *any* judge in the state.

Today, modern communications technologies generate far more, and far more private, information about us than ever before. In the recent past, police would use "pen register" and "trap and trace" devices to find out which phone numbers called each other. Today, the internet-connected services we use generate information far more revealing than phone numbers. This information includes not just who we speak to and for how long, but also where we are, what we talk about, what we read, and what we research online. Now, the federal government uses its statutory pen trap authority to intercept this more revealing data as "dialing, routing, addressing, and signaling" or "DRAS" information. DRAS information includes not only phone call data, but also the "to" and "from" addresses of email messages, records about instant message conversations, data associated with social networking identities, and at least some information about the websites you visit.

This bill would expand the definition of pen register collection from the capture of phone numbers to DRAS information more broadly. It purportedly harmonizes Wisconsin's pen trap law with the corresponding federal statute. However, the bill not only replicates problems with the federal law but also differs in ways that would leave Wisconsinites with even lower protections from privacy intrusions by local law enforcement than they have from the federal government.

Federal law now allows law enforcement to install a pen register to intercept DRAS information under an extremely low standard. A federal judge must grant access to this information any time an attorney for the Government or a state law enforcement officer certifies "that the information likely to be obtained by [installation of a pen register or trap and trace device] *is relevant to an ongoing criminal investigation*." 18 U.S.C. 3123(a) (emphasis supplied). Even if the judge disagrees with the government's certification—for example, finding that installation of the pen trap device would only generate irrelevant information—the court *must* issue the order.

The proposed Wisconsin law uses nearly identical language, requiring a circuit judge anywhere in Wisconsin, even one in a county with no connection to the device, to issue a pen register order if any district attorney merely "certifie[s] to the court that the information to be obtained . . . is relevant to an ongoing criminal investigation." Wis. Stat. § 968.36(1) & SB 331 Section 3 (amending 968.35(1) to allow any DA to seek and any court to grant order, regardless of where the device is located).[1]

Perhaps it made sense for the standard to be so low when a pen register could only gather simple telephone dialing information that the Supreme Court held was not protected by the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 742 (1979). But given the breadth of information that today's internet generates, the pen register standard is insufficiently protective of privacy. Email addresses can convey the substance of a communication, such as a message sent to alcoholicsanonymous@gmail.com. Website addresses can do the same. Further, some DRAS information can reveal the physical location of the people communicating.[2] Moreover, it is unclear how the definition of DRAS information maps onto the sensitive personal communications data, leaving gaps and uncertainties that put privacy at risk. This bill would reproduce the privacy weaknesses in federal law, without taking into account the substantial differences between phone numbers and DRAS information. Rather than doing this, Wisconsin should fashion a statute that accommodates the needs of law enforcement while better protecting the privacy of novel categories of personal information generated by modern communications tools.

But the problems with the bill are even worse than the problems with the comparable federal law in at least two ways:

(1) the bill does not appear to contain a limitation that prevents law enforcement from using a pen register to capture the contents of communications; and
(2) it appears to permit the warrantless collection of sensitive location data even after the Supreme Court's ruling in *Carpenter v. United States*.

SB 331 does not contain the federal law prohibition on using a pen trap device to collect communications content. The Supreme Court held in *Smith* that law enforcement does not need a warrant to collect dialed phone numbers, but only because they do not contain content. 442 U.S. at 741 ("[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.") (emphasis in original). Accordingly, the federal statutes expressly prohibit pen registers from recording "the contents of any communication." 18 U.S.C. 3127(3), (4).

---

[1] Establishing statewide jurisdiction in this way poses a risk that investigators will forum shop for a friendly judge, making abuse of the already low standard even easier.

[2] *See e.g. Pell and Soghoian: A Lot More than a Pen Register, and Less than a Wiretap*, 16 YALE J.L. & TECH. 134 (2013) (describing how cell phone registration process, act of making a call, or transmitting data automatically generates location data of varying degrees of precision.)

Additionally, the government must use reasonably available technology to exclude the collection of the contents of any wire or electronic communications. 18 U.S.C. 3121(c). The Wisconsin bill and background statutes contain neither of these provisions in the pen register context, risking unconstitutional intrusions into the content of communications. *See Berger v. New York*, 388 U.S. 41, 58-60 (1967) (law enforcement may not intercept contents of communications without a warrant); *Katz v. United States*, 389 U.S. 347, 355-56 (1967) (same).

Moreover, the bill does not prohibit law enforcement from collecting constitutionally-protected location data. In *Carpenter*, the Supreme Court held that the government's warrantless acquisition of a person's cell phone location records infringes on reasonable expectations of privacy under the Fourth Amendment. 138 S. Ct. 2206, 2217 (2018). Because of the high sensitivity of location data, the unavoidability of its creation, and its ability to reveal the whole of a person's movements over time, the Fourth Amendment's warrant protections apply. Location data can place an individual in a protected space—such as a home, church, or doctor's office—and otherwise reveal private and sensitive information. Nevertheless, the bill contains no provisions that would ensure that the constitutional privacy interests in location data are protected by a warrant requirement and unavailable to law enforcement on the minimal pen register standard.

For these reasons, the ACLU of Wisconsin urges committee members to vote against this legislation.