DIVISION OF PUBLIC DEFENDER SERVICES
State of Connecticut

OFFICE OF CHIEF PUBLIC DEFENDER
55 FARMINGTON AVENUE, 8TH FLOOR
HARTFORD, CT 06105

ATTORNEY TASHUN BOWDEN-LEWIS
CHIEF PUBLIC DEFENDER
TEL: (860) 509-6429
FAX: (860) 509-6499

Testimony of the Office of Chief Public Defender
Jennifer Bourn, Chief of Legal Services

Judiciary Committee – March 22, 2023
S.B. No. 3 – An Act Concerning Online Privacy, Data and Safety Protections and an Employer's Duty to Disclose Known Instances of Sexual Harassment or Assault Committed by an Employee When Making Employment Recommendations

The Office of Chief Public Defender **opposes Section 9** of **S.B. No. 3, An Act Concerning Online Privacy, Data and Safety Protections and an Employer's Duty to Disclose Known Instances of Sexual Harassment or Assault Committed by an Employee When Making Employment Recommendations**, which would require a court to order a provider of electronic communications services or remote computing services not to disclose to the owner of the data being sought the existence of a search warrant for a period of up to 90 days if "there is reason to believe that notification of the existence of the warrant may result in:

> (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing the investigation.

Although this Office is opposed to this provision for several reasons, we are available to meet and discuss this proposal further and work on language to address the issues raised. A review and comparison of federal statutes and our state statutes and current procedures would be helpful and instructive.

Borrowing language from a federal statute is problematic. Respectfully, the federal statute at issue (18 USC § 2705) was enacted in 1986 and last modified in 1999 – long before **smart phones** were ubiquitous. The rule this proposal seeks to adopt was not written with cell phones, or the third-party providers who store cell phone data, in mind. Instead, the rule was designed to cover data and information inherently less private and invasive than data from a cell phone. The acute privacy interests in the information stored on a cell phone warrant greater protection than this proposal affords.

As courts have started to recognize (*see, e.g*., *Riley v. California*, 573 U.S. 373 (2014); *State v. Smith*, 344 Conn. 229 (2022)), cell phones contain a vast amount of highly personal and private information and require special consideration and modification of Fourth Amendment rules that pre-date the age of the smart phone. Before cell phones, our homes enjoyed the highest level of protection under the Constitution. But the U.S. Supreme Court has recognized that the search of a cell phone is ***more*** intrusive than the search of a home because of the volume and scope of the private information stored on it.

We would never tolerate law enforcement conducting a search of someone's home and seizure of items in it without notification of the owner. The same should be true when the government seeks to search through and seize our highly personal information on our cell phones.

Similarly, search and seizure issues relating to third-party providers who store cell phone data – sometimes a mirror copy of everything on the phone – warrant special consideration and rules generated specifically with those unique privacy interests in mind. The U.S. Supreme Court has also recognized in different contexts that just because information is stored by a third party does not mean that the subject of the information doesn't have an expectation of privacy protected by the Fourth Amendment. *See, e.g., Carpenter v. United States*, 138 S. Ct. 2206 (2018) (cell site location information); *United States v. Jones*, 565 U.S. 400 (2012) (GPS tracking device attached to vehicle). This rationale certainly applies to cell phone information that is backed up on iCloud, Google, or some other third-party provider.

It is worth noting that law enforcement routinely sends preservation letters to third-party providers before getting a warrant, requiring companies to preserve whatever information is there at the time of the letter. Thus, even if the subscriber or customer is subsequently notified about a warrant by the third-party provider, the individual cell phone user does not have the ability to delete the third-party company's records. The third party's records will remain intact whether the user is notified or not, so there is no justification for failing to inform a person that such highly personal and vast information has been seized by the government.

Finally, the proposed language would appear in the general warrant application statute, General Statutes § 54-33c. A warrant is constitutionally required to obtain the contents of someone's cell phone. But a warrant is not always constitutionally required for certain

third-party records. For example, General Statutes § 54-47aa sets forth a procedure of obtaining ex parte orders to compel disclosure of certain carrier or provider telephone and internet records (call-identifying information, communications data, geo-location data or basic subscriber information). That information is more limited than what can be obtained when there is a search warrant for the entire contents of a cell phone stored in an iCloud account, for example. Yet under General Statutes § 54-47aa (f), law enforcement must, within 48 hours of the order, mail notice to the subscriber or customer whose information is being sought. That notification period may be delayed for up to 90 days for the same reasons articulated in this bill. It does not make sense to afford lesser protection to the content of cell phones.

Changing "shall" to "may" to allow the court the discretion to decline to issue such an order when it applies to the content of cell phones, which warrant greater protection under our law, is helpful but does not address all of the constitutional issues raised herein.

In sum, constitutional requirements about the search and seizure of cell phone data are quickly evolving. Such vast and acute privacy interests were not contemplated or at stake when the model for this proposed bill, 18 USC § 2705, was drafted. Nor should substantially similar language in General Statutes § 54-47aa be applied at all in the context of cell phones. Language should not be lifted from these other sources and applied to cell phone warrants without serious discussion and study of the constitutional and policy implications.

This Office is willing to work with stakeholders on these issues. But, as drafted, this Office remains opposed to Section 9 of this bill. It takes no position on the remainder of the bill. Therefore, this Office requests that the Committee delete Section 9 from this bill. Thank you.