May 2024

State-Level Fourth Amendment Is Not For Sale Act[1]

WHEREAS, the Fourth Amendment to the United States Constitution guarantees that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized;"

WHEREAS, the United States Supreme Court has observed that "Few protections are as essential to individual liberty as the right to be free from unreasonable searches and seizures. The Framers made that right explicit in the Bill of Rights following their experience with the indignities and invasions of privacy wrought by general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence. Ever mindful of the Fourth Amendment and its history, the Court has viewed with disfavor practices that permit police officers unbridled discretion to rummage at will among a person's private effects." *Byrd v. United States*, 138 S. Ct. 1518, 1526 (2018). Accordingly, "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [the United States Supreme] Court has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter v. United States*, 138 S.Ct. 2206, 2214 (2018)

WHEREAS, law enforcement agencies are increasingly evading warrant requirements by purchasing personal data from data brokers and other data collectors – a practice that was well-described by the Project on Government Oversight as follows: "Normally, if law enforcement officers want to access your [personal] data, they need a warrant. But a glaring loophole in current law allows law enforcement and government intelligence agencies to pay third party data brokers to gain access to your private, sensitive [personal] data — no warrant needed. The government can (and often does) purchase the personal... data of American citizens from unregulated brokers who offer it up to the highest bidder, all without any court oversight. This is the equivalent of police bypassing the requirement to get a warrant to search someone's apartment by simply handing their landlord an envelope of cash;" and

WHEREAS, law enforcement has been able to effectively and efficiently enforce our criminal laws for more than 230 years without needing to evade Fourth Amendment

[1] Adapted from S.1265, 117th Congress (2021-2022)

warrant requirements that are essential to protecting Americans' liberty and privacy in the digital age;

THEREFORE BE IT RESOLVED, that the *[Name of Legislative Body]* adopts the following:

SECTION 1. DEFINITIONS

(A) "Personal Data" shall mean information collected from or generated by a specific person, as part of a consumer transaction or the use of a consumer product or service, that is linked or reasonably linkable to that specific person or that specific person's electronic device. Personal data shall include, without limitation, a person's (1) name, billing information, social security number, billing address, or demographic data, (2) web browsing or search history, (3) application usage history, (4) location information, (5) financial information, (5) health information, (6) biometric information, (7) characteristics of protected classifications under state or federal law, (8) device identifier, such as a media access control address, international mobile equipment identity, or Internet protocol address, and (9) communications' content.

(B) "Covered individual" shall mean:

(1) A person who is located inside the State of [STATE NAME]; or

(2) A person:

(a) Who is located outside the State of [STATE NAME] or whose location cannot be determined; and

(b) Who is a resident of State of [STATE NAME], as defined in [CITE TO PROVISION OF STATE LAW DEFINING "RESIDENT"].

(C) "Governmental entity" shall mean an agency, instrumentality, or other entity of the State or a political subdivision thereof, including multijurisdictional agencies, instrumentalities, and entities.

(D) "Law enforcement entity" shall mean an agency or other instrumentality of a governmental entity, including the employees and agents thereof, that is authorized by law, regulation, or government policy to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal law.

(E) "Location information" shall mean information derived or otherwise calculated from the transmission or reception of any signal that reveals the approximate or actual geographic location of a customer, subscriber, or device.

(F) "Obtain in exchange for anything of value" shall mean to obtain or receive access to personal data (1) in exchange for money or other valuable consideration, (2) in

connection with services or benefits being provided as consideration, or (3) as part of the provision of a fee, including an access fee, service fee, maintenance fee, or licensing fee.

(G) "Third party" shall mean a person who:

(1) Is not a governmental entity; and

(2) Is not the person to whom the personal data pertains.

SECTION 2. PROHIBITING WARRANTLESS PURCHASES OF PERSONAL DATA

(a) In connection with any criminal, civil, or other investigatory or enforcement activity:

(1) In exchange for anything of value, a law enforcement entity may not obtain or receive access to any covered individual's personal data from a third party.

(2) A law enforcement entity may not request, obtain, or receive access to any covered individual's personal data from any federal, state, or local law enforcement or other government agency or department if such personal data was obtained from a third party in exchange for anything of value.

(3) A governmental entity, including a law enforcement entity, may not provide or share with any federal, state, or local law enforcement agency or department any covered individual's personal data that was obtained from a third party in exchange for anything of value.

(4) Subsections (1)-(3) shall not apply where:

(a) The law enforcement entity has obtained a valid, judicially-issued, probable cause warrant for the personal data of a specifically identified, covered individual(s);

(b) The law enforcement entity asserts, in good faith, that the exigent circumstance exception to warrant requirements applies due to an emergency involving imminent danger of death or serious physical injury to a person that requires disclosure without delay;

(c) The personal data is lawfully available to the public through government records or widely distributed media;

(d) The personal data pertains a specific covered individual, was voluntarily made available to the public by that covered individual, and was obtained in compliance with all applicable laws, regulations, contracts, privacy policies, and terms of service;

(e) The specific covered individual to whom the personal data pertains intended law enforcement to be a recipient of the personal data, as evidenced by case-specific, express consent from the covered individual;

(f) The third party providing the data was authorized by the specific covered individual to whom the personal data pertains to provide the personal data to the law enforcement entity, as evidenced by case-specific, express consent from the covered individual; or

(g) The personal data is being provided to or by the National Center for Missing and Exploited Children.

(b) The Attorney General of [STATE NAME] shall adopt specific procedures that are reasonably designed to prevent the acquisition and retention, prohibit the dissemination, and require the prompt destruction of any covered individual's personal data that is acquired by any Governmental Entity in violation of subsection (A); however, such data shall be retained and may exclusively be used as evidence of a violation of this Act.

SECTION 3. ENFORCEMENT

(A) Any violation of this Act constitutes an injury, and any person may institute proceedings for injunctive relief, declaratory relief, a writ of mandate, and/or attorney fees in any court of competent jurisdiction to enforce this Act.

(B) Any personal data acquired in violation of this Act, and any evidence derived therefrom, may not be used, received in evidence, or otherwise disseminated in any investigation or in any trial, hearing, or other proceeding in or before any court, grand jury, or Governmental Entity, except as evidence of a violation of this Act.

SECTION 4. SEVERABILITY

(A) The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person or circumstance, is held invalid, the remainder of this Act, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

SECTION 5. EFFECTIVE DATE

(A) This Act shall take effect immediately upon adoption.