AN ACT TO REGULATE POLICE USE OF LATERAL SURVEILLANCE

An emerging trend is police reliance on privately-owned surveillance, also known as "lateral surveillance." Lateral surveillance devices — from internet-connected security cameras and video doorbells to automated license plate readers — have proliferated in recent years.

Lateral surveillance can undermine democratic accountability around police use of technology. When agencies seek to purchase their own surveillance devices, they usually must justify the program to lawmakers to obtain funding. In approving a technology, lawmakers might implement safeguards such as restricting how the technology may be used or how long data may be retained. Then, the procurement process generally entails some form of evaluation of the technology in question and comparison across different vendors. But these guardrails are circumvented when surveillance is privately purchased and owned. Agencies can dramatically expand their surveillance reach with no public debate and at no cost. Moreover, certain existing rules governing police surveillance may not apply in the lateral surveillance context, creating a regulatory loophole.

This statute has three main objectives. First, it seeks to identify those circumstances in which lateral surveillance becomes de facto police surveillance (which the statute describes as "Direct Access" to lateral surveillance), and it requires police to obtain democratic authorization in those cases. Second, it sets forth rules addressing some of the key issues unique to lateral surveillance — such as arrangements in which, in exchange for financial subsidies, private individuals have been required to turn over data to the police. Third, it clarifies that existing rules governing police use of surveillance apply in the context of lateral surveillance.

SECTION I: DEFINITIONS

Editor's Note. *Subsection (a)'s definition of lateral surveillance includes a broad range of technologies, from standard video cameras to facial recognition systems. Legislators also may wish to consider regulating data brokers which aggregate and sell data, although this type of surveillance is beyond the scope of the Act. "Direct Access," as set forth in Subsection (b), is intended to capture those circumstances in which privately-owned surveillance is operating as de facto police surveillance.*

(a) **"Lateral Surveillance Technology"** or **"Lateral Surveillance System"** shall mean any privately-owned electronic device, hardware, software, or other system which collects, retains, analyzes, or stores data or communications associated with any individual or group, including but not limited to audio and visual data, locational data, and biometric data. This shall include, but is not limited to:

(i) cameras, including closed-circuit television cameras and internet protocol cameras;

(ii) location-tracking technologies, including automated license plate readers and cell-site simulators;

(iv) software or hardware tools used to gain unauthorized access to a computer or other electronic device; and

(v) biometric technologies, including facial recognition systems.

(b) **"Access"** shall mean (a) operating, logging into, controlling, or otherwise using a lateral surveillance system, or (b) viewing, downloading, transferring, or utilizing data or information derived from a lateral surveillance system.

(c) **"Direct Access"** shall mean law enforcement access to a particular lateral surveillance system and/or data or information derived therefrom in which such access is either (a) real-time, (b) ongoing, or (c) on demand.

(d) A **"Request-Based Platform"** shall mean software which generates and submits requests for access to lateral surveillance technology and/or data or information derived therefrom and which enables such access upon approval by the recipient of the request.

SECTION II: NO SUBSIDIES ABSENT DEMOCRATIC AUTHORIZATION

Editor's Note. *In some jurisdictions, individuals have been offered subsidies to purchase lateral surveillance devices on the condition that they grant police access to them. Under this arrangement, these privately-owned devices are operating as de facto police devices.*

(a) Absent express legislative authorization to the contrary, agencies shall not participate in any program which subsidizes, in part or whole, the purchase of lateral surveillance technology on the condition that private individuals or entities agree to grant law enforcement access to such technology and/or data or information derived therefrom.

SECTION III: DEMOCRATIC AUTHORIZATION GENERALLY REQUIRED

Editor's Note. *Police access to lateral surveillance can vastly expand an agency's surveillance capabilities without any legislative authorization, or even the budgetary and regulatory constraints that ordinarily come into play in the procurement process. The purpose of this provision is to identify those circumstances in which private surveillance becomes de facto police surveillance and to require legislative authorization in those cases. Subsection (b) provides a limited, temporary exception to the authorization requirement in exigent circumstances or in response to an offense that is in progress (for example, police seeking access to the cameras of a store being robbed). Subsection (c) clarifies that authorization may cover the use of a single device, a set of devices (e.g., a set of ALPRs operated by a homeowner association), or a technology in general (e.g., all CCTV cameras), as policymakers deem fit.*

(a) Absent express authorization by a legislative body having authority to regulate the agency, a law enforcement agency shall not have Direct Access to Lateral Surveillance Technology and/or data or information derived therefrom.

(b) Notwithstanding Section III(a) of this Act, a law enforcement agency may have Direct Access to Lateral Surveillance Technology and/or data or information derived therefrom without democratic authorization on a temporary basis, not exceeding twenty-four hours (a) in exigent circumstances involving imminent danger of death or serious injury to a person or (b) in response to a felony offense, violent crime, or property damage exceeding $100 being

committed at the time of the access.

(c) Democratic authorization under Section III(a) of this Act may cover an agency's use of a single device, a set of devices, or a technology in general.

SECTION IV: REQUEST-BASED PLATFORMS

Editor's Note. *The special rules in this section apply only to request-based platforms. First, to address the potential for coercive requests, police must make clear that individuals may refuse to grant access to lateral surveillance. Second, to address the potential for bias on the part of request recipients, requests must be sufficiently specific — this is intended to prohibit requests that, for example, simply ask for videos of "suspicious persons" or individuals of a particular race. Third, to address concerns about police requests for surveillance of First Amendment activities, the Act requires such requests to relate to a specific criminal offense. These concerns might also arise when police make direct, in-person requests for data from device-owners (as opposed to using a request-based platform). Lawmakers may wish to regulate these interactions as well — this can be accomplished by specifying that the provisions of this Section apply both to requests submitted through a Request-Based Platform and to requests made directly in-person.*

(a) Any law enforcement request for lateral surveillance technology and/or data or information derived therefrom submitted through a Request-Based Platform shall, in addition to any other requirements provided by law:
   (i) expressly state that individuals are under no obligation to provide access;
   (ii) include specific details about the individuals or activities under investigation;
   (iii) if the request includes race as part of a suspect description, contain at least two additional non-race descriptors; and
   (iv) provide a method for users to opt out of receiving future requests.

(b) Agencies shall not submit requests related to lawful protests or other protected First Amendment activities unless such requests also relate to a specific felony offense, violent crime, or property damage exceeding $100.

SECTION V: COURT ORDERS

Editor's Note. *To the extent that existing law requires police to obtain a court order, warrant, or other authorization to conduct certain types of surveillance (for example, surveillance which entails the tracking of a suspect's locations or movements), this provision clarifies that such requirements also apply in the lateral surveillance context. Existing laws governing the use of a particular technology (for example, facial recognition technology) apply to privately-owned technology of the same type. Likewise, existing laws governing the use of a particular type of data (for example, "video data") apply to privately-held data of the same type.*

(a) Any law which requires a law enforcement agency to obtain a warrant, court order, or other authorization to access a particular surveillance technology shall apply regardless of whether that technology is privately or publicly-owned.

(b) Any law which requires a law enforcement agency to obtain a warrant, court order, or other

authorization to access a particular type of data derived from a surveillance technology shall apply regardless of whether that data is derived from a privately or publicly-owned surveillance technology.

(c) For purposes of this Section, "law" shall mean (1) state and federal statutory law and (2) clearly-established constitutional law.[1]

SECTION VI: LATERAL SURVEILLANCE DATA

Editor's Note. *The purpose of this provision is to ensure that agencies cannot circumvent existing restrictions on police-owned surveillance by relying on lateral surveillance. For example, if a law imposes a particular retention period for police ALPR data, this provision ensures that police cannot exceed this period by relying on private ALPR data. This provision applies only to law enforcement; it is not intended to regulate the storage, handling, sharing, and/or use of surveillance data by private individuals.*

(a) Any federal or state law regulating the storage, handling, sharing, and/or use of a particular type of data by law enforcement shall apply regardless of whether such data was originally derived from a privately or publicly-owned surveillance technology.

(b) The regulations to which this section applies include, but are not limited to, laws pertaining to data retention, the handling of personally identifiable information ("PII"), and the use of analytics such as facial recognition.

SECTION VII: TRANSPARENCY AND OVERSIGHT

Editor's Note. *Because lateral surveillance technologies are in private hands, policymakers may have limited ability to exercise oversight. The purpose of this Section is to increase transparency and accountability around police use of lateral surveillance.*

(a) Each law enforcement agency with Direct Access to Lateral Surveillance Technology and/or data or information derived therefrom shall issue a Report on the Use of Lateral Surveillance on a quarterly basis.

(i) A "Report on the Use of Lateral Surveillance" shall mean a public report detailing, for each Lateral Surveillance Technology and/or data or information derived therefrom to which the agency has Direct Access:

(A) The type of surveillance technology being accessed and, if applicable, the number of devices accessed;

(B) The general location of the surveillance technology and/or data derived

[1] Lawmakers should consider whether, under state constitutional law, the incorporation by reference of prospective federal law constitutes an impermissible delegation of legislative authority to Congress. *Compare* State v. Williams, 119 Ariz. 595, 598–99 (1978) (en banc) ("[A]n incorporation by state statute of rules, regulations, and statutes of federal bodies to be promulgated subsequent to the enactment of the state statute constitutes an unlawful delegation of legislative power."), *with* McFaddin v. Jackson, 738 S.W.2d 176, 180 (Tenn. 1987) (holding that incorporation of prospective federal law is not an impermissible delegation, stating "that the legislature retains the power to withdraw its approval of any future amendment the Congress might make").

therefrom; and

(C) The types of offenses the technology was used to investigate.

(b) Any state or federal law requiring audits of police use of surveillance technology shall apply to police use of lateral surveillance technology.

(c) Regarding agency use of Lateral Surveillance Technology that is not subject to auditing under Section VII(b) of this Act, the State Attorney General shall, within one year of the effective date of this Act, propose to the State Legislature additional auditing procedures covering such use.

SECTION VIII: REMEDIES

Editor's note. *The purpose of specifying that the unauthorized use, retention, or sharing of data constitutes a cognizable injury is to ensure that individuals subjected to unlawful surveillance have standing to sue under the Act. This provision may need to be modified in light of state standing requirements.*

(a) **Civil Cause of Action**: Any person or entity injured as a result of an agency's violation of this Act shall have a civil cause of action against such agency for damages (but not less than liquidated damages in the amount of $10,000) and reasonable costs and attorneys' fees. A court shall award punitive damages in an amount no less than $10,000 if the agency's violation of this Act was willful.

(i) The unauthorized use, retention, or sharing of data regarding an individual or entity shall constitute a cognizable injury under this Act.

(b) **Injunctions**: The State Attorney General or any court of this State, upon the motion of a person or entity bringing suit under this Act, may prohibit an agency from accessing any lateral surveillance technology and/or data or information derived therefrom where necessary to stop ongoing substantial violations or this Act, or to prevent future substantial violations of this Act.

(c) **Administrative Remedies**: Violation of this Act by an employee of a law enforcement agency shall be grounds for termination, demotion, or any other appropriate consequences for such employee, on the decision of such agency.

(d) **Exclusion**: Lateral surveillance technology and/or data or information derived therefrom obtained in violation of the terms of this Act shall not be used against a criminal defendant in any state or local prosecution.