WORKING DRAFT

AUTHORIZED DATABASES AND POLICING TECHNOLOGY (ADAPT) ACT

This document presents a model statute drafted by the Policing Project at New York University School of Law that is designed to bring front-end accountability to the use of policing technology. Our Authorized Databases and Police Technology (ADAPT) Act builds from the framework established by the ACLU's Community Control Over Police Surveillance (CCOPS) model statute, which was drafted nearly four years prior to the drafting of this document, but adds new language to regulate the use of policing databases along with policing technologies.

We make this working draft available for public review in the hopes of soliciting additional feedback and encouraging broader dissemination and use.

POLICING PROJECT AT NYU LAW

POLICINGPROJECT.ORG | FOLLOW US ON TWITTER @POLICINGPROJECT

TABLE OF CONTENTS

Section 1. Purpose and Scope

(A) The purpose of this Act is to ensure accountability, public approval, and transparency, around policing technology and databases.

(B) This Act cover the use of policing technology and databases by (i) police and other law enforcement agencies; (ii) any other governmental agencies performing a policing function; and (iii) any private party performing a policing function (hereinafter referred to as "agency").

(C) A "policing function" describes law enforcement actions, peace-keeping actions, and investigative actions typically conducted by the police or other law enforcement agencies, but which might involve other agencies as well.

(D) This Act applies to policing technology and databases.

(1) "Policing technology" shall mean any system used as part of a policing function, including software or electronic devices, that is capable of collecting, retaining, or analyzing information associated with or capable of being associated with any specific individual or group, including but not limited to audio, video, images, text, meta-data, location, spectral imaging, or biometric information.

(a) "Policing technology" includes, but is not limited to: cell site simulators; automated license plate readers (ALPRs); gunshot detectors; facial recognition software; drones; thermal imaging systems; predictive policing software; body-worn cameras; social media analytics software; and audio or video recorders that are capable of transmitting or can be accessed remotely.

(b) "Policing technology" does not include: routine office technology, such as televisions, computers, email systems and printers, that is in widespread public use; manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; and internal police department computer aided dispatch or record management systems, unless the systems are equipped with predictive analytics capabilities.

(2) "Policing database" shall mean any system used as part of a policing function that is capable of accessing, storing, cataloging, or analyzing information associated with or capable of being associated with any specific individual or group, including but not limited to audio, video, images, text, meta-data, location, spectral imaging, or biometric information.

(a) "Policing database" includes, but is not limited to: fingerprint databases; DNA databases; gang-databases; automated license plate reader databases; or criminal history databases.

(b) "Policing database" does not include: systems for storing case-files; systems for office and clerical purposes; or investigative information that is not tagged to a specific individual, or cannot be used to identify a specific individuals.

Section 2. Approval for Policing Technology and Database Acquisition or Use

(A) Absent an emergency situation, an agency must obtain written approval by the City Council or designated committee prior to purchasing, acquiring, or using any new policing technology or database, or using an existing policing technology or database in a new manner not previously approved.

(B) With regard to a policing database, "in a manner not previously approved" includes linking or cross-referencing existing databases, adding new categories of data to a database, or using new analytic tools on an existing database.

Section 3. Standard for Approval of Policing Technology or Database

(A) In deciding whether to approve the request, the City Council or designated committee shall consider whether the public safety benefits of the use of the policing technology or database outweigh the economic, social, and community costs, including potential negative impacts on civil liberties and civil rights and potential disparate impacts on particular communities or groups.

(B) At least sixty (60) days prior to seeking approval of a policing technology or database, pursuant to Section 2(A), an agency shall submit to the City Council and make publicly available a written policing technology or database "Use Report," along with a draft of the municipal agency's proposed policing technology or database "Use Policy" concerning the technology or database at issue.

(C) The public shall have forty-five (45) days subsequent to filing of the policing technology or database "Use Report" and "Use Policy" to submit formal comments to the City Council or designated committee.

Section 4. Policing Technology or Database Use Report and Use Policy

(A) A Policing Technology or Database "Use Report" shall describe in plain and accessible language the use, purposes, and impacts of the technology. This document would include, at a minimum, the following:

(1) Description and Purpose: A description of the policing technology or database, how it works, and the purposes for which it will be used;

(2) Efficacy: A statement explaining why the technology or database is necessary to achieve its stated purposes; the basis for thinking that it will be effective in doing so; and a description of any existing technologies or databases that the agency already is using that perform similar functions;

(3) Data Collection: For policing technologies that collect data, a statement describing the types of data that will be collected or analyzed using the technology; any measures that the agency will take to minimize the inadvertent collection of additional data; how the agency will keep the data secure; and whether data will be shared with any other government or private entities, and if so, whether the entities will be required to comply with the policing technology "Use Policy" as part of the data sharing agreement;

(4) For policing databases:

(a) Data Collection: A statement describing the types of data that will be collected or analyzed

using the database; explaining the categories of individuals whose data will be included in the database; and detailing how the data is collected.

(b) Data Storage: A statement describing how the agency will keep the data secure, whether data will be shared with any other government or private entities, and if so, whether the entities will be required to comply with the policing database "Use Policy" as part of the data sharing agreement;

(c) Data Analysis: A statement describing the process of searching the database, including the level of suspicion required to search for data on any individual and any procedural authorization required within the municipal agency.

(5) Potential Harms: A statement describing any potential harms that use of the technology or database may impose, including privacy harms, racially disparate impacts, or constitutional violations. The statement should also make clear what steps, if any, the department plans to take to minimize potential harms, to prevent unauthorized use of the technology, and to audit its use to ensure that it is used in accordance with agency policy;

(6) Fiscal Impact: Statement describing the fiscal impact, including any personnel costs associated with monitoring its use or complying with public records requests.

(B) The draft policing technology or database "Use Policy" should, at a minimum, address the following:

(1) Authorized and prohibited use(s) of any policing technology, including:
(a) Which agency personnel will have authority to use the technology;

(b) The legal and procedural rules that will govern each authorized use, including whether prior approval from a supervisor or court is required before the technology is used;

(2) Authorized and prohibited use(s) of any databases, including:
(a) Which agency personnel will have authority to add data to the database;

(b) Which agency personnel will have authority to search the database;

(c) The legal and procedural rules that will govern each authorized search of the database, including whether prior approval from a supervisor or court is required, what level of suspicion is needed before the database is used, and how the search results will be analyzed;

(3) Data retention, including:
(a) How long data will be retained by the policing technology or database;

(b) The process by which data will be deleted after the retention period elapses;

(4) Data access, analysis, and release:
(a) The circumstances under which data collected using the policing technology may be accessed for further investigation or included in a database;

(b) The circumstances under which data may be shared with other government agencies, or with members of the public;

(5) Documentation and supervisory review:

(a) Whether and how agency officials must document their use of the technology or database;

(b) What responsibilities supervisors will have, if any, to document and review each deployment or use.

(C) No later than ninety (90) days following the effective date of this Act, any agency possessing or using policing technology or databases regulated by this Act shall conspicuously and publicly post the following information:

(1) The name of the agency responsible for ensuring compliance with all regulations, laws, and protocols related to this Act;

(2) The name of the agency responsible for publication of the policing technology and database "Use Reports" and "Use Policies";

(3) Where policing technology and database "Use Reports" and "Use Policies" will be posted in a centralized, conspicuous, and publicly accessible manner;

(4) The timetable for reporting on and establishing use policies for technologies and databases currently in use.

Section 5. Review of Preexisting Uses of Policing Technology and Databases

(A) No later than three hundred and sixty five (365) days following the effective date of this Act, any covered entity seeking to continue the use of any policing technology adopted in the last five (5) years that was in use prior to the effective date of this Act, or to continue the sharing of data therefrom, must commence the approval process in accordance with Section 2(A).

(B) No later than three hundred and sixty five (365) days following the effective date of this Act, any covered entity seeking to continue the use of any policing database that was in use prior to the effective date of this Act must commence the approval process in accordance with Section 2(B).

Section 6. Annual Policing Technology and Database Report and Annual Public Meeting

(A) Any agency that operates an approved policing technology must prepare an annual "Policing Technology and Database Report" that includes:

(1) A list of all approved policing technologies or databases in possession or use by the agency, indicating which have been used at least once during the prior calendar year;

(2) Copies of the most recent policing technology or database "Use Policies" for each approved technology or database;

(3) The number of civilian complaints or internal disciplinary referrals received in the past year

(concerning the use of policing technologies or databases, broken down by the technology or database at issue;

(4) The results of any internal audits conducted in the past year concerning the use of any policing technology or database, as well as any actions taken in response;

(5) Total annual costs for each policing technology or database, including any personnel costs, if known; if the agency is unable to provide a concrete estimate of associated personnel costs, the agency should briefly describe the sorts of tasks that personnel have performed over the past year to support the use of the technology or database at issue.

(B) Within sixty (60) days of submitting and publicly releasing the annual "Policing Technology and Database Report" pursuant to Section 6(A), the agency shall hold one or more well-publicized and conveniently located community engagement meetings ("Annual Public Meeting") at which the general public is invited to discuss and ask questions regarding the annual "Policing Technology and Database Report" and the agency's use of policing technologies or databases.

Section 7. Triennial Assessments of Policing Technologies and Databases

(A) Three (3) years after the approval of a policing technology or database pursuant to Sections 2(A) and 2(B), and every fifth year following, the City Council or designated entity shall produce and submit to the City Council a policing technology or database "Use Assessment."

(B) A "Use Assessment" shall address, at a minimum, the following:

(1) A reappraisal of the initial evaluation performed in Section 3(A), including whether the public safety benefits of the policing technology or database have outweighed its economic, social, and community costs, including potential adverse impacts on civil liberties and/or civil rights, and potential disparate impacts on particular communities or groups;

(2) With respect to each cost identified in response to Section 8(B)(1), what remedial adjustments to laws and policies should be made so as to achieve a more just and equitable outcome going forward;

(3) In light of the responses to Section 8(B)(1)-(2), whether the balance of benefits and costs of the new technology or database support its continued use.

Section 8. Remedies; Penalties; Whistleblower Protections

(A) Failure to obtain City Council approval of any policing technology or database pursuant to this Act, or the willful omission or misrepresentation of material information about the policing technology or database as part of the request for approval, will result in the immediate cessation of its use.

(B) Use of policing technologies or databases in a manner or for a purpose beyond that described in the request for approval will result in the cessation of any activities outside the scope of the "Use Policy" described in Section 4 of this Act.

(C) Any person or group may institute proceedings for injunctive relief, declaratory relief, writ of mandate in any court of competent jurisdiction to enforce the provisions described in Sections 2 through 7 of this Act.

(D) A court shall award costs and reasonable attorney's fees to a plaintiff who is the prevailing party in any action under Section 7(A); or to a prevailing party in any action under Section 7(B) of this Act where the use of policing technology or database substantially differs from the scope of the "Use Policy" previously provided.

(E) Whistleblower protections:

(1) Any individual coming forward, in good faith and through lawful disclosure, with evidence that an agency failed to comply with the provisions of this Act shall be protected against any adverse action taken against them in retaliation for their disclosure.

(2) No agency or anyone acting on behalf of an agency may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because the employee or applicant was perceived to, about to, or did assist in a disclosure described in Section 7(E)(a).

(3) Within ninety (90) days of the effective date of this Act, the City Council shall conspicuously post and make publicly available the process for submitting a whistleblower complaint regarding a violation of this Act.

Section 9. Contractual Agreements

(A) It shall be unlawful for the city or any agency to enter into any contract or other agreement that conflicts with the provisions of this Act, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

Section 10. Budget and Resources

(A) The City Council shall allocate sufficient funds enable agencies to comply with both the prior approval and subsequent reporting requirements.

Section 11. Severability

(A) The provisions in this Act are severable. If any part of 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 12. Effective Date

This Act shall take effect on [DATE].