

AN ORDINANCE OF COUNCIL ENACTING ARTICLE 551 OF THE CODIFIED ORDINANCES OF THE CITY OF HUNTINGTON, AS REVISED, ESTABLISHING THE CITY OF HUNTINGTON PUBLIC SAFETY TECHNOLOGY AND CONSTITUTIONAL RIGHTS ORDINANCE; ESTABLISHING GOVERNANCE STANDARDS FOR THE USE OF CERTAIN PUBLIC SAFETY TECHNOLOGIES; PROVIDING FOR AUTHORIZED USES, PROHIBITED USES, DATA RETENTION, DATA SHARING, OVERSIGHT, TRANSPARENCY, AUDITS, ENFORCEMENT, AND OTHER RELATED MATTERS

WHEREAS, this Council has previously approved a contract pursuant to which the City will endeavor to utilize various technologies, including automated license plate readers (ALPR), live video cameras, drone as first responder systems, acoustic gunshot detection systems, and artificial intelligence-assisted investigative software for the detection and prosecution of serious and violent crimes within the City; and

WHEREAS, while the implementation of these systems is anticipated to be of significant value to the Huntington Police Department in the detection and prosecution of violent crimes and drug crimes, it is incumbent upon Council and the Administration to enact common sense guidelines and policies to prevent the misuse of the technologies; and

WHEREAS, Council further acknowledges its responsibility and the responsibility of the Administration to set use parameters to assure compliance with all municipal, state and federal laws, including, but not limited to, the Driver's Privacy Protection Act of 1994, 18 U.S.C. §2721-2725; the Computer Fraud and Abuse Act, 18 U.S.C. 1030; the statute prohibiting the deprivation of rights under the color of law, 18 U.S.C. §242; the Federal Cyber Stalking and Interstate Stalking Act, 18 U.S.C. §2261(A)(2); and the West Virginia statute prohibiting the use of photo monitoring devices to prove traffic violations, W.Va. Code §17C-6-7; and

WHEREAS, it is further necessary that Council enact guidelines to establish practical transparency measures in matters concerning the use of this technology;

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE CITY OF HUNTINGTON, CABELL AND WAYNE COUNTIES, WEST VIRGINIA, that Article 551 of the Codified Ordinances of the City of Huntington, as revised, is hereby **ENACTED** to read as follows:

**ARTICLE 551
PUBLIC SAFETY TECHNOLOGY**

551.01 PURPOSE.

The City Council finds:

- (a) Public safety is a core function of municipal government.
- (b) Modern technology can assist law enforcement in many ways including locating violent offenders, dismantling drug trafficking organizations, recovering stolen vehicles, locating missing persons, and solving serious crimes.
- (c) Nevertheless, the Fourth Amendment to the United States Constitution and Article III of the Constitution of West Virginia protect citizens from unreasonable government intrusion.
- (d) The technologies governed by this ordinance observe activity occurring in public places where individuals generally do not have a reasonable expectation of privacy; however, the City recognizes that the collection, retention, and use of such information must be subject to meaningful Constitutional safeguards.
- (e) The City rejects both mass surveillance and unnecessary restrictions that prevent law enforcement from protecting the public.
- (f) This ordinance establishes enforceable safeguards to ensure that public safety technology is used only for legitimate law enforcement purposes, subject to transparency, accountability, and constitutional limitations.

551.02 APPLICATION.

This ordinance applies to the following technologies:

- (a) Automated License Plate Readers (ALPR);
- (b) Live video cameras;
- (c) Drone as First Responder systems;
- (d) Acoustic gunshot detection systems; and
- (e) Artificial intelligence-assisted investigative software.

551.03 DEFINITIONS.

As used in this article:

- (a) "Authorized User" means an individual who has been granted individual credentialed access to a covered Public Safety Technology System by the Chief of Police or the Chief's designee, whose official duties require such access, and who has completed all required training.
- (b) "Authorized Use" means any use expressly permitted by this ordinance and reasonably related to a documented criminal investigation, emergency response, missing person investigation, stolen vehicle investigation, or other lawful public safety purpose authorized herein.
- (c) "Public Safety Technology" means any technology governed by Section 551.02 of this ordinance.
- (d) "Public Safety Technology System" means any hardware, software, cloud-based platform, sensor, camera, drone, database, or related technology governed by this ordinance.
- (e) "Public Safety Technology Data" means any image, audio, license plate information, metadata, geolocation information, alert, or other electronically stored information generated or collected through a Public Safety Technology System.
- (f) "Documented Criminal Investigation" means an investigation supported by a case number, incident number, call for service number, intelligence report, or other official law enforcement documentation.

551.04 DEPLOYMENT AND PLACEMENT STANDARDS.

(a) Public Safety Technology governed by this ordinance shall be deployed only where reasonably related to a legitimate public safety objective.

(b) Deployment decisions shall be based upon one or more of the following:

- (1) Documented crime patterns;
- (2) Drug trafficking activity;
- (3) Recovery of stolen vehicles;
- (4) Traffic ingress and egress routes;
- (5) Critical infrastructure protection;
- (6) School safety;
- (7) Officer safety;
- (8) Emergency response needs;
- (9) Missing person investigations;
- (10) Special events presenting documented public safety concerns; or
- (11) Other documented public safety considerations authorized by law.

(c) Public Safety Technology shall not be deployed for the purpose of monitoring persons based solely upon: race; color; national origin; religion; sex; disability; political activity; participation in

lawful First Amendment activities; or any other characteristic protected by federal or state law.

(d) The Chief of Police shall maintain written documentation identifying the public safety justification for each permanent deployment location.

(e) Deployment locations shall be reviewed periodically. Public Safety Technology shall be relocated or removed when the original documented public safety justification no longer exists or when another location presents a greater documented public safety need.

551.05 PROHIBITED ACTS.

No person shall:

- (a) Knowingly access, use, or disclose Public Safety Technology, a Public Safety Technology System, or Public Safety Technology System Data without being an Authorized User, or, being an Authorized User, knowingly access, use, or disclose Public Safety Technology, a Public Safety Technology System, or Public Safety Technology System Data for a purpose other than an Authorized Use; or
- (b) Knowingly and without authorization tamper with, disable, obstruct, damage, remove, or interfere with the operation of any Public Safety Technology System equipment, including a body-worn camera, or knowingly cause such equipment to fail to record or transmit data it would otherwise have recorded or transmitted.

551.06 AUTHORIZED USERS.

(a) Access to any Public Safety Technology System shall be limited to Authorized Users.

(b) The Chief of Police shall maintain a current written list of Authorized Users.

(c) Each Authorized User shall receive individual login credentials.

(d) Shared accounts and shared passwords are prohibited.

(e) Authorized Users shall complete training on this ordinance and applicable departmental policies before receiving access.

551.07 AUTHORIZED USES.

Permitted uses of the Public Safety Technology, Public Safety Technology System, or Public Safety Technology System Data authorized by this ordinance include the investigation of or emergency response to a known or suspected:

- (a) Homicide;
- (b) Attempted homicide;
- (c) Kidnapping;
- (d) Robbery;
- (e) Felony assault;
- (f) Human trafficking;
- (g) Drug trafficking;
- (h) Organized criminal enterprises;
- (i) Terrorism;

- (j) Missing persons;
- (k) Amber Alerts;
- (l) Silver Alerts;
- (m) Stolen vehicles;
- (n) Active warrants;
- (o) School threats;
- (p) Critical infrastructure protection;
- (q) Disaster response;
- (r) Officer safety;
- (s) Criminal investigations involving conduct that reasonably may constitute a felony; and
- (t) Other imminent threats to life or public safety as authorized by law.

551.08 PROHIBITED USES.

Public Safety Technology, Public Safety Technology System, or Public Safety Technology System Data governed by this ordinance shall never be used for:

- (a) Tracking persons based solely upon the lawful exercise of constitutional rights or participation in lawful activities protected by federal or state law.
- (b) Immigration enforcement unless required by federal warrant or other lawful court order.
- (c) Traffic, parking, or code enforcement.
- (d) Revenue generation.
- (e) Personal curiosity.
- (f) Civil investigations unrelated to legitimate public safety purposes.
- (g) Pattern analysis subject to the provisions of Section 551.10.

551.09 PUBLIC SAFETY TECHNOLOGY DATA SEARCHES.

(a) Searches of Public Safety Technology Data shall be conducted only by Authorized Users.

(b) Every search shall include:

- (1) Authorized User Number;
- (2) Date;
- (3) Time;
- (4) Reason for the search; and
- (5) Case number or incident number, when applicable.

551.10 HISTORICAL LOCATION AND MULTI-LOCATION ANALYSIS.

- (a) Historical Public Safety Technology Data may be searched only when authorized under Section 551.07 and reasonably limited in time, geographic scope, and investigative purpose.
- (b) Pattern, multi-location, or aggregated analysis may be conducted only for a Documented Criminal Investigation or another Authorized Use under this article and with documented supervisory approval.
- (c) A warrant shall be obtained whenever required by the Fourth Amendment to the United States Constitution, Article III of the Constitution of West Virginia, or controlling federal or state law. Nothing in this section limits the use of historical Public Safety Technology Data pursuant to a recognized exception to the warrant requirement.
- (d) Searches conducted under this section shall comply with all documentation, audit, retention, verification, and data-sharing requirements established by this article.
- (e) This section shall be reviewed following any controlling decision of the Supreme Court of the United States, the United States Court of Appeals for the Fourth Circuit, or the Supreme Court of Appeals of West Virginia, or following enactment of governing legislation by the West Virginia Legislature.

551.11 DATA RETENTION.

- (a) Routine data shall be retained for no more than thirty (30) days, or such shorter period as may be required by applicable federal or state law.
- (b) Evidence associated with a criminal investigation shall be retained pursuant to applicable criminal evidence laws and policies.
- (c) Automatic deletion shall occur upon expiration of the retention period.
- (d) No data shall be retained indefinitely absent lawful authority.

551.12 DATA SHARING.

Data sharing shall occur only:

- (a) Pursuant to written agreements approved by the Chief of Police and the City Attorney;
- (b) With law enforcement agencies possessing comparable privacy and security protections;
- (c) For documented criminal investigations or other authorized public safety purposes; and
- (d) Subject to complete audit capability.

The City shall not provide access to, or share, Public Safety Technology Data with another governmental entity for the purpose of circumventing any limitation or prohibition established by

this ordinance.

“Written agreements” shall not include mutual aid agreements or memoranda of understanding with other law enforcement agencies executed prior to the adoption of this ordinance.

551.13 VENDOR RESTRICTIONS.

No vendor may:

- (a) Sell, license, disclose, monetize, retain beyond the period authorized by this ordinance use to train or improve artificial intelligence or machine learning systems, analyze for product development, or otherwise derive a commercial benefit from Public Safety Technology Data or any derivative thereof, except to the extent reasonably necessary to perform its contractual obligations.
- (b) Retain records required to be deleted under this ordinance.
- (c) Disclose Public Safety Technology Data except pursuant to lawful legal process or the City's written authorization.

The vendor shall promptly notify the City of any subpoena, warrant, court order, or other legal demand for Public Safety Technology Data unless prohibited by law.

551.14 VERIFICATION BEFORE ENFORCEMENT.

An automated alert shall never constitute probable cause by itself. Prior to initiating enforcement action, officers shall independently verify:

- (a) License plate;
- (b) Vehicle description;
- (c) Registration information;
- (d) Hot list status; and
- (e) Other relevant circumstances.

551.15 CYBERSECURITY.

All covered Public Safety Technology Systems shall:

- (a) Use encryption;
- (b) Require multi-factor authentication;
- (c) Maintain immutable audit logs; and
- (d) Receive annual penetration testing.

551.16 PUBLIC TRANSPARENCY.

The Chief of Police shall provide to the Mayor and City Council an annual report, on or before January 30 of each year, including:

- (a) Number of searches conducted;
- (b) Crime investigations assisted;
- (c) Outside agency searches or requests for assistance;

- (d) Documented policy violations; and
- (e) Discipline imposed for violations of this ordinance or departmental policy.

The annual report shall not disclose information that would compromise an active criminal investigation, reveal confidential law enforcement techniques, or identify protected personal information.

551.17 AUDITS.

- (a) Quarterly internal audits shall be conducted to ensure compliance with this ordinance and applicable departmental policy.
- (b) An independent annual audit shall be completed and presented publicly to the City Council.
- (c) Audit findings shall include, at a minimum:
 - (1) Compliance with authorized use requirements;
 - (2) Compliance with search documentation requirements;
 - (3) Compliance with data retention requirements;
 - (4) Compliance with data sharing requirements;
 - (5) Documented policy violations; and
 - (6) Corrective actions taken.

551.18 MISUSE.

- (a) Unauthorized Access or Disclosure.

No person shall knowingly:

- (1) Access or attempt to access any Public Safety Technology System or Public Safety Technology Data without authorization;
- (2) Use Public Safety Technology Data for any purpose not authorized by this ordinance;
- (3) Disclose Public Safety Technology Data except as authorized by law or this ordinance; or
- (4) Provide another person with credentials or access for the purpose of circumventing the requirements of this ordinance.

- (b) Tampering with Public Safety Technology.

No person shall knowingly disable, damage, remove, obstruct, interfere with, or otherwise impair the operation of any Public Safety Technology System owned or operated by the City except during authorized installation, maintenance, repair, replacement, or testing.

551.19 FOURTH AMENDMENT RULE OF CONSTRUCTION.

This ordinance shall be interpreted in favor of protecting constitutional liberties while enabling legitimate public safety objectives. Nothing in this ordinance shall be construed to authorize generalized surveillance, indiscriminate tracking of law-abiding persons, or investigative practices inconsistent with the Fourth Amendment to the United States Constitution or Article III of the Constitution of West Virginia.

551.20 SEVERABILITY.

If any provision, subsection, sentence, clause, phrase, or application of this ordinance is held to be invalid or unconstitutional by a court of competent jurisdiction, such determination shall not affect the validity of the remaining portions of this ordinance, which shall remain in full force and effect. To this end, the provisions of this ordinance are declared to be severable.

551.21 WRITTEN POLICIES APPLICABLE TO THE HUNTINGTON POLICE DEPARTMENT.

The Chief of Police is directed and authorized to establish written policies consistent with this ordinance applicable to use of the technology described in this article. In addition to the provisions herein, said policies shall establish guidelines for usage reporting by authorized users, prior authorization by a superior for any specific use in non-emergent situations, post-usage authorization by a superior for any specific use in emergent situations, and a disciplinary guideline applicable to misuse under this ordinance or under the written policies. The guidelines shall be approved by the Chief of Police and the Mayor and shall be made available to the public in the Clerk's office. Any changes to the written policies shall immediately be made publicly available in a like manner.

551.99 PENALTY.**(a) Administrative Sanctions for Authorized Users.**

Any Authorized User who knowingly violates this ordinance or any policy adopted pursuant to this ordinance shall be subject to administrative action, and where applicable consistent with the provisions of W.Va. Code §8-14-20 and §8-14a-1, *et seq.* concerning the discipline of professional police officers, including:

- (1) Immediate suspension or revocation of system access;
- (2) Mandatory retraining;
- (3) Employee discipline, up to and including termination of employment; or
- (4) Referral for criminal investigation where the conduct may constitute a violation of federal or state law.

(b) Enforcement.

Any violation of subsection 551.18 shall be subject to enforcement in accordance with the general penalty provisions of the Codified Ordinances of the City of Huntington (see Article 101.99) and applicable provisions of West Virginia law. Nothing in this ordinance shall be construed to limit the authority of the City to pursue any other remedy authorized by law.

(c) Other Remedies Preserved.

Nothing in this ordinance shall preclude:

- (1) Criminal prosecution under applicable federal, state or municipal law;
- (2) Civil remedies otherwise authorized by law;
- (3) Injunctive or equitable relief; or
- (4) Administrative discipline imposed by the City.

BE IT FURTHER ORDAINED that the enactment of Article 551 of the Codified Ordinances of the City of Huntington, as revised, shall become effective after its adoption by Council and approval by the Mayor.

SPONSORED BY: _____

APPROVED AS TO FORM BY: _____

ACTION TAKEN BY COUNCIL: _____

DATE: _____

LISA ADKINS, CITY CLERK

DATE: _____

PATRICK J. FARRELL, MAYOR

APPROVE

DATE: _____

VETO