SENATE BILL 587

By: **Senator Sydnor**
Introduced and read first time: January 29, 2021
Assigned to: Judicial Proceedings

A BILL ENTITLED

AN ACT concerning

Facial Recognition Privacy Protection Act

FOR the purpose of requiring certain governmental units to produce and update certain reports relating to the development, procurement, or use of facial recognition services at certain intervals through a certain process; requiring certain governmental units to communicate certain information to the public by certain deadlines, post certain reports on certain websites, and submit certain reports to the Department of Information Technology; requiring certain governmental units to ensure that certain decisions are subject to certain review; requiring certain governmental units to perform certain testing of a facial recognition service before deploying the facial recognition service; requiring a provider of a certain facial recognition service to make available a certain application programming interface for certain testing of the service; requiring a provider of a certain facial recognition service to develop and implement a certain plan under certain circumstances; requiring certain governmental units to conduct certain training; prohibiting certain governmental units from using a facial recognition service for certain purposes under certain circumstances; authorizing a court to issue a certain order under certain circumstances; prohibiting certain governmental units from applying a facial recognition service to an individual on certain bases; requiring certain governmental units to disclose the use of facial recognition services to certain individuals in a certain manner under certain circumstances; requiring certain governmental units to maintain certain records; requiring certain judges to report certain information to the Court of Appeals on or before a certain date each year; declaring certain findings of the General Assembly; defining certain terms; providing for the application and effect of this Act; and generally relating to facial recognition services.

BY adding to
    Article – State Government
    Section 10–1701 through 10–1711 to be under the new subtitle "Subtitle 17. Facial
        Recognition Services"
    Annotated Code of Maryland

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
    [Brackets] indicate matter deleted from existing law.

(2014 Replacement Volume and 2020 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – State Government

SUBTITLE 17. FACIAL RECOGNITION SERVICES.

10–1701.

(A)   IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B)   "ACCOUNTABILITY REPORT" MEANS A REPORT PRODUCED IN ACCORDANCE WITH § 10–1704 OF THIS SUBTITLE.

(C)   (1)   "ENROLL" MEANS THE PROCESS BY WHICH A FACIAL RECOGNITION SERVICE CREATES A FACIAL TEMPLATE FROM ONE OR MORE IMAGES OF AN INDIVIDUAL AND ADDS THE FACIAL TEMPLATE TO A GALLERY USED BY THE FACIAL RECOGNITION SERVICE FOR RECOGNITION OR PERSISTENT TRACKING OF INDIVIDUALS.

(2)   "ENROLL" INCLUDES THE ACT OF ADDING AN EXISTING FACIAL TEMPLATE DIRECTLY INTO A GALLERY USED BY A FACIAL RECOGNITION SERVICE.

(D)   (1)   "FACIAL RECOGNITION SERVICE" MEANS TECHNOLOGY THAT ANALYZES FACIAL FEATURES AND IS USED BY A UNIT FOR THE IDENTIFICATION, VERIFICATION, OR PERSISTENT TRACKING OF INDIVIDUALS IN STILL OR VIDEO IMAGES.

(2)   "FACIAL RECOGNITION SERVICE" DOES NOT INCLUDE:

(I)   THE ANALYSIS OF FACIAL FEATURES TO GRANT OR DENY ACCESS TO AN ELECTRONIC DEVICE; OR

(II)   THE USE OF AN AUTOMATED OR SEMI–AUTOMATED PROCESS FOR THE PURPOSE OF REDACTING A RECORDING FOR RELEASE OR DISCLOSURE OUTSIDE A LAW ENFORCEMENT AGENCY TO PROTECT THE PRIVACY OF A SUBJECT DEPICTED IN THE RECORDING IF THE PROCESS DOES NOT GENERATE OR RESULT IN THE RETENTION OF ANY BIOMETRIC DATA OR SURVEILLANCE INFORMATION.

(E)   "FACIAL TEMPLATE" MEANS THE MACHINE–INTERPRETABLE PATTERN

OF FACIAL FEATURES THAT IS EXTRACTED FROM ONE OR MORE IMAGES OF AN INDIVIDUAL BY A FACIAL RECOGNITION SERVICE.

(F)   "IDENTIFICATION" MEANS THE USE OF A FACIAL RECOGNITION SERVICE BY A UNIT TO DETERMINE WHETHER AN UNKNOWN INDIVIDUAL MATCHES ANY INDIVIDUAL:

(1)   WHOSE IDENTITY IS KNOWN TO THE UNIT; AND

(2)   WHO HAS BEEN ENROLLED BY REFERENCE TO THAT IDENTITY IN A GALLERY USED BY THE FACIAL RECOGNITION SERVICE.

(G)   "MEANINGFUL HUMAN REVIEW" MEANS REVIEW OR OVERSIGHT BY ONE OR MORE INDIVIDUALS WHO:

(1)   ARE TRAINED IN ACCORDANCE WITH § 10–1709 OF THIS SUBTITLE; AND

(2)   HAVE THE AUTHORITY TO ALTER THE DECISION UNDER REVIEW.

(H)   (1)   "ONGOING SURVEILLANCE" MEANS TRACKING THE PHYSICAL MOVEMENTS OF A SPECIFIED INDIVIDUAL THROUGH ONE OR MORE PUBLIC PLACES OVER TIME, WHETHER IN REAL TIME OR THROUGH THE APPLICATION OF A FACIAL RECOGNITION SERVICE TO HISTORICAL RECORDS.

(2)   "ONGOING SURVEILLANCE" DOES NOT INCLUDE A SINGLE RECOGNITION OR ATTEMPTED RECOGNITION OF AN INDIVIDUAL IF NO ATTEMPT IS MADE TO SUBSEQUENTLY TRACK THE INDIVIDUAL'S MOVEMENTS OVER TIME AFTER THE INDIVIDUAL HAS BEEN RECOGNIZED.

(I)   "UNIT" HAS THE MEANING STATED IN § 10–1301 OF THIS TITLE.

(J)   "VERIFICATION" MEANS THE USE OF A FACIAL RECOGNITION SERVICE BY A UNIT TO DETERMINE WHETHER AN INDIVIDUAL IS A SPECIFIC INDIVIDUAL:

(1)   WHOSE IDENTITY IS KNOWN TO THE UNIT; AND

(2)   WHO HAS BEEN ENROLLED BY REFERENCE TO THAT IDENTITY IN A GALLERY USED BY THE FACIAL RECOGNITION SERVICE.

10–1702.

THE GENERAL ASSEMBLY FINDS THAT:

(1)   THE USE OF FACIAL RECOGNITION SERVICES BY UNITS OF STATE AND LOCAL GOVERNMENT CAN PRESENT RISKS TO PRIVACY, DEMOCRATIC FREEDOMS, AND CIVIL LIBERTIES THAT SHOULD BE CONSIDERED AND ADDRESSED;

(2)   FACIAL RECOGNITION TECHNOLOGY CAN BE USED IN A VARIETY OF BENEFICIAL WAYS, INCLUDING FOR IMPROVING SECURITY, PROVIDING INDIVIDUALS WITH EFFICIENT IDENTIFICATION EXPERIENCES, LOCATING MISSING OR INCAPACITATED INDIVIDUALS, IDENTIFYING VICTIMS OF CRIME, AND KEEPING THE PUBLIC SAFE; AND

(3)   IT IS NECESSARY TO ESTABLISH SAFEGUARDS THAT WILL ALLOW GOVERNMENT TO USE FACIAL RECOGNITION SERVICES IN WAYS THAT BENEFIT SOCIETY WHILE PROHIBITING USES THAT THREATEN THE PRIVACY, DEMOCRATIC FREEDOMS, AND CIVIL LIBERTIES OF INDIVIDUALS IN THE STATE.

10–1703.

THIS SUBTITLE DOES NOT APPLY TO A UNIT THAT:

(1)   IS REQUIRED TO USE A SPECIFIC FACIAL RECOGNITION SERVICE:

(I)   IN ACCORDANCE WITH A FEDERAL REGULATION OR ORDER; OR

(II)   THROUGH A PARTNERSHIP WITH A FEDERAL AGENCY TO FULFILL A CONGRESSIONAL MANDATE; OR

(2)   USES A FACIAL RECOGNITION SERVICE IN ASSOCIATION WITH A FEDERAL AGENCY TO VERIFY THE IDENTITY OF INDIVIDUALS PRESENTING THEMSELVES FOR TRAVEL AT AN AIRPORT OR SEAPORT.

10–1704.

(A)   (1)   EACH UNIT USING OR INTENDING TO DEVELOP, PROCURE, OR USE A FACIAL RECOGNITION SERVICE SHALL PRODUCE AN ACCOUNTABILITY REPORT FOR THE FACIAL RECOGNITION SERVICE.

(2)   EACH UNIT SHALL:

(I)   CLEARLY COMMUNICATE THE ACCOUNTABILITY REPORT TO THE PUBLIC:

1.	AT LEAST **90** DAYS BEFORE THE UNIT PUTS THE FACIAL RECOGNITION SERVICE INTO OPERATIONAL USE; OR

2.	FOR A FACIAL RECOGNITION SERVICE IN USE ON OCTOBER 1, 2021, ON OR BEFORE JANUARY 1, 2022;

(II)	POST THE ACCOUNTABILITY REPORT ON THE PUBLIC WEBSITE OF THE UNIT; AND

(III)	SUBMIT THE ACCOUNTABILITY REPORT TO THE DEPARTMENT OF INFORMATION TECHNOLOGY.

(3)	THE DEPARTMENT OF INFORMATION TECHNOLOGY SHALL POST EACH SUBMITTED ACCOUNTABILITY REPORT ON ITS PUBLIC WEBSITE.

(B)	EACH ACCOUNTABILITY REPORT SHALL INCLUDE, AT A MINIMUM, IN CLEAR AND UNDERSTANDABLE LANGUAGE, THE FOLLOWING INFORMATION:

(1)	(I)	THE NAME, VENDOR, AND VERSION OF THE FACIAL RECOGNITION SERVICE; AND

(II)	A DESCRIPTION OF THE GENERAL CAPABILITIES AND LIMITATIONS OF THE FACIAL RECOGNITION SERVICE, INCLUDING REASONABLY FORESEEABLE CAPABILITIES OUTSIDE THE SCOPE OF THE PROPOSED USE OF THE UNIT;

(2)	(I)	THE TYPE OR TYPES OF DATA INPUTS THAT THE FACIAL RECOGNITION SERVICE USES WHEN IT IS DEPLOYED;

(II)	HOW THE DATA THAT THE FACIAL RECOGNITION SERVICE USES IS GENERATED, COLLECTED, AND PROCESSED; AND

(III)	THE TYPE OR TYPES OF DATA THE FACIAL RECOGNITION SERVICE IS REASONABLY LIKELY TO GENERATE;

(3)	A DESCRIPTION OF THE PURPOSE AND PROPOSED USE OF THE FACIAL RECOGNITION SERVICE, INCLUDING:

(I)	WHAT DECISIONS DATA FROM THE FACIAL RECOGNITION SERVICE WILL BE USED TO MAKE OR SUPPORT;

(II)	WHETHER DATA FROM THE FACIAL RECOGNITION SERVICE WILL BE USED TO SUPPORT A DECISION OR AS THE SOLE BASIS FOR MAKING A

DECISION; AND

(III) THE INTENDED BENEFITS OF THE USE OF THE FACIAL RECOGNITION SERVICE, INCLUDING ANY DATA OR RESEARCH DEMONSTRATING THE INTENDED BENEFITS;

(4) A USE AND DATA MANAGEMENT POLICY, INCLUDING PROTOCOLS FOR:

(I) HOW AND WHEN THE FACIAL RECOGNITION SERVICE WILL BE DEPLOYED OR USED AND BY WHOM, INCLUDING:

1. THE FACTORS THAT WILL BE USED TO DETERMINE WHERE, WHEN, AND HOW THE FACIAL RECOGNITION SERVICE IS DEPLOYED, AND OTHER RELEVANT INFORMATION, INCLUDING WHETHER THE FACIAL RECOGNITION SERVICE WILL BE OPERATED CONTINUOUSLY OR USED ONLY UNDER SPECIFIC CIRCUMSTANCES; AND

2. IF THE FACIAL RECOGNITION SERVICE WILL BE OPERATED OR USED BY ANOTHER ENTITY ON THE UNIT'S BEHALF, A DESCRIPTION OF THE OTHER ENTITY'S ACCESS TO THE FACIAL RECOGNITION SERVICE AND ANY APPLICABLE PROTOCOLS;

(II) ANY MEASURES TAKEN TO MINIMIZE INADVERTENT COLLECTION OF ADDITIONAL DATA BEYOND THE AMOUNT NECESSARY FOR THE SPECIFIC PURPOSE FOR WHICH THE FACIAL RECOGNITION SERVICE WILL BE USED;

(III) DATA INTEGRITY AND RETENTION POLICIES APPLICABLE TO THE DATA COLLECTED USING THE FACIAL RECOGNITION SERVICE, INCLUDING:

1. HOW THE UNIT WILL MAINTAIN AND UPDATE RECORDS USED IN CONNECTION WITH THE FACIAL RECOGNITION SERVICE;

2. HOW LONG THE UNIT WILL KEEP THE DATA; AND

3. THE PROCESS THAT WILL BE USED TO DELETE THE DATA;

(IV) ANY ADDITIONAL RULES THAT WILL GOVERN THE USE OF THE FACIAL RECOGNITION SERVICE AND WHAT PROCESSES WILL BE REQUIRED BEFORE EACH USE OF THE FACIAL RECOGNITION SERVICE;

(V) 1. DATA SECURITY MEASURES APPLICABLE TO THE

FACIAL RECOGNITION SERVICE, INCLUDING:

A. MEASURES FOR THE SECURE STORAGE AND ACCESS OF DATA COLLECTED USING THE FACIAL RECOGNITION SERVICE; AND

B. NOTIFICATION PROCEDURES AND ACTIONS THAT WILL BE TAKEN BY THE FACIAL RECOGNITION SERVICE PROVIDER IN THE EVENT OF A SECURITY BREACH INVOLVING DATA COLLECTED USING THE FACIAL RECOGNITION SERVICE;

2. WHETHER THE UNIT INTENDS TO SHARE ACCESS TO THE FACIAL RECOGNITION SERVICE OR THE DATA FROM THE FACIAL RECOGNITION SERVICE WITH ANY OTHER ENTITY AND, IF SO, THE REASON FOR SHARING ACCESS; AND

3. THE RULES AND PROCEDURES BY WHICH A UNIT SHARING DATA WITH ANY OTHER ENTITY WILL ENSURE THAT THE OTHER ENTITY COMPLIES WITH THE UNIT'S USE AND DATA MANAGEMENT POLICY AS PART OF THE DATA SHARING AGREEMENT; AND

(VI) THE UNIT'S TRAINING PROCEDURES, INCLUDING:

1. PROCEDURES IMPLEMENTED IN ACCORDANCE WITH § 10–1709 OF THIS SUBTITLE; AND

2. HOW THE UNIT WILL ENSURE THAT ALL PERSONNEL WHO OPERATE THE FACIAL RECOGNITION SERVICE OR ACCESS ITS DATA ARE KNOWLEDGEABLE ABOUT AND ABLE TO ENSURE COMPLIANCE WITH THE USE AND DATA MANAGEMENT POLICY BEFORE USE OF THE FACIAL RECOGNITION SERVICE;

(5) THE UNIT'S TESTING PROCEDURES, INCLUDING THE UNIT'S PROCESSES FOR PERIODICALLY UNDERTAKING OPERATIONAL TESTS OF THE FACIAL RECOGNITION SERVICE IN ACCORDANCE WITH § 10–1707 OF THIS SUBTITLE;

(6) A DESCRIPTION OF ANY POTENTIAL IMPACTS OF THE FACIAL RECOGNITION SERVICE ON CIVIL RIGHTS AND LIBERTIES, INCLUDING:

(I) POTENTIAL IMPACTS ON PRIVACY AND POTENTIAL DISPARATE IMPACTS ON MARGINALIZED COMMUNITIES; AND

(II) THE SPECIFIC STEPS THE UNIT WILL TAKE TO MITIGATE THE POTENTIAL IMPACTS AND PREVENT UNAUTHORIZED USE OF THE FACIAL RECOGNITION SERVICE; AND

(7)   THE UNIT'S PROCEDURES FOR RECEIVING FEEDBACK, INCLUDING THE METHODS USED FOR RECEIVING FEEDBACK FROM INDIVIDUALS AFFECTED BY THE USE OF THE FACIAL RECOGNITION SERVICE AND FROM THE COMMUNITY AT LARGE, AS WELL AS THE PROCEDURES FOR RESPONDING TO THE FEEDBACK.

(C)   BEFORE FINALIZING AND IMPLEMENTING THE ACCOUNTABILITY REPORT, THE UNIT SHALL CONSIDER ISSUES RAISED BY THE PUBLIC THROUGH:

(1)   A PUBLIC REVIEW AND COMMENT PERIOD; AND

(2)   COMMUNITY CONSULTATION MEETINGS DURING THE PUBLIC REVIEW PERIOD.

(D)   (1)   SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, EACH UNIT SHALL UPDATE THE UNIT'S ACCOUNTABILITY REPORT EVERY 2 YEARS.

(2)   EACH UPDATE SHALL BE SUBJECT TO THE PUBLIC COMMENT AND COMMUNITY CONSULTATION MEETINGS REQUIREMENTS DESCRIBED IN SUBSECTION (C) OF THIS SECTION.

(E)   A UNIT SEEKING TO USE A FACIAL RECOGNITION SERVICE FOR A PURPOSE NOT DISCLOSED IN THE UNIT'S MOST RECENT ACCOUNTABILITY REPORT SHALL FIRST SEEK PUBLIC COMMENT AND COMMUNITY CONSULTATION ON THE PROPOSED NEW USE AND ADOPT AN UPDATED ACCOUNTABILITY REPORT IN ACCORDANCE WITH THE REQUIREMENTS OF THIS SECTION.

10–1705.

(A)   EACH UNIT USING A FACIAL RECOGNITION SERVICE SHALL PREPARE AND PUBLISH AN ANNUAL REPORT THAT DISCLOSES:

(1)   THE EXTENT OF THE UNIT'S USE OF THE FACIAL RECOGNITION SERVICE;

(2)   AN ASSESSMENT OF COMPLIANCE WITH THE TERMS OF THE UNIT'S ACCOUNTABILITY REPORT;

(3)   ANY KNOWN OR REASONABLY SUSPECTED VIOLATIONS OF THE UNIT'S ACCOUNTABILITY REPORT, INCLUDING COMPLAINTS ALLEGING VIOLATIONS; AND

(4)   ANY REVISIONS TO THE UNIT'S ACCOUNTABILITY REPORT

RECOMMENDED BY THE UNIT FOR THE NEXT UPDATE OF THE REPORT.

(B)   EACH UNIT SHALL SUBMIT THE ANNUAL REPORT REQUIRED UNDER SUBSECTION (A) OF THIS SECTION TO THE DEPARTMENT OF INFORMATION TECHNOLOGY.

(C)   EACH UNIT SHALL HOLD A COMMUNITY MEETING TO REVIEW AND DISCUSS THE ANNUAL REPORT REQUIRED UNDER SUBSECTION (A) OF THIS SECTION WITHIN 60 DAYS BEFORE THE REPORT IS SUBMITTED UNDER SUBSECTION (B) OF THIS SECTION.

10–1706.

(A)   EACH UNIT THAT USES A FACIAL RECOGNITION SERVICE TO MAKE DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING INDIVIDUALS SHALL ENSURE THAT THE DECISIONS ARE SUBJECT TO MEANINGFUL HUMAN REVIEW.

(B)   FOR THE PURPOSE OF SUBSECTION (A) OF THIS SECTION, DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING INDIVIDUALS INCLUDE:

(1)   THE DENIAL OF CONSEQUENTIAL SERVICES OR SUPPORT, INCLUDING FINANCIAL AND LENDING SERVICES, HOUSING, INSURANCE, EDUCATION ENROLLMENT, CRIMINAL JUSTICE, EMPLOYMENT OPPORTUNITIES, HEALTH CARE SERVICES, AND ACCESS TO FOOD, WATER, AND OTHER BASIC NECESSITIES; AND

(2)   DECISIONS THAT IMPACT ACCESS TO CIVIL RIGHTS OF INDIVIDUALS.

10–1707.

(A)   BEFORE A UNIT DEPLOYS A FACIAL RECOGNITION SERVICE IN THE CONTEXT IN WHICH IT WILL BE USED AND SUBJECT TO SUBSECTION (B) OF THIS SECTION, THE UNIT SHALL TEST THE FACIAL RECOGNITION SERVICE IN OPERATIONAL CONDITIONS.

(B)   THE UNIT SHALL TAKE REASONABLE STEPS TO:

(1)   ENSURE BEST–QUALITY RESULTS IN OPERATIONAL CONDITIONS BY FOLLOWING ALL REASONABLE GUIDANCE PROVIDED BY THE DEVELOPER OF THE FACIAL RECOGNITION SERVICE; AND

(2) MITIGATE ANY MATERIAL UNFAIR PERFORMANCE DIFFERENCES ACROSS SUBPOPULATIONS.

10–1708.

(A) A PROVIDER OF A FACIAL RECOGNITION SERVICE USED BY A UNIT SHALL MAKE AVAILABLE AN APPLICATION PROGRAMMING INTERFACE TO ENABLE INDEPENDENT AND REASONABLE TESTS OF THE FACIAL RECOGNITION SERVICE FOR ACCURACY AND UNFAIR PERFORMANCE DIFFERENCES ACROSS DISTINCT SUBPOPULATIONS.

(B) IF ANY UNFAIR PERFORMANCE DIFFERENCES REGARDING A FACIAL RECOGNITION SERVICE ARE IDENTIFIED THROUGH TESTING PERFORMED UNDER SUBSECTION (A) OF THIS SECTION, THE PROVIDER OF THE FACIAL RECOGNITION SERVICE SHALL DEVELOP AND IMPLEMENT A PLAN TO MITIGATE THE IDENTIFIED PERFORMANCE DIFFERENCE WITHIN 90 DAYS AFTER THE IDENTIFICATION.

10–1709.

(A) EACH UNIT THAT USES A FACIAL RECOGNITION SERVICE SHALL CONDUCT PERIODIC TRAINING OF ALL INDIVIDUALS WHO OPERATE THE FACIAL RECOGNITION SERVICE OR WHO PROCESS PERSONAL DATA OBTAINED FROM THE USE OF THE FACIAL RECOGNITION SERVICE.

(B) THE TRAINING REQUIRED UNDER THIS SECTION SHALL INCLUDE COVERAGE OF:

(1) THE CAPABILITIES AND LIMITATIONS OF THE FACIAL RECOGNITION SERVICE;

(2) PROCEDURES TO INTERPRET AND ACT ON THE OUTPUT OF THE FACIAL RECOGNITION SERVICE; AND

(3) TO THE EXTENT APPLICABLE TO THE DEPLOYMENT CONTEXT, THE MEANINGFUL HUMAN REVIEW REQUIREMENT FOR DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING INDIVIDUALS.

10–1710.

(A) A UNIT MAY NOT USE A FACIAL RECOGNITION SERVICE TO ENGAGE IN ONGOING SURVEILLANCE UNLESS:

(1) A WARRANT IS OBTAINED TO AUTHORIZE THE USE OF THE FACIAL

RECOGNITION SERVICE FOR ONGOING SURVEILLANCE ON THE BASIS OF FACTS SUBMITTED BY THE APPLICANT FOR THE WARRANT THAT:

(I)   THERE IS PROBABLE CAUSE FOR THE BELIEF THAT AN INDIVIDUAL IS COMMITTING, HAS COMMITTED, OR IS ABOUT TO COMMIT A PARTICULAR OFFENSE LISTED IN § 10–406 OF THE COURTS ARTICLE;

(II)   THERE IS PROBABLE CAUSE FOR THE BELIEF THAT PARTICULAR EVIDENCE CONCERNING THAT OFFENSE WILL BE OBTAINED THROUGH ONGOING SURVEILLANCE OF THE INDIVIDUAL; AND

(III)   NORMAL INVESTIGATIVE PROCEDURES:

1.   HAVE BEEN TRIED AND HAVE FAILED; OR

2.   REASONABLY APPEAR TO BE UNLIKELY TO SUCCEED IF TRIED OR TO BE TOO DANGEROUS;

(2)   IF THE UNIT REASONABLY DETERMINES THAT ONGOING SURVEILLANCE IS NECESSARY TO PREVENT OR RESPOND TO AN EMERGENCY INVOLVING IMMINENT DANGER OR RISK OF DEATH OR SERIOUS PHYSICAL INJURY TO AN INDIVIDUAL, WRITTEN APPROVAL IS OBTAINED FROM THE HEAD OF THE UNIT, OR THE HEAD'S DESIGNEE, BEFORE USING THE FACIAL RECOGNITION SERVICE AND A WARRANT IS SUBSEQUENTLY OBTAINED WITHIN 48 HOURS AFTER THE ONGOING SURVEILLANCE BEGINS; OR

(3)   A COURT ORDER IS OBTAINED AUTHORIZING THE USE OF THE FACIAL RECOGNITION SERVICE FOR THE SOLE PURPOSE OF LOCATING OR IDENTIFYING A MISSING PERSON OR IDENTIFYING A DECEASED PERSON.

(B)   A COURT MAY ISSUE AN EX PARTE ORDER UNDER SUBSECTION (A)(3) OF THIS SECTION IF A LAW ENFORCEMENT OFFICER CERTIFIES AND THE COURT FINDS THAT THE INFORMATION LIKELY TO BE OBTAINED IS RELEVANT TO LOCATING OR IDENTIFYING A MISSING PERSON OR IDENTIFYING A DECEASED PERSON.

(C)   A UNIT MAY NOT APPLY A FACIAL RECOGNITION SERVICE TO ANY INDIVIDUAL BASED ON THE INDIVIDUAL'S RELIGIOUS, POLITICAL, OR SOCIAL VIEWS OR ACTIVITIES, PARTICIPATION IN A PARTICULAR NONCRIMINAL ORGANIZATION OR LAWFUL EVENT, OR ACTUAL OR PERCEIVED RACE, ETHNICITY, CITIZENSHIP, PLACE OF ORIGIN, AGE, DISABILITY, GENDER, GENDER IDENTITY, SEXUAL ORIENTATION, OR OTHER CHARACTERISTIC PROTECTED BY LAW.

(D)   A UNIT MAY NOT USE A FACIAL RECOGNITION SERVICE TO CREATE A

RECORD DESCRIBING ANY INDIVIDUAL'S EXERCISE OF RIGHTS GUARANTEED BY THE FIRST AMENDMENT OF THE U.S. CONSTITUTION OR BY THE MARYLAND DECLARATION OF RIGHTS UNLESS:

      (1)   THE USE IS SPECIFICALLY AUTHORIZED BY APPLICABLE LAW AND RELATES TO AND IS WITHIN THE SCOPE OF AN AUTHORIZED LAW ENFORCEMENT ACTIVITY; AND

      (2)   THERE IS REASONABLE SUSPICION TO BELIEVE THE INDIVIDUAL HAS COMMITTED, IS COMMITTING, OR IS ABOUT TO COMMIT A SERIOUS CRIMINAL OFFENSE.

10–1711.

      (A)   IF A UNIT IS USING A FACIAL RECOGNITION SERVICE ON A CRIMINAL DEFENDANT, THE UNIT SHALL DISCLOSE THE USE TO THE CRIMINAL DEFENDANT IN A TIMELY MANNER BEFORE TRIAL.

      (B)   EACH UNIT USING A FACIAL RECOGNITION SERVICE SHALL MAINTAIN RECORDS OF ITS USE OF THE FACIAL RECOGNITION SERVICE THAT ARE SUFFICIENT TO FACILITATE PUBLIC REPORTING AND AUDITING OF COMPLIANCE WITH THE APPLICABLE ACCOUNTABILITY REPORT.

      (C)   ON OR BEFORE JANUARY 31 EACH YEAR, EACH JUDGE WHO HAS ISSUED A WARRANT FOR ONGOING SURVEILLANCE USING A FACIAL RECOGNITION SERVICE OR AN EXTENSION OF A WARRANT FOR ONGOING SURVEILLANCE USING A FACIAL RECOGNITION SERVICE THAT EXPIRED DURING THE IMMEDIATELY PRECEDING CALENDAR YEAR, OR WHO HAS DENIED APPROVAL OF A REQUEST FOR A WARRANT FOR ONGOING SURVEILLANCE USING A FACIAL RECOGNITION SERVICE DURING THE IMMEDIATELY PRECEDING CALENDAR YEAR, SHALL REPORT TO THE COURT OF APPEALS:

      (1)   THAT THE WARRANT OR EXTENSION WAS APPLIED FOR;

      (2)   THAT THE WARRANT OR EXTENSION WAS GRANTED AS APPLIED FOR, WAS MODIFIED, OR WAS DENIED;

      (3)   IF THE WARRANT WAS GRANTED, THE PERIOD FOR WHICH THE ONGOING SURVEILLANCE WAS AUTHORIZED BY THE WARRANT AND THE NUMBER AND DURATION OF ANY EXTENSIONS OF THE WARRANT;

      (4)   THE IDENTITY OF THE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER AND UNIT MAKING THE APPLICATION AND THE INDIVIDUAL AUTHORIZING

THE APPLICATION; AND

      (5)   **THE NATURE OF THE PUBLIC SPACES WHERE THE ONGOING SURVEILLANCE WAS CONDUCTED.**

      SECTION 2. AND BE IT FURTHER ENACTED, That this Act supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by a political subdivision regarding the development, use, or deployment of facial recognition services.

      SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2021.