MODEL LEGISLATION

TO IMPLEMENT

GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES

BY

THE CONSTITUTION PROJECT

The Constitution Project
1025 Vermont Avenue, NW. Third Floor
Washington, DC 20005
(202) 580-6920 (tel)
(202) 580-6929 (fax)
info@constitutionproject.org
www.constitutionproject.org

PREFACE

In May 2006, the Constitution Project's Liberty and Security Initiative released *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties,* available at www.constitutionproject.org. The Constitution Project is an independent think tank that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. The Project's Liberty and Security Initiative is guided by a bipartisan, ideologically diverse, committee of prominent Americans, who share a commitment to preserving civil liberties while enhancing security in a post-9/11 world.

In the *Guidelines for Public Video Surveillance,* the Liberty and Security Initiative examines recent developments regarding the use of Video Surveillance Systems, including rapidly advancing technology, the increased threat of terrorism, and the fact that existing legal regulations have failed to keep pace with these modern changes. The report then offers a set of guidelines to enable communities considering Video Surveillance Systems to develop a robust and effective regime that simultaneously protects the core constitutional rights and values of its residents, avoids potential liability stemming from infringement of these rights, and still permits law enforcement to fully address the real and dangerous threats of the modern world. The *Guidelines* offer practical advice to any community that has established—or is considering establishing—a video surveillance system.

The Constitution Project offers this model legislation to codify the recommendations in the *Guidelines for Public Video Surveillance.* This model code provides legislative language to enable state and local government officials to adopt these recommendations with ease. We are grateful to the Samuelson Law, Technology & Public Policy Clinic at U.C. Berkeley's Boalt Hall School of Law, for their extensive work in drafting this model legislation, and to the Public Welfare Foundation and the Community Foundation for their support of the Liberty and Security Initiative's work.

We hope that communities considering implementation of Public Video Surveillance Systems will use this model legislation in establishing such Systems in their own jurisdictions.

The Constitution Project
September 2006

PUBLIC VIDEO SURVEILLANCE SYSTEMS

ARTICLE 1
GENERAL PROVISIONS

SECTION 101. FINDINGS.

The [legislature/governing body] finds and declares as follows:

(a) Public video surveillance technology may offer communities potentially useful tools for preventing, deterring and investigating terrorism and crimes.

(b) These systems and new technologies also create the possibility of more intrusive forms of surveillance, with the potential to upset the existing balance between law enforcement needs and constitutional rights and values.

(c) Modern video surveillance must be balanced with the need to protect our core constitutional rights and values, including among others privacy and anonymity, free speech and association, government accountability, and equal protection.

(d) Lawmakers should ensure that new surveillance capabilities conform to constitutional rights and values.

SECTION 102. PURPOSE.

(a) The purpose of this [act] is to ensure that all public video surveillance systems:
    (1) further a legitimate, clearly articulated law enforcement purpose;
    (2) can effectively achieve their articulated purpose;
    (3) can achieve their articulated purpose more efficiently than could alternative means;
    (4) minimally impact constitutional rights and values;
    (5) employ an open and publicly accountable review, approval and implementation process; and
    (6) employ technological and administrative safeguards to reduce the potential for Misuse and abuse of the System.

(b) Systems that do not meet the above qualifications should not be approved.

SECTION 103. DEFINITIONS.

"Appending Data" means using technology to attach personally identifiable information, such as name, address, or criminal history, to Footage or other records of the Public Video Surveillance System such that those subsequently accessing the Footage or records can also access attached personal information.

"Automatic Identification" means use of a Public Video Surveillance System in conjunction with biometric or other digital technologies to ascertain or confirm the identity of an individual whose image is captured on Video Surveillance Footage, whether in real time, as applied to Recorded Footage, or prospectively.

"Automatic Tracking" means the use of a Public Video Surveillance System to follow a specific individual or his or her vehicle with technology operating independently of immediate or direct human control, regardless of whether his or her identity is known, so as to create a seamless record of his or her activity during a specific period.

"Community Group" means a locally-based organization representing residential, recreational, economic or other interests of those individuals living and working in the area to be surveilled and its adjacent neighborhoods.

"Governing Body" means the local elected officials accountable to the jurisdiction for which a Public Video Surveillance System is being considered. This may include, but is not limited to, such bodies as the City Council, Board of Supervisors, State Legislature, Office of the Mayor, or other Executive office.

"Harm" means physical, financial or emotional injury and is not limited to legal wrongs or violations of legal duties.

"Initial Review" means any review of Footage occurring at the same time, or within [one hour], of the occurrence of the actual events in the Video Surveillance Footage.

"Installation" shall mean an arrangement of cameras allowing them to operate without direct manual control.

"Interest Group" means an organization advancing issue-based concerns, including but not limited to civil liberties, community safety, privacy, racial justice, economic justice, needs of the homeless and seniors. Interest Groups need not be locally based.

"Misuse" means use, operation of or interaction with a PVS System in a manner inconsistent with the use restrictions described in Article III of this statute or otherwise not conforming to the approved purposes of the PVS System.

"Observation" means real-time viewing of live camera images.

"Operating Agency" means the governmental agency or other entity responsible for using and/or maintaining the Video Surveillance System. In most cases this will be the local law enforcement agency.

"Operator" means a person authorized to use the System, working for or under the supervision or control of the Operating Agency.

"Pan, Tilt, and Zoom" means manipulating a camera to view areas outside the original image frame or measurably increase the resolution of the images rendered.

"Permanent Public Video Surveillance System" or "PPVS System" means an Installation of one or more government owned and operated video cameras focused on a public place, not handheld by System Operators, implemented for an indefinite period of time or for longer than [240 days – the maximum time permitted for a Temporary Public Video Surveillance System pursuant to Section 210 of this model legislation], and the primary purpose of which extends beyond a single, specific law enforcement investigation.

"Public Video Surveillance System" or "PVS System" or "System" means one or more government owned and operated cameras focused on a public place and remotely operated.

"Recorded" refers to images that are preserved and stored by a Public Video Surveillance System for later review. This includes preservation for any length of time beyond a short window necessary to perform an "Initial Review" of the Footage.

> ***Legislative Note:*** *This definition is intended to permit camera monitors to quickly re-wind and re-play Footage, or to quickly review Footage that is temporarily Recorded during a one-hour lunch break (see one hour period in definition of "Initial Review"), without considering that Footage Recorded, provided that the images are not preserved beyond that one-hour time period.*

"Reviewer" means the "Governing Body" or a commissioner or commission appointed by the Governing Body that reviews proposals and executes the "Impact Assessment" pursuant to Sections 202 - 209.

"Secondary Purpose" means an intentional, planned use of a System, a component of it, or the collected data, for a purpose other than an original approved purpose for the System.

"Targeted Public Consultation" means the process of meeting and conferring with a cross section of "Community Groups" and "Interest Groups" for the purpose of seeking guidance on the design of a Public Video Surveillance System, Section 206.

"Temporary Public Video Surveillance System" or "TPVS System" means a Public Video Surveillance System not considered a Permanent Public Video Surveillance System.

"Third Parties" means individuals or entities (other than the individual requesting access to records relating to his or her self) that are not under the supervision or control of the Operating Agency.

"Video Surveillance Footage" or "Surveillance Footage" or "Footage" means any images Recorded by a Public Video Surveillance System including time and location data and any additional metadata or information appended to the images on the Footage.

ARTICLE 2
PROCEDURES FOR REVIEW, APPROVAL, AND IMPLEMENTATION OF PUBLIC VIDEO SURVEILLANCE SYSTEMS

PART 1. PUBLIC VIDEO SURVEILLANCE SYSTEMS - AUTHORITY TO REVIEW, APPROVE AND IMPLEMENT.

SECTION 201. AUTHORITY TO REVIEW, APPROVE AND IMPLEMENT PVS SYSTEMS.

(a) The Governing Body shall retain non-delegable authority to approve implementation of Permanent Public Video Surveillance Systems. Law enforcement, a member of the public, or the Governing Body itself may initially suggest implementation of a Permanent Public Video Surveillance System. To draft the formal proposal to implement such a System, the Governing Body may, at its option:

(1) appoint an independent commissioner or commission to draft proposals for Public Video Surveillance Systems and execute Impact Assessments; or

(2) retain authority to draft proposals and execute Impact Assessments.

(b) Operators of prospective Temporary Public Video Surveillance (TPVS) Systems may seek approval of the Governing Body through the Impact Assessment, Sections 203-209, or pursuant to an order from a court of competent jurisdiction in accordance with the provisions of Section 210 (Approval of Temporary Public Video Surveillance Systems).

PART 2. PERMANENT PUBLIC VIDEO SURVEILLANCE SYSTEMS - IMPACT ASSESSMENT REQUIRED.

SECTION 202. IMPACT ASSESSMENT REQUIRED FOR PERMANENT PUBLIC VIDEO SURVEILLANCE SYSTEMS.

(a) Except as provided in Section 212 (Systems with Limited Technological Capabilities), no Permanent Public Video Surveillance (PPVS) System shall be approved or installed unless a completed Impact Assessment, Sections 203-209 (PVS Impact Assessment), is on file with the Governing Body.

(b) The Impact Assessment shall serve as the evaluative basis for all decisions to approve and implement Permanent Public Video Surveillance Systems.

PART 3. PUBLIC VIDEO SURVEILLANCE IMPACT ASSESSMENT.

SECTION 203. PUBLIC VIDEO SURVEILLANCE IMPACT ASSESSMENT.

(a) The PVS Impact Assessment shall consist of five steps:

(1) PVS proposal, Section 204.

(2) Public input on PVS Proposal, Section 205.

(3) Draft PVS Impact Report, Section 208.
(4) Period of Public Comment on Draft PVS Impact Report, Section 207.
(5) Final PVS Impact Report, Section 209.

(b) Impact Assessment proceedings shall be subject to the [state public records act, open meetings laws, sunshine acts in jurisdiction]. Meetings held pursuant to Targeted Public Consultation, Section 206, need not be open to the public, but still must meet the public disclosure requirements specified in section 206(b) (Targeted Public Consultation).

SECTION 204. PVS PROPOSAL.

(a) Initial Proposal Required. The Impact Assessment of a PVS System begins with an initial proposal outlining the intended purpose and scope of the System, prepared by the Reviewer.

(b) The proposal shall include:
(1) articulation of the legitimate law enforcement purposes that justify the System; and
(2) details of the technological design and geographical scope of the System, including locations on which cameras are to be focused, the visual coverage of the System, and the proposed technical specifications of the entire System.
(c) Proposals detailing Systems that exhibit limited technological capabilities as described in Section 212 shall be subject to the review processes described therein, and need only comply with the remainder of the PVS Impact Assessment, Sections 205-209, to the extent noted in Section 212.

Legislative Note: *This model statute does not specify standards for whom or what agencies can suggest a PVS System. Rather, provision (a) provides that whether law enforcement, another government agency or a citizens' group initially suggests a PVS System, the Reviewer shall be responsible for drawing up a proposal that details its intended purpose and scope. This insures that descriptions of planned Systems will be sufficiently detailed that they can be effectively evaluated by members of the public.*

SECTION 205. PUBLIC INPUT REQUIRED.

(a) Public input is required on the PVS Proposal and will inform the Draft PVS Impact Report. The Reviewer shall solicit public input on the PVS Proposal through either Targeted Public Consultation, Section 206, or a period of Public Comment, Section 207.

(b) A period of Public Comment on the Draft PVS Impact Report is required and will inform the Final PVS Impact Report.

SECTION 206. TARGETED PUBLIC CONSULTATION.

(a) Targeted Public Consultation shall consist of meetings or other communication offering a broad cross-section of community and Interest Groups the opportunity to review and comment on the PVS proposal.

(b) The Reviewer shall make public
    (1) a list of entities and individuals participating in targeted consultations;
    (2) all documents passed between community and Interest Groups and the Reviewer during the targeted consultation process; and
    (3) summary notes of meetings taken as a part of the Targeted Public Consultation process.

SECTION 207. PUBLIC COMMENT.

(a) The Reviewer shall facilitate public comment.

(b) The report or proposal on which comment is sought shall be made available to the public via local government print and electronic publications. Local press outlets shall be notified and local regulations with respect to public hearings and soliciting public comments shall apply.

(c) The Reviewer shall provide a reasonable period of time for meaningful public comment. This time period shall be at least [60] days.

(d) Public comment shall include opportunity for members of the public to submit written comments and at least one public hearing held in accordance with relevant local regulations for public hearings.

(e) The Reviewer will compile a complete written record of public comment.

(f) Following the period of public comment:
    (1) If comments applied to the PVS Proposal, the Reviewer will prepare the Draft PVS Impact Report, Section 208.
    (2) If comments applied to the Draft PVS Impact Report, the Reviewer will revise the report in light of public comments, including altering recommendations if appropriate. The Reviewer will then submit the revised report and indexed public comments to the Governing Body to facilitate decision-making.

Legislative Note: *Public Comment on the PVS Proposal is optional, and may be substituted for by Targeted Public Consultation, see Section 205(a) and 206, supra. Public Comment on the Draft PVS Impact Report is mandatory, see Section 205(b), supra, and 208, infra.*

SECTION 208. DRAFT PVS IMPACT REPORT.

(a) Following the Targeted Public Consultation or public comment required under section 205 (Public Input Required), the Reviewer shall prepare and make available to the public a comprehensive report to be known as the Draft PVS Impact Report.

(b) The Draft PVS Impact Report shall address specific issues raised by the public during consultation or comment and shall include:
    (1) Articulation and evaluation of the legitimate law enforcement purposes that justify the System.
    (2) Details of the technological design and geographical scope of the System, including locations to be surveilled, the visual coverage of the System, and the proposed technical specifications of the System.
    (3) Analysis of whether and how the proposed System will effectively address its purposes.
    (4) Assessment of the proposal's cost, including initial outlay, projected maintenance expenses and personnel costs.
    (5) Comparison of the cost and utility of the System to alternative means of attaining the same purpose.
    (6) Analysis of the impact of the System on constitutional rights and values, including:
        (i) privacy and anonymity;
        (ii) freedom of speech and association;
        (iii) government accountability;
        (iv) due process;
        (v) equal protection.
    (7) Assessment of potential incidental costs or benefits of the System and their likelihood.
    (8) Analysis of possible "spillover effects," or consequences of the System for areas not surveilled, including the possibilities of crime increases in adjacent neighborhoods.
    (9) With the foregoing factors in mind, an overall cost-benefit analysis of the proposed System. This may include, where appropriate, an analysis of the PVS experiences of similar cities or cities with similar Systems, including relevant similarities or differences of those cities and their Systems.
    (10) A recommendation to guide the decision of the Governing Body.

(c) All communications material to the Reviewer's recommendation, including all communications with outside individuals and groups, shall be introduced on the record in the Draft PVS Impact Report.

SECTION 209. FINAL PVS IMPACT REPORT.

(a) Based on the Draft PVS Impact Report, the Targeted Consultation and the public comment period(s), the Governing Body will determine whether to approve, modify or reject the proposed PVS System within a reasonable span of time. In order to

facilitate its decision, the Governing Body may request from the Reviewer, community and Interest Groups or government agencies additional information about potential costs, benefits or effects of the System, or may choose to hold a public hearing.

(b) The Governing Body will modify the revised Draft PVS Impact Report as appropriate and issue it publicly as a Final PVS Impact Report. This report will include a section stating the Governing Body's final decision and the basis for that decision. All communications material to the Governing Body's final decision, including all communications with outside individuals and groups, shall be introduced on the record in the Final PVS Impact Report.

PART 4. TEMPORARY PUBLIC VIDEO SURVEILLANCE SYSTEMS - APPROVAL BY IMPACT ASSESSMENT OR COURT ORDER.

SECTION 210. APPROVAL OF TEMPORARY PUBLIC VIDEO SURVEILLANCE SYSTEMS.

(a) Approval for a Temporary Public Video Surveillance (TPVS) System may be sought through the Impact Assessment, Sections 203-209, or pursuant to an order from a court of competent jurisdiction. Each application for a court order authorizing Temporary Public Video Surveillance shall be made in writing upon oath or affirmation of the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons].

(b) Applications for a court order shall state or describe each of the following:
   (1) the identity of the individual making the application, and of the [Operating Agency] that is to execute the order;
   (2) the law enforcement purposes of the proposed System, and how the Surveillance System is likely to produce evidence useful in serving these purposes;
   (3) other means attempted or considered to investigate or combat the crimes at issue, and explanations of why they have been or are likely to be unsuccessful or impractical;
   (4) reasons the purpose of the System would be frustrated by the Impact Assessment process;
   (5) the time period for which the System is to be deployed, which shall not exceed [120 days];
   (6) the places and activities to be surveilled, and a description of why surveillance of those locations is expected to further law enforcement objectives; and
   (7) any protections or safeguards incorporated into the System design to minimize the intrusion into the constitutional rights and values of individuals whose images will be captured by the surveillance.

(c) The court shall grant a "Temporary Video Surveillance Order" if it is persuaded that:

(1) the articulated law enforcement purposes of the System are legitimate;
(2) the Surveillance System is likely to produce evidence useful in serving these purposes;
(3) the planned surveillance could reasonably be considered likely to be more effective or less dangerous than other available means of investigating or combating the crimes at issue;
(4) there is a public interest in rapid deployment or secrecy of the TPVS System that would be compromised by the public comment process;
(5) the proposed System will be deployed for a limited time no longer than reasonably necessary to achieve the stated objectives, and not exceeding [120 days];
(6) the System will feature no greater scope or capabilities than reasonably necessary to achieve a legitimate law enforcement purpose;
(7) surveillance of the stated locations is reasonably necessary to further the System's legitimate law enforcement objectives; and
(8) reasonable protections and safeguards will be taken to minimize intrusion into the constitutional rights and values of individuals whose images will be captured by the surveillance but who are not suspected of criminal activity.

(d) When amendments to System design could allow a proposed System to meet the above requirements and still fulfill the purpose of the System, courts may require such amendments rather than reject applications for TPVS outright.

(e) A court approving a TPVS System will issue a "Temporary Video Surveillance Order," specifying the time period and locations to be surveilled.

(f) The Operator may file a time period extension request with a court of competent jurisdiction, which may at its discretion require evidence demonstrating need or issue a written judgment on the basis of the written request.
(1) The time period covered by the extension shall not exceed [the maximum number of days specified in Subsection (c)(5) above. 120 in this model statute].
(2) No requests for extensions shall be granted that will result in a TPVS System operating for more than [the maximum number of days specified in Subsection (c)(5) above, plus the maximum extension period. This shall be the maximum number of days allowed for operation before a temporary System will be considered a permanent System for purposes of this statute. 240 days in this model statute.] total days.
(i) A System shall be considered in operation from the day it is first turned on for use until the day it is permanently turned off to be dismantled. Interim periods during which the System may be temporarily turned off count as time in which the System is in operation, and count against the maximum number of days available for a System to be considered temporary.
(ii) Systems operated longer than [the maximum TPVS period - 240 days in this model statute] shall be considered permanent Systems

for the purposes of this statute, and shall be subject to the requirements of Subsection (f)(3) of this Section.

(3) Operators seeking to extend the operation of a TPVS System beyond the maximum period of days must

(i) prior to the expiration of the maximum period set forth in Subsection (f)(2), apply to the court for a second extension to cover the time period necessary for completing the Impact Assessment process under Sections 203-209.

(ii) seek approval of the System through the Impact Assessment process set forth in Sections 203 - 209.

(4) Temporary Systems initially approved under the Impact Assessment (rather than by court order), and now seeking approval as permanent Systems, shall be considered to have changed their purpose, and shall be reviewed in accordance with the provisions of Section 215, Change in Purpose of Public Video Surveillance System.

Legislative Note: *As above with respect to Automatic Identification, localities should feel free to adapt this Section to conform to state or local rules or practices regarding obtaining warrants or other court orders.*

SECTION 211. APPROVAL OF TEMPORARY PUBLIC VIDEO SURVEILLANCE SYSTEMS UNDER EXIGENT CIRCUMSTANCES.

(a) Upon informal application by the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons], a [judge of competent jurisdiction] may grant oral approval for a Temporary Public Video Surveillance System, without an order, if he or she determines all of the following:

(1) There are grounds upon which an order could be issued under this chapter.

(2) There is probable cause to believe that an emergency situation exists.

(3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate public video surveillance before an application for an order could with due diligence be submitted and acted upon.

(b) If the person seeking oral approval for public video surveillance under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such person may authorize and proceed with the emergency employment of a Temporary Public Video Surveillance System without an order, if he or she determines all of the following:

(1) There are grounds upon which an order could be issued under this chapter.

(2) There is probable cause to believe that an emergency situation exists.

(3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate Automatic Identification or

Tracking before an application for an order could with due diligence be submitted and acted upon.

(c) Approval for a Temporary Public Video Surveillance System under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval under subsection (a) of this section or a determination under subsection (b) of this Section, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under subsection (a) or determination under subsection (b) and be retroactive to the time of such oral approval or determination.

PART 5. SYSTEMS WITH LIMITED TECHNOLOGICAL CAPABILITIES - ALTERNATIVE IMPACT ASSESSMENT AVAILABLE.

SECTION 212. ALTERNATIVE IMPACT ASSESSMENT FOR PVS SYSTEMS WITH LIMITED TECHNOLOGICAL CAPABILITIES.

(a) The Governing Body may elect to perform an Alternative Impact Assessment in place of the PVS Impact Assessment if and only if the Reviewer concludes in the PVS Proposal that the System incorporates the following safeguards:
   (1) Data gathered by the Video Surveillance System is automatically deleted after [96 hours] (or earlier), unless specific data is requested by law enforcement pursuant to Section 314.
   (2) The Video Surveillance System does not have Automatic Tracking or Identification capabilities.
   (3) Data gathered by the Video Surveillance System is protected by adequate data security measures for the duration of its retention, pursuant to Section 325.
   (4) The video surveillance data is unavailable to Third Parties except as provided in Sections 315, 320-324.

(b) The Alternative Impact Assessment shall include:
   (1) A combined PVS Proposal and Draft PVS Impact Report, Sections 204 and 208. The Draft Report may *exclude* the assessment of "potential incidental costs or benefits of the System and their likelihood" otherwise required pursuant to Section 208(b)(7).
   (2) A period of Public Comment, Section 207,
   (3) A Final PVS Impact Report, Section 209.

(c) The Alternative Impact Assessment need not include Targeted Public Consultation.

Legislative Note: *The Alternative Impact Assessment thus consolidates the PVS Proposal and the Draft PVS Impact Report. The Reviewer may simultaneously author both the Proposal and Draft Report, forego Targeted Public Consultation, and advance immediately to Public Comment. This should save significant time and resources, and provides an incentive for jurisdictions to consider limiting their Systems' technological capacity. This in turn helps safeguard the*

Constitutional interests of citizens. Note also that one example of data security measures would be encryption at the moment of recording.

PART 6. EXISTING SYSTEMS - PERIODIC AUDITS REQUIRED, REVIEW IN CASE OF MISUSE OR HARM, ALTERATIONS OR CHANGE IN PURPOSE.

SECTION 213. PERIODIC AUDITS REQUIRED.

(a) The Reviewer will conduct a periodic review of implemented PVS Systems to assess each System's effectiveness, impact on the community, and adherence to the System's stated primary purpose.
   (1) The Reviewer will publicly announce its intention to conduct an audit and provide instructions as to how individuals and organizations can submit comments or seek meetings.
   (2) The Reviewer is not obligated to hold public hearings or to solicit meetings with community and Interest Groups.
   (3) The Reviewer will accept written comments submitted by members of the public and will grant meetings to community and Interest Groups upon request as appropriate.
   (4) The Reviewer will consult the Operating Agency, System records, complaints, disciplinary records and other records to determine the extent to which the System has:
      (i) assisted law enforcement in advancing the purposes for which the PVS was established;
      (ii) been Misused; or
      (iii) been used for Secondary Purposes.
   (5) In light of the Reviewer's findings and comments submitted, the Reviewer (if separate from the Governing Body) will recommend to the Governing Body whether to renew, cancel or alter the System.
   (6) The Governing Body will issue a public report stating its decision to renew, cancel or alter the System in order to resolve or ameliorate problems identified by the audit. The report will detail the reasons for its decision, with specific references to the Reviewer's findings and conclusions and comments submitted. Decisions to significantly alter the System by removing key limitations on its technological capacity or otherwise significantly increasing its potential for invasive use are subject to immediate review under the Alternative Impact Assessment.

(b) The reviewing period will be established by the Governing Body and will not exceed [a reasonable time period to be established by the jurisdiction, but no longer than two years] between reviews.

SECTION 214. SYSTEMS ALREADY IN EXISTENCE AT PASSAGE OF THIS ACT.

Pre-existing PVS Systems shall be reviewed in accordance with procedures for periodic audits, Section 213, and must undergo such a review within one year of adoption of this Act.

SECTION 215. CHANGE IN PURPOSE OF PUBLIC VIDEO SURVEILLANCE SYSTEM.

(a) If the primary law enforcement purpose of a PVS System changes, it shall be immediately reviewed under the Alternative Impact Assessment under Section 212.

(b) A change in purpose may be found either:
  (1) explicitly, where a new purpose for the Public Video Surveillance System is announced by the Operator; or
  (2) implicitly, where during review under Section 213, 214, 216 or 217, it comes to the Reviewer's attention that requests for access to or retention of Footage for legitimate law enforcement Secondary Purposes occur with approximately equal or greater frequency than requests serving the System's primary purpose.

SECTION 216. REVIEW REQUIRED IN CASES OF MISUSE AND HARM.

(a) A PVS System shall be subject to an immediate audit when credible evidence is brought to the attention of the Governing Body or Reviewer demonstrating:
  (1) use or Misuse of a PVS System by any individual(s) resulting in grave Harm to a person when such Harm is not the necessary and legitimate outcome of a legitimate law enforcement investigation; or
  (2) repeated and similar instances of use or Misuse of a PVS System by multiple Operators resulting in Harm to others when such Harm is not the necessary and legitimate outcome of a legitimate law enforcement investigation.

(b) Pending results of the audit, the Governing Body shall have the discretion to suspend the System.

(c) The Reviewer will examine features of the System contributing to Misuse and consult with legal and technical experts, community and Interest Groups, or others as appropriate.

(d) The Reviewer shall issue a public report of findings and recommendations, except that certain findings may remain confidential to the extent necessary to protect ongoing investigations.

(e) The Governing Body will consider the recommendations in determining whether to alter or cancel the System, and whether to refer the matter for disciplinary action.

Legislative Note: *The criteria above are intended primarily to encapsulate two scenarios. The first is action by a single individual resulting in serious Harm to others. This would indicate that the System has the capacity to do serious Harm when Misused, and thus should be reviewed for means to reduce this Harm. The second scenario envisions multiple occurrences of similar types of abuse or Misuse. Even if the individual incidents do not result in especially serious Harm to individuals, the repetitive nature of the Misuse may indicate a flaw in the System that ought to be remedied.*

Relevant factors in determining whether to suspend, alter or cancel the System may include whether the alleged abuse is likely to continue and to be sufficiently pervasive or serious to outweigh the benefits of maintaining operation.

SECTION 217. REVIEW REQUIRED AFTER ALTERATIONS TO EXISTING SYSTEMS.

When alterations are made to a technologically limited PVS System approved under the Alternative Impact Assessment, Section 212, and the alterations remove technological limitations permitting the System to qualify for the Alternative Impact Assessment, the altered System shall be immediately subject to a PVS Impact Assessment, Sections 203-209.

PART 7. SANCTIONS; COMPLIANCE WITH REVIEW PROCESS.

SECTION 218. ENFORCEMENT BY STATE ATTORNEY GENERAL.

(a) The state Attorney General or equivalent state review panel shall be empowered to investigate and review failures to comply with the provisions of this article, and to issue orders for compliance.

(b) Upon a finding of failure to comply, the state may withhold funds from the Operating Agency until compliance is attained.

SECTION 219. PRIVATE RIGHT OF ACTION.

(a) Any resident of the jurisdiction subject to the authority of the Governing Body may commence a civil action on his or her own behalf against the Governing Body for failure to comply with the provisions of this article.

(b) Remedies available to such a plaintiff shall include:
    (1) Issuance of an injunction limiting or barring further use of the Surveillance System until compliance is achieved.
    (2) Provision of reasonable attorney's fees.

Legislative Note: *Nothing in this legislation prohibits plaintiffs claiming injuries caused by use or Misuse of a PVS System from introducing failure to comply with the provisions of this article as evidence.*

ARTICLE 3
USE RESTRICTIONS

PART 1. RESTRICTED USE OF RECORDING, AUTOMATIC IDENTIFICATION, AUTOMATIC TRACKING, AND PAN, TILT, AND ZOOM.

SECTION 301. SPECIFICATIONS OF SYSTEM.

Public Video Surveillance Systems shall conform to the specifications outlined in a Final PVS Impact Report under Section 209 or court order under Section 210.

> ***Legislative Note:*** *Although careful planning and analysis of a Public Video Surveillance System's technical specifications is important, it is also essential that the System as built conforms to those specifications.*

SECTION 302. AUTOMATIC IDENTIFICATION PROHIBITED ABSENT AUTHORIZATION.

Except as provided in Sections 303, 309, and 310, using a Public Video Surveillance System for purposes of Automatic Identification is prohibited.

> ***Legislative Note:*** *The use of Automatic Identification technology raises specialized concerns regarding constitutional rights and values. Even in public, most people expect to remain anonymous unless they are seen, recognized, and remembered by another individual present in that location. Pervasive use of automated identification undermines this expectation—implicating privacy, anonymity, and First Amendment freedoms. Thus, use of Automatic Identification should be permissible only after obtaining a court order in accordance with the rules and procedures set forth in Section 303 or pursuant to the exigency and federal counterterrorism exceptions in Section 309 and 310.*

SECTION 303. ORDER AUTHORIZING AUTOMATIC IDENTIFICATION.

(a) Each application for an order authorizing Automatic Identification using a Public Video Surveillance System shall be made in writing upon oath or affirmation of the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons] to [a judge of competent jurisdiction]. Each application shall include all of the following information:

(1) the identity of the individual making the application, and of the [Operating Agency] that is to execute the order;

(2) a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including:

(i) details regarding the particular offense that has been, is being, or is about to be committed;

(ii) a particular description of the location or locations of such offense; and

(iii) the identity, if known, or a description of the person(s) believed to be involved in the commission of the offense and who is (are) to be identified;

(3) a statement of the period of time over which the Automatic Identification is to be performed, including whether the identification is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both;

(4) a full and complete statement of the facts concerning all previous applications for Automatic Identification known to the individual authorizing and making the application involving any of the same persons or particular offenses specified in the application, and the action taken by the judges on these applications; and

(5) if the application is for the extension of an order authorizing Automatic Identification, a statement setting forth the results of the Automatic Identification under the original order, or a reasonable explanation of the failure to obtain results.

(b) The judge may require the applicant to furnish additional testimony or documentary evidence in support of an application for an order under this Section.

(c) Upon application made under this Section, the judge may enter an ex parte order, as requested or modified, authorizing Automatic Identification within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

(1) There is probable cause to believe that an individual is committing, has committed, or is about to commit an offense, the investigation and/or prevention of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report, or use for an approved Secondary Purpose, if the required showing under Section 317 has also been made.

(2) There is probable cause to believe that evidence of or information about that crime or the individual who is suspected of committing or planning that crime will be obtained through the use of Automatic Identification as described in the application.

(3) Other investigative techniques have been tried and were unsuccessful, or such techniques reasonably appear to be unlikely to succeed or to be impractical.

(d) *Time Period Authorized:* For requests for Automatic Identification covering already existing Footage, the application must justify the time period contained within the request to demonstrate that it serves the purposes outlined under Subsection (c) of this Section. For requests for Automatic Identification on Footage that has not yet been Recorded, the maximum authorized time period for Automatic Identification shall be 30 days (measured either in real time or in duration of Recorded Footage). Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (a) of this Section, and upon the court making findings

required by subsection (c) of this Section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event any longer than 30 days.

(e) Each order authorizing Automatic Identification shall specify all of the following:
    (1) a particular description of the person(s) to be automatically identified;
    (2) a description of the location(s) of the camera(s) or of the location(s) depicted in the Footage on which the Automatic Identification is to be performed;
    (3) the identity of the [Operating Agency] authorized to perform the Automatic Identification; and
    (4) the period of time during which such Automatic Identification is authorized, including whether the identification is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both, and if the order is for extension of a previous order, the period of time during which Automatic Identification has already been performed.

Legislative Note: *Localities should adapt this Section as appropriate to conform to state or local rules or practices regarding obtaining warrants or other court orders.*

SECTION 304. APPENDING DATA TO PUBLIC VIDEO SURVEILLANCE FOOTAGE PROHIBITED.

Except as provided in Section 305, Appending Data to public Video Surveillance Footage is prohibited.

SECTION 305. OPERATOR GUIDELINES FOR APPENDING DATA.

(a) The Operating Agency shall promulgate clear and specific guidelines detailing the situations in which it is appropriate to append data to public Video Surveillance Footage, provided that no Automatic Identification may be performed except pursuant to the terms of Section 303. The Operating Agency may provide for less stringent standards for appending identification data obtained through personal Observation or other non-automated methods.

(b) Any Operator who violates the Operator's guidelines for Appending Data to public Video Surveillance Footage shall be subject to administrative discipline under Section 328.

SECTION 306. NOTIFICATION OF INDIVIDUALS SUBJECT TO IDENTIFICATION ON SURVEILLANCE FOOTAGE.

(a) Within a reasonable time, but no later than 90 days, after the termination of the period of an order authorizing Automatic Identification or extensions thereof, or after personally identifiable information about an individual has been appended to Video Surveillance Footage, the Operating Agency shall serve upon persons who have been

identified in Surveillance Footage an inventory which shall include notice of all of the following:

(1) The fact of entry of the order or appending of identifying information.

(2) The date of the entry of the order or appending of information, and the period of time covered by the order or Footage.

(b) The judge, upon the filing of a motion, may, in his or her discretion, make available to the person identified or his or her counsel for inspection the portions of Footage on which Automatic Identification techniques have been performed, and any information resulting from the Automatic Identification, which the judge determines to be in the interest of justice.

(c) On an ex parte showing of a legitimate law enforcement purpose to a judge, the serving of the report required by this section may be postponed. The period of postponement shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted.

(d) A criminal defendant shall be notified that he or she was identified as a result of Automatic Identification that was performed pursuant to this chapter. The notice shall be provided prior to the entry of a plea of guilty or nolo contendere, or at least 20 days prior to any trial, hearing, or proceeding in the case other than an arraignment or grand jury hearing; provided that if the defendant would otherwise be entitled to receive such information earlier under state rules of criminal procedure, the earlier disclosure requirements shall apply.

Legislative Note: *Reports of instances of Automatic Tracking are not subject to this notice requirement, to the extent that Automatic Tracking occurs without Automatic Identification. If Automatic Identification occurs in conjunction with Automatic Tracking, the notice obligation would apply.*

SECTION 307. AUTOMATIC TRACKING.

Except as provided in Sections 308, 309, and 310, using a Public Video Surveillance System for purposes of Automatic Tracking or Appending Data to public Video Surveillance Footage is prohibited.

SECTION 308. ORDER AUTHORIZING AUTOMATIC TRACKING.

(a) Each application for an order authorizing Automatic Tracking using a Public Video Surveillance System shall be made in writing upon oath or affirmation of the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons] to [a judge of competent jurisdiction]. Each application shall include all of the following information:

(1) the identity of the individual making the application, and of the [Operating Agency] that is to execute the order;

(2) a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including:
    (i) details regarding the particular offense that has been, is being, or is about to be committed;
    (ii) a particular description of the location or locations of such offense; and
    (iii) the identity, if known, or a description of the person(s) believed to be involved in the commission of the offense and who is (are) to be tracked;
(3) a statement of the period of time over which the Automatic Tracking is to be performed, whether the Automatic Tracking is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both;
(4) a full and complete statement of the facts concerning all previous applications for Automatic Tracking known to the individual authorizing and making the application involving any of the same persons or particular offenses specified in the application, and the action taken by the judges on these applications; and
(5) if the application is for the extension of an order authorizing Automatic Tracking, a statement setting forth the results of the Automatic Tracking under the original order, or a reasonable explanation of the failure to obtain results.

(b) The judge may require the applicant to furnish additional testimony or documentary evidence in support of an application for an order under this Section.

(c) Upon application made under subsection (a) of this Section, the judge may enter an ex parte order, as requested or modified, authorizing Automatic Tracking within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:
    (1) There is probable cause to believe that an individual is committing, has committed, or is about to commit an offense, the investigation and/or prevention of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report, or use for an approved Secondary Purpose, if the required showing under Section 317 has also been made.
    (2) There is probable cause to believe that evidence of or information about that crime or the individual who is suspected of committing or planning that crime will be obtained through the use of Automatic Tracking as described in the application.
    (3) Other investigative techniques have been tried and were unsuccessful, or such techniques reasonably appear to be unlikely to succeed or to be impractical.[0]

(d) *Time Period Authorized:* For requests for Automatic Tracking covering already existing Footage, the application must justify the time period contained within the request to demonstrate that it serves the purposes outlined under Subsection (c) of this Section. For requests for Automatic Tracking on Footage that has not yet been Recorded, the maximum authorized time period for Automatic Tracking shall be 30

days (measured either in real time or in duration of Recorded Footage). Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (a) of this Section, and upon the court making findings required by subsection (c) of this Section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event any longer than 30 days.

(e) Each order authorizing Automatic Tracking shall specify all of the following:
    (1) a particular description of the person(s) to be automatically tracked;
    (2) a description of the location(s) of the camera(s) or of the location(s) depicted in the Footage on which the Automatic Tracking is to be performed;
    (3) the identity of the [Operating Agency] authorized to perform the Automatic Tracking; and
    (4) the period of time during which such Automatic Tracking is authorized, including whether the Automatic Tracking is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both, and if the order is for extension of a previous order, the period of time during which Automatic Identification has already been performed.

Legislative Note: *As above with respect to Automatic Identification, localities should adapt this Section as appropriate to conform to state or local rules or practices regarding obtaining warrants or other court orders.*

SECTION 309. AUTOMATIC IDENTIFICATION OR AUTOMATIC TRACKING UNDER EXIGENT CIRCUMSTANCES.

(a) Upon informal application by the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons], a [judge of competent jurisdiction] may grant oral approval for Automatic Identification or Automatic Tracking, without an order, if he or she determines all of the following:
    (1) There are grounds upon which an order could be issued under this chapter.
    (2) There is probable cause to believe that an emergency situation exists.
    (3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate Automatic Identification or Automatic Tracking before an application for an order could with due diligence be submitted and acted upon.

(b) If the individual seeking oral approval for Automatic Identification or Automatic Tracking under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such individual may authorize and proceed with the emergency employment of Automatic Identification or Automatic Tracking without an order, if he or she determines all of the following:
    (1) There are grounds upon which an order could be issued under this chapter.
    (2) There is probable cause to believe that an emergency situation exists.

(3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate Automatic Identification or Automatic Tracking before an application for an order could with due diligence be submitted and acted upon.

(c) Approval for Automatic Identification or Automatic Tracking under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval under subsection (a) of this section or a determination under subsection (b) of this Section, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under subsection (a) or determination under subsection (b) and be retroactive to the time of such oral approval or determination.

SECTION 310. AUTOMATIC IDENTIFICATION OR AUTOMATIC TRACKING PURSUANT TO A FEDERAL COUNTERTERRORISM WATCHLIST.

Notwithstanding Sections 302 and 307, an Operating Agency may engage in Automatic Identification and/or Automatic Tracking pursuant to a federal counterterrorism watch list that is part of the Terrorist Screening Database maintained by the federal Terrorist Screening Center (TSC).

> ***Legislative Note:*** *We recommend creating this exception to the prohibition on Automatic Identification and Automatic Tracking for the use of anti-terrorism watch lists compiled by the federal government. This recommendation is based upon the national security and secrecy concerns underlying the federal lists as well as the practical concern that local officials likely would not be permitted access to the underlying data they would need to justify judicial approval. This exception does not apply to any other watch lists, regardless of source.*

SECTION 311. PAN, TILT, OR ZOOM PROHIBITED ABSENT REASONABLE SUSPICION OF CRIMINAL ACTIVITY .

(a) The Operator shall not use the Pan, Tilt, or Zoom features of a video surveillance camera or System in a way that targets particular individuals absent a reasonable suspicion of criminal activity.

(b) The Operating Agency shall promulgate guidelines for the use of Pan, Tilt, or Zoom features of cameras to prevent use of such features in a way that discriminates against individuals on the basis of race, ethnic origin, religion, age, gender, class, economic status, or sexual orientation.

SECTION 312. SYSTEMS APPROVED FOR LIVE OBSERVATION ONLY.

(a) Public Video Surveillance Systems approved, according to Article I of this [act], solely for live Observation shall not retain Footage or other data, except for a short

period of time during which an Operator performs an Initial Review of Footage, or as required by Section 327.

(b) Where a Public Video Surveillance System is capable of recording upon request or instruction of the Operator, the Operating Agency shall promulgate guidelines which limit the circumstances under which recording is permitted, consistent with the purpose of the System as articulated by the [Governing Body] in its Final PVS Impact Report, Section 209.

Legislative Note: *This Section applies to all Systems that are only approved for live Observation, regardless of the method of review undertaken (Impact Assessment, Alternative Impact Assessment, or court order). Put simply, if a System is not approved for recording, it should not be capable of recording.*

SECTION 313. PRE-ARCHIVAL AND ARCHIVAL FOOTAGE; RETENTION PERIOD.

(a) Operating agencies implementing Public Video Surveillance Systems approved for and capable of recording shall designate an initial period during which retained Recorded Footage is considered pre-archival for purposes of Sections 314 and 316-317. The specification of this period shall be based on the Operating Agency's actual practice for completing routine reviews of Recorded Footage, and shall not exceed 7 days.

(b) All Footage retained beyond the pre-archival period as specified under subsection (a) of this Section shall be considered archival for purposes of Sections 314 and 316-317.

(c) All Footage and accompanying data must be automatically deleted after expiration of 7 days, unless:
  (1) Footage is specifically requested for extended retention under Section 314; or
  (2) retention of Footage or information is required in order to comply with Section 327.

(d) An Operator or Operating Agency shall not be civilly or criminally liable for the destruction of Footage or accompanying data in accordance with the rules established under this Section.

Legislative Note: *This Section establishes two different categories of Recorded Footage, which will require different levels of review and authorization before access is allowed to Operators. As a general matter, Footage which has been retained for a longer period of time should require a higher standard of review before access is allowed. Rules for access are provided in Sections 315-324.*

SECTION 314. REQUESTS FOR EXTENDED RETENTION OF ARCHIVAL RECORDED FOOTAGE BEYOND RETENTION PERIOD.

(a) Footage may be retained beyond the retention period designated pursuant to Section 313 only upon specific request of an Operator. Each request shall be submitted in writing upon oath or affirmation of an Operator to [the chief executive officer of the Operating Agency, or his or her designee], and shall include all of the following:
    (1) a full and complete statement of the purpose for which the requested Footage is to be retained; and
    (2) a detailed description of what is contained in the requested Footage, including details regarding the particular offense or offenses of which the Footage may provide evidence, and the identity or identities, if known, of the person or persons whose image(s) is or are depicted in the Footage.

(b) A request submitted under subsection (a) of this Section may be granted if [the chief executive officer of the Operating Agency, or his or her designee] determines, based on all the facts submitted in the request, one of the following:
    (1) The purpose for which the Footage will be retained is consistent with the approved purpose of the Public Video Surveillance System as articulated by the [Governing Body] in its Final PVS Impact Report, Section 209, and there is a reasonable suspicion that the Footage in question contains evidence of criminal activity or is relevant to an ongoing investigation or pending criminal trial.
    (2) The purpose for which the Footage will be retained is a Secondary Purpose, and there is probable cause to believe that the Footage in question contains evidence of criminal activity or is relevant to an ongoing investigation or pending criminal trial.

(c) Footage retained pursuant to a properly granted request under this Section need not be automatically deleted after the expiration of the retention period set under Section 313.

(d) If a request for extended retention under subsection (b) of this Section has been granted, retained Footage may be accessed and used by the Operator and Operating Agency for the uses consistent with the reasons given in support of the retention request only. Access to Footage retained under subsection (b) of this Section for purposes other than that given in support of the retention request must comply with the requirements for access to archival Footage in Section 316-317.

(e) Footage may be retained beyond the retention period in connection with a formal complaint or disciplinary proceeding or investigation against an Operator or other member of the Operating Agency, where there is reason to believe that the Footage in question is relevant to that incident or investigation. Requests for such retention should follow the procedures set forth in subsections (a) and (b) of this Section.

Legislative Note: *Note that requests for extended retention must ultimately come from the Operator, but the showing required to retain the Footage may be based on facts and circumstances disclosed by other governmental agencies. This section is intended to include requests to retain Footage of critical public infrastructure, such as the Brooklyn Bridge, over an extended period of time. This would enable law enforcement to review such Footage to detect any activities to scout or "case" the location over time as part of a terrorist plot. Such patterns might not become apparent during the pre-archival period of one week.*

PART 2. ACCESS TO AND USE OF RECORDED FOOTAGE.

SECTION 315. ACCESS TO OR DISCLOSURE OF PUBLIC VIDEO SURVEILLANCE FOOTAGE AND DATA TO THIRD PARTIES PROHIBITED.

Except as otherwise provided in Sections 320-324 of this [act], the Operator or Operating Agency shall not disclose Footage or other data gathered or compiled by or stored in a Public Video Surveillance System to Third Parties, or provide to or allow Third Parties to access such Footage or data.

Legislative Note: *Communities should restrict, to the extent possible, use of public video surveillance data by Third Parties. Especially to the extent the data reveals identifiable individuals, sharing of data without the consent of the individuals severely undermines individuals' confidence in official motives for collecting such information, and further threatens constitutional rights and values. While releasing Footage may be beneficial in some cases, in general disclosures to Third Parties creates increased risk of the information being used for improper and unaccountable purposes. Please see Sections 320-324 for the situations in which disclosure to and access by Third Parties is permissible.*

SECTION 316. OPERATING AGENCY ACCESS TO AND USE OF RECORDED FOOTAGE FOR PRIMARY PURPOSE.

An Operator or Operating Agency may access and use Recorded Footage for purposes consistent with purpose of the System as articulated by the [Governing Body] in its Final PVS Impact Report, Section 209, or in accordance with the order obtained under Section 314. No additional approval is required for such use, once the Footage has been properly retained pursuant to Section 313 or 314.

Legislative Note: *This provision applies to all Recorded Footage, regardless of how long it has been retained.*

SECTION 317. OPERATING AGENCY ACCESS TO AND USE OF RECORDED FOOTAGE FOR SECONDARY PURPOSE.

(a) Except as provided in this Section, the Operator or Operating Agency may not access or use Recorded Footage for a Secondary Purpose.

(b) *Administrative approval for pre-archival Footage:* Pre-archival Recorded Footage may be accessed and used by the Operator or Operating Agency for a Secondary Purpose upon specific request of an Operator, provided that:

(1) Each such request is made in writing upon oath or affirmation of an Operator to [the chief executive officer of the Operating Agency, or his or her designee], and includes all of the following:

(i) a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including: (A) details regarding the particular offense that has been, is being, or is about to be committed; (B) a particular description of the location or locations of such offense; and (C) the identity, if known, or a description of the person(s) believed to be involved in the commission of the offense; and

(ii) a description of the Footage to be accessed or used, including identification of the cameras through which the Footage was obtained, and the time periods for which access is requested.

(2) A request submitted under subsection (b)(1) of this Section may be granted if [the chief executive officer of the Operating Agency, or his or her designee] determines, based on all the facts submitted in the request, all of the following:

(i) there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense carrying a term of imprisonment greater than one year; and

(ii) there is probable cause to believe that evidence of or information about that crime or the individual who committed that crime will be obtained by access to the Footage described in the application.

(c) *Court approval for archival Footage:* Archival Recorded Footage may be accessed and used by the Operator or Operating Agency for a Secondary Purpose upon the [Operator, Operating Agency, or district attorney's] application for an order from a court of competent jurisdiction authorizing access to archival Recorded Footage.

(1) Each such application must be made in writing upon oath or affirmation of an Operator to [a judge of competent jurisdiction], and shall include all of the following:

(i) a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including: (A) details regarding the particular offense that has been, is being, or is about to be committed; (B) a particular description of the location or locations of such offense;

and (C) the identity, if known, or a description of the of the person(s) believed to be involved in the commission of the offense.

(ii) a description of the Footage to be accessed or used, including identification of the cameras through which the Footage was obtained, and the time periods for which access is requested.

(2) Upon application made under subsection (c)(1) of this Section, the judge may enter an order, as requested or modified, authorizing access to archival Recorded Footage within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

(i) there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense carrying a term of imprisonment greater than one year; and

(ii) there is probable cause to believe that evidence of or information about that crime or the individual who committed that crime will be obtained by access to the Footage described in the application.

(3) Each order authorizing use of Footage for a Secondary Purpose shall specify all of the following:

(i) a particular description of the Footage to which access is granted, including the location of the camera or of the location depicted in the Footage, and the time when the Footage was Recorded

(ii) the identity of the person(s), or if their identity is unknown, a description of, the person(s) believed to be involved in the commission of the offense and depicted in the Footage to which access is granted.

(d) Footage retained under Section 314 may be accessed and used by the Operator or Operating Agency as part of the investigation and prosecution of the offense under which the request for retention was made.

Legislative Note: *In general, the use Public Video Surveillance Systems should be limited to the purpose for which the System was approved under Article I of this [act]. Therefore, potential use for Secondary Purposes should be paid closer scrutiny. This section provides different procedures for access to Footage for Secondary Purposes based on whether that Footage is pre-archival or archival. Approval for access to pre-archival Footage need only be sought from an appropriate administrative official, while access to archival Footage requires approval of a judge.*

Subsection (c)(2)(i) of this section places a limit on use for Secondary Purposes of Footage by requiring that the offense being investigated carry a sentence of more than one year imprisonment. Jurisdictions may use their judgment in altering this limitation to suit their needs, such as by listing the particular offenses or classes of offenses that are appropriate subjects for the use for Secondary Purposes of Footage.

SECTION 318. OPERATING AGENCY ACCESS TO AND USE OF RECORDED FOOTAGE FOR SECONDARY PURPOSES UNDER EXIGENT CIRCUMSTANCES.

(a) Upon informal application by the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons], a [judge of competent jurisdiction] may grant oral approval for access to Recorded Footage for a Secondary Purpose, without an order, if he or she determines all of the following:
    (1) There are grounds upon which an order could be issued under this chapter.
    (2) There is probable cause to believe that an emergency situation exists
    (3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

(b) If the person seeking oral approval for access to Recorded Footage for a Secondary Purpose under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such person may authorize and proceed with the emergency access to Recorded Footage without an order, if he or she determines all of the following:
    (1) There are grounds upon which an order could be issued under this chapter.
    (2) There is probable cause to believe that an emergency situation exists with respect to the investigation of an offense the investigation and/or prevention of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report.
    (3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

(c) Approval for access to Recorded Footage for a Secondary Purpose under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval under subsection (a) of this section or a determination under subsection (b) of this Section, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under subsection (a) or determination under subsection (b) and be retroactive to the time of such oral approval or determination.

Legislative Note: *This exception for access to Recorded Footage for Secondary Purposes under exigent circumstances makes no distinction between pre-archival and archival Footage.*

SECTION 319. INCIDENTAL USE OF PUBLIC VIDEO SURVEILLANCE SYSTEM BY OPERATING AGENCY.

When using a Public Video Surveillance System for approved purposes, if the Operator observes any activities or events arousing reasonable suspicion of criminal activity, the Operator may use that information for other legitimate law enforcement activities, even those inconsistent with the purposes of the PPVS System.

SECTION 320. CRIMINAL DEFENDANTS.

(a) In accordance with [state and federal rules of criminal procedure], defendants in criminal cases may obtain Video Surveillance Footage related to the charges pending against them that is within the government's possession, custody, or control.

(b) If Video Surveillance Footage is intended to be used in the prosecution's case in chief in a criminal trial, the criminal defendant shall be provided with all of the following:
   (1) copies of all the Footage intended to be used in the prosecution's case in chief at trial. The Footage provided shall include both the particular segments contemplated for use in the case in chief, and all other Footage Recorded by the same camera within 24 hours of the segments intended to be used;
   (2) copies of any Automatic Identification or Automatic Tracking orders and their accompanying applications, if any warrants were obtained or applied for; and
   (3) access logs [and other relevant data] corresponding with the provided Footage.

(c) Footage disclosed to criminal defendants under this section shall not be disclosed to the public, except to the extent necessary to defend against the criminal charges in the action under which the Footage is disclosed.

> ***Legislative Note:*** *State and federal procedures and standards for access to Recorded Footage by criminal defendants should be adhered to in providing Video Surveillance Footage to such parties. This section should not be interpreted to have any effect on the government's duty to disclose material, exculpatory evidence to a criminal defendant.*

SECTION 321. ACCESS TO RECORDED FOOTAGE IN CIVIL SUITS BETWEEN PRIVATE LITIGANTS PROHIBITED.

(a) Data collected by Public Video Surveillance Systems shall not be available to the parties or discoverable in civil trials between private litigants, except as provided in Subsection (b) of this Section.

(b) Data collected by a Public Video Surveillance System shall be available to a private litigant upon a showing to the presiding judge that such Footage is needed to prevent imminent Harm to life or limb, such as in a proceeding to obtain a restraining order.

Legislative Note: *This section is not intended to preclude access to video surveillance data in a suit alleging police misconduct, in which the government would typically be a party to the litigation. To the extent that under applicable state laws police misconduct suits would be considered litigation between private litigants, this provision may need to be modified accordingly.*

SECTION 322. ACCESS TO RECORDED FOOTAGE UNDER THE STATE [PUBLIC RECORDS ACT].

Public Video Surveillance Footage and data from a Public Video Surveillance System shall not be considered [public records] for purposes of the [state public records or freedom of information act].

Legislative Note: *Given the potential threats to privacy and other constitutional rights and values posed by wide disclosure of Footage and data collected by Public Video Surveillance Systems, and the expense of reviewing and providing this information, this information should not be available to the public under state public records or freedom of information acts. Other measures, such as publicly accountable approval procedures and audit requirements, reintroduce a measure of public accountability to these Systems.*

SECTION 323. ACCESS TO RECORDED FOOTAGE BY OTHER GOVERNMENTAL ENTITIES.

(a) Except as provided in Subsection (b) of this Section, or as [required by federal law], a governmental authority other than the Operating Agency may not access or use Recorded Footage.

(b) A governmental authority other than the Operating Agency for the PVS System may apply for an order authorizing access to Recorded Footage.
  (1) Such applications must be made in writing upon oath or affirmation of an Operator to [a judge of competent jurisdiction], and shall include all of the following:
    (i) a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including: (A) details regarding the particular offense that has been, is being, or is about to be committed; (B) a particular description of the location or locations of such offense; and (C) the identity, if known, or a description of the of the person(s) believed to be involved in the commission of the offense.
    (ii) a description of the Footage to be accessed or used, including identification of the cameras through which the Footage was obtained, and the time periods for which access is requested.
  (2) Upon application made under subsection (b)(1) of this Section, the judge may enter an ex parte order, as requested or modified, authorizing access to Recorded Footage within the territorial jurisdiction of the court in which the

judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

(i) there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense carrying a term of imprisonment greater than one year; and

(ii) there is probable cause to believe that evidence of or information about that crime or the individual who committed that crime will be obtained by access to the Footage described in the application.

(3) Each order authorizing access to Recorded Footage under this section shall specify all of the following:

(i) a particular description of the Footage to which access is granted, including the location of the camera or of the location depicted in the Footage, and the time when the Footage was Recorded; and

(ii) the identity of the person(s), or if their identity is unknown, a description of, the person(s) believed to be involved in the commission of the offense and depicted in the Footage to which access is granted.

Legislative Note: *Note that here, unlike when access to Footage is being requested by the Operating Agency, the distinctions between archival and pre-archival Footage, and use for primary or Secondary Purposes, are irrelevant—all requests for access to Footage are judged by the same standard.*

SECTION 324. ACCESS TO RECORDED FOOTAGE BY OTHER GOVERNMENTAL ENTITIES UNDER EXIGENT CIRCUMSTANCES.

(a) Upon informal application by [a designated official in the requesting government agency] of a governmental authority other than the Operating Agency for the PVS System, a [judge of competent jurisdiction] may grant oral approval for access to Recorded Footage, without an order, if he or she determines all of the following:

(1) There are grounds upon which an order could be issued under this chapter.

(2) There is probable cause to believe that an emergency situation exists.

(3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

(b) If the person seeking oral approval for access to Recorded Footage under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such person may authorize and proceed with the emergency access to Recorded Footage without an order, if he or she determines all of the following:

(1) There are grounds upon which an order could be issued under this chapter.

(2) There is probable cause to believe that an emergency situation exists with respect to the investigation of an offense the investigation and/or prevention

of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report.

(3) There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

(c) Approval for access to Recorded Footage under this section shall be conditioned upon filing with the judge, within 72 hours of the oral approval, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under subsection (a) or determination under subsection (b) and be retroactive to the time of such oral approval or determination.

PART 3. INTEGRITY AND SECURITY OF PERMANENT PUBLIC VIDEO SURVEILLANCE SYSTEM AND STORED DATA.

SECTION 325. SECURITY SAFEGUARDS FOR PUBLIC VIDEO SURVEILLANCE SYSTEM AND STORED DATA.

(a) Access to Recorded data and the physical facilities of a Public Video Surveillance System shall be strictly limited to Operators.

(b) The Operating Agency shall implement and maintain reasonable technological security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of public video surveillance data.

Legislative Note: *Technological safeguards can be costly and complicated. We believe, however, that they are necessary to protect against the significant privacy risks that come with implementation of a technologically sophisticated Public Video Surveillance System. Further measures, such as encrypting all data and entrusting the encryption keys to an independent body that releases Recorded data only upon proper authorization from a judge or administrative official, may be required at the enacting body's discretion.*

SECTION 326. TRAINING FOR OPERATORS WITH ACCESS TO PUBLIC VIDEO SURVEILLANCE SYSTEM.

(a) The [Operating Agency] of a Public Video Surveillance System shall provide training for all Operators. Training must cover all the following topics:

(1) the technical operation of the System, including manipulation of the cameras and access to the data storage facilities;

(2) all applicable laws, rules, and policies regarding the System; and

(3) sanctions for Misuse or abuse.

(b) Access to a Public Video Surveillance System and its facilities and stored data, including but not limited to control rooms, databases, and cameras, by the Operator

and its employees or agents shall be limited to enumerated lists of authorized Operators who have completed the requisite training program described in subsection (a) of this Section, except where data must be provided to Third Parties as enumerated in Sections 320-324.

SECTION 327. RECORD-KEEPING REQUIREMENTS FOR PUBLIC VIDEO SURVEILLANCE SYSTEMS.

Detailed records must be kept regarding the operation of and access to the Public Video Surveillance System, including:

(a) an ongoing log of all those who maintain, operate, observe, inspect, or access the Public Video Surveillance System and/or any data or Footage collected by that System, including the purposes of each activity, the names of the individuals engaging in that activity, and the times dates when such access occurs;

(b) an ongoing log of all Recorded Footage, including how long the Footage has been retained, why the Recorded Footage was retained, and copies of any orders for extended retention, if they exist; and

(c) an ongoing log of all disclosures of Recorded Footage, including a description of what is contained in the Footage, the names of any parties to which the Footage was disclosed, when the Footage was disclosed, the reasons for disclosure, and copies of any orders for disclosure, if they exist.

Legislative Note: *The maintenance of complete and detailed records of all use of the Video Surveillance System is necessary for ongoing review of the effectiveness and appropriateness of the System as a law enforcement tool. In addition, when published as part of an audit under Section 213, this information can provide some of the public accountability normally attained via public records act requests.*

PART 4. SANCTIONS, ENFORCEMENT, REMEDIES.

SECTION 328. ADMINISTRATIVE DISCIPLINE.

(a) The Operating Agency shall provide procedures for investigation of and discipline for abuse or Misuse of the Public Video Surveillance System. This shall include a means by which employees of the agency and members of the public may confidentially report suspected violation of the provisions of this [act].

(b) Any employee who is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment by his or her employer because of lawful acts done by the employee on behalf of his or her employer or others in furtherance of an action under this [act], including investigation for, initiation of, testimony for, or assistance in an action filed or to be

filed under this [act], shall be entitled to all relief necessary to make the employee whole.

SECTION 329. EXCLUSIONARY RULE.

(a) A criminal defendant in any trial, hearing, or proceeding against him or her may move to suppress the contents of Footage observed or Recorded pursuant to this chapter, or evidence derived therefrom, on any of the following grounds:
    (1) The Footage or other information from the Public Video Surveillance System was collected in a manner constituting a substantial violation of a provision of this [act].
    (2) The order of authorization or approval under which the Footage was collected is insufficient on its face, such that it would be unreasonable for an Operator to rely on its sufficiency.
    (3) The Footage or other information was not collected in conformity with the order of authorization or approval.

(b) A motion under subsection (a) of this Section shall be made, determined, and subject to review in accordance with [state law].

Legislative Note: *In order to be effective, this provision requiring the exclusion of evidence gathered in violation of this act must likely be enacted at the state level. In addition, this Section should reference state statutory provisions regarding the making and adjudicating of motions to suppress.*

SECTION 330. PRIVATE RIGHT OF ACTION.

(a) Any person who is:
    (1) depicted in Video Surveillance Footage, or described by data attached to Video Surveillance Footage, which is improperly disclosed, accessed, or retained in violation of this [act];
    (2) Automatically Tracked in violation of Sections 307, 308, or 309;
    (3) Automatically Identified in violation of Sections 302, 303, or 309, including both individuals whose images appear in video Footage on which Automatic Identification is performed, and individuals whose personal information is revealed as a result of Automatic Identification or appended to Video Surveillance Footage;
    (4) the subject of Pan, Tilt, or Zoom activity in violation of Section 311; or
    (5) publicly but mistakenly identified as appearing in Video Surveillance Footage depicting commission of a criminal act; may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) In an action under this Section, appropriate relief includes:
    (1) such injunctive and other equitable or declaratory relief as may be appropriate;

(2) actual damages but not less than liquidated damages computed at the rate of:
    (i) one hundred dollars ($100) a day for each day of violation or one thousand dollars ($1,000), whichever is greater, if defendant's conduct is negligent; or
    (ii) five hundred dollars ($500) a day for each day of violation or five thousand dollars ($5,000), whichever is greater, if defendant's conduct is intentional or reckless.
(3) punitive damages, if defendant's conduct was intentional or reckless; and
(4) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) A good faith reliance on a court warrant or order, or administrative approval under this [act] is a complete defense against any civil or criminal action brought under this chapter or any other law.

(d) A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the alleged violation.

Legislative Note: *This Section provides relief to individuals who have been Harmed by violation of the use restrictions under Article 3 of this [act]. However, claims for violations of Article 2 of this [act] having to do with procedures for implementation may be made in the same action as claims for violations under this Article, although the remedies for such violations are different. Furthermore, evidence of violations of Article 2 of this [act] may in some cases be relevant to claims under this Article, as where, for example, the stated purpose of the System is relevant to whether a violation has occurred. Actions under this section may be maintained against individual Operators or the Operating Agency.*

SECTION 331. ENFORCEMENT BY STATE ATTORNEY GENERAL.

(a) The state Attorney General or equivalent state review panel shall be empowered to investigate and review failures to comply with the provisions of this Article, and to issue orders for compliance.

(b) Upon a finding of a pattern or practice of violations of this Article, the state may withhold funds from the Operating Agency until the Attorney General is satisfied that a full investigation has been made and steps have been taken by the Operating Agency to reduce the incidence of violation.

PART 5. OTHER.

SECTION 332. PUBLIC NOTICE OF PUBLIC VIDEO SURVEILLANCE.

(a) Jurisdictions employing a Public Video Surveillance System must post notices in locations subject to public video surveillance that state, in clear language, that such

location is subject to Observation and, if applicable, recording, by a Public Video Surveillance System.

(b) Notices posted pursuant to subsection (a) shall posted within 7 days of the initiation of the System, and shall be in clear language, large type, and in a conspicuous location plainly visible to persons present in the surveilled area. Notices need not, however, disclose the precise location of the camera(s).

(c) If the Public Video Surveillance System is temporary and installed pursuant to a court order obtained under Section 210, notices of surveillance, including a description of the locations surveilled, must be published in local newspapers or through electronic means according to applicable pubic notice regulations no later than 30 days after (1) termination of the surveillance or (2) a determination that such disclosure will no longer jeopardize the investigation or reasonably related investigations. Notices published pursuant to this subsection must be published for no fewer than 7 consecutive days.

Legislative Note: *To permit informed choices and provide accountability, those subject to video surveillance should be made aware of it. While for security as well as aesthetic and social reasons, many communities may want to hide or disguise the actual cameras, there is generally no basis for hiding the fact that an area is under government surveillance. These notifications need not be intrusive, but should nevertheless be visible. We recommend that authorities place small placards in the surveilled area noting the presence of video surveillance and providing contact information for those wishing more information on the camera System. Subsection (c) intends to provide an exception for purposes which require a measure of secrecy at their Installation.*

SECTION 333. PRIVATELY COLLECTED PUBLIC VIDEO SURVEILLANCE DATA.

The government shall not use privately collected video surveillance of public places with such regularity as to effectively circumvent the provisions of this act. If the Operating Agency obtains Footage of public places from private cameras, the use and retention of such Footage shall be subject to all the requirements of Article 3 of this Act, to the same extent as if the Footage had been obtained from government owned and operated cameras.