Local
Surveillance
Oversight
Ordinances
FEBRUARY 2021

Samuelson Clinic Student White Paper
Authored by Ari Chivukula ’21
and Tyler Takemoto ’22
Under the supervision of
Catherine Crump and Juliana DeVries
Acknowledgements

Tyler Takemoto and Ari Chivukula authored this white paper under the supervision of Clinic faculty members Catherine Crump and Juliana DeVries. They would like to thank the experts who made themselves available for interviews or reviewed drafts, especially Brian Hofer, Mailyn Fidler, and Chad Marlow. Thanks also to the many Samuelson Clinic students and faculty members who reviewed and consulted on this white paper as it was being drafted.
I. Introduction

Since 2015, sixteen jurisdictions across eight states have passed local surveillance technology oversight ordinances meant to bring more transparency and democratic control to local government use of surveillance technology.\(^1\) Passage of these ordinances appears to be in response to an effort by civil liberties and civil rights groups concerned about the increasingly powerful surveillance tools making it into the hands of local law enforcement agencies.\(^2\) Broadly speaking, these ordinances require government agencies to meet public reporting and approval requirements before acquiring or using surveillance technology.

This white paper analyzes these surveillance technology oversight ordinances by examining the text of the ordinances themselves.\(^3\) It outlines the history of surveillance technology oversight ordinances and describes and compares their general features. We have analyzed the text of the sixteen municipal surveillance ordinances currently in effect.\(^4\) We explore the similarities


\(^3\) The scope of this project is limited to the text of the ordinances themselves. We do not attempt to analyze, for example, whether local governments are complying with the ordinances in practice or whether compliance has the effect of decreasing surveillance overall, although such analysis would be useful to undertake. For one analysis of the surveillance technology oversight ordinances in practice, see Mailyn Fidler, Local Police Surveillance and the Administrative Fourth Amendment, 36 Santa Clara High Tech. L.J. 481, 557–560 (2020).

\(^4\) As of writing, municipal surveillance ordinances are under consideration in Boston, Massachusetts and San Diego, California; we do not analyze these two because they have not yet taken effect. Christopher Gavin, Boston Councilors Seek to Make City’s Array of Surveillance Technologies More Transparent, Boston.com (Nov. 12, 2020), https://perma.cc/3XDN-87WB; Teri Figueroa, San Diego City Council Unanimously Back Ordinances to Govern Surveillance Technologies (Nov. 10, 2020, 8:40 PM), https://perma.cc/CR7N-ZAP2. Also excluded from our analysis is an ordinance in Northampton, MA that bans surveillance technology in public spaces for more than one day; we do not include it primarily because it does not have a civilian oversight component. Northampton, Mass., Code of Ordinances art. III, § 285-52. We additionally exclude Pittsburgh, Pennsylvania’s “Select Surveillance” ordinance, which imposes restrictions on and City Council oversight of facial recognition technology and predictive policing technology but
between the ordinances (for example, almost all require an elected body to approve acquisition of new surveillance technology) as well as the differences (for example, some ordinances have robust enforcement mechanisms, while others do not). This analysis is meant to assist policymakers in understanding the range and scope of the existing ordinances as they consider adopting or amending surveillance technology oversight ordinances for their jurisdictions. It is also intended to assist members of the public in understanding how different jurisdictions regulate surveillance at the local level so they can decide whether to support or oppose these ordinances.

II. What are surveillance technology oversight ordinances?

While government surveillance can assist law enforcement in investigating and prosecuting crimes, it can also enable targeting and discrimination against vulnerable communities. During the Civil Rights Movement, the federal government systematically monitored racial justice organizers and leaders of the Black community. In the Twenty-First Century, government surveillance capabilities, including at the local level, have increased dramatically, raising serious civil liberties and civil rights concerns. After September 11, 2001, the New York Police Department surveilled mosques with cameras and automatic license plate readers. And in 2020, law enforcement monitored Black Lives Matters protestors using Amazon’s Ring doorbell cameras and drones. Community organizers, journalists, and other activists have long recognized the harm of invasive government surveillance on the Black community, as well as on

{\textbf{does not apply more broadly. Pittsburgh, Pa., Code of Ordinances title 1, art. III, § 116.15 (Sept. 20, 2020). We include an “administrative policy” passed in Grand Rapids, Michigan because of its similarity to the municipal surveillance ordinances passed in other jurisdictions. § 15-03. We refer to the ordinances and this administrative policy collectively as “surveillance technology oversight ordinances.”}}

5 See, e.g., Ángel Díaz, New York City Police Department Surveillance Technology, Brennan Center for Justice (Oct. 4, 2019), \url{https://perma.cc/63DR-P4EL} (detailing impact of various surveillance technologies used in New York City on race, gender, and age bias).


Indigenous people, people of color and those perceived to be Muslims or immigrants, underscoring the need for public oversight of government surveillance power.  

The surveillance technology oversight ordinances reviewed in this report were a response to these problems. Civil liberties and civil rights groups at the national and local level, including the ACLU, the Electronic Frontier Foundation, the NAACP, the National Network of Arab American Communities, Restore the Fourth, Oakland Privacy, the Surveillance Technology Oversight Project in New York, and the Seattle Privacy Coalition, have led the effort to push jurisdictions to adopt these ordinances, which the ACLU refers to as Community Control Over Police Surveillance (“CCOPS”) ordinances. The ACLU launched its CCOPS campaign on September 21, 2016; it included a model ordinance for local jurisdictions to use. So far seven jurisdictions in California, three in Massachusetts, and six others across the country have adopted surveillance technology oversight ordinances. 

These ordinances require government actors to meet public reporting and elected body approval requirements before acquiring or using surveillance technology. The ordinances rely on an understanding that more public access to information about surveillance technology will bring about better policies and practices around surveillance. The effort also intends to recognize that local communities vary in their values and history and that local circumstances should drive how communities regulate surveillance technology. Supporters have lauded these ordinances as a “promising first step that protects both the safety and civil liberties” of the most vulnerable.


15 See id.

while detractors have called them “a solution in search of a problem,” because of an alleged
dearth of documented misuses of surveillance technology, as well as a “burdensome and paper-
intensive approach.”\footnote{Emilie Raguso, \textit{Officials Approve New Rules on City Surveillance; May be First in the Nation}, Berkeleyside (Mar. 15, 2018, 8:39 PM), \url{https://perma.cc/3WED-64AJ}.} This white paper is not meant to answer the question whether either of
these perspectives is correct but to explain how the text of existing surveillance technology
ordinances vary in ways that may impact their effectiveness.

III. \textbf{What are the major components of surveillance technology oversight ordinances?}

Generally speaking, surveillance technology oversight ordinances tell local government
departments what they need to do before acquiring surveillance technology. The ordinances
then define the steps local authorities must take to prepare policies that dictate the use of the
surveillance technologies once acquired and how the public and elected bodies will have a chance
to periodically review how local authorities are using these technologies.

The sixteen ordinances analyzed in this section were passed between 2015 and 2020, across eight
states (with seven in California and three in Massachusetts). Each applies to a county, village, or
city with the exception of an ordinance for Bay Area Rapid Transit (\textit{“BART”}), a California
transportation agency.

This section reviews and analyzes the sixteen surveillance technology oversight ordinances in
eight major areas. First, we look at how the different ordinances define what qualifies as a
surveillance technology. Second, we look at whether every government body in the jurisdiction
must follow the ordinance or whether the ordinance only applies to some departments. Third,
we look at whether the ordinance requires that proposals for new surveillance technology
include impact reports and use policies and whether annual reports are required after the
acquisition of the new technology. Fourth, we look at whether the ordinance requires an elected
body to review surveillance technology reports or proposed surveillance technology policies.
Fifth, we note whether the ordinance applies retroactively to surveillance technologies already
in use. Sixth, we analyze whether the ordinance creates or engages an independent body in the
process of surveillance technology acquisition and review. Seventh, we explain the mechanisms
created to enforce the ordinance. Eighth, and finally, we compare the various exceptions to the
requirements set out in the ordinances. Our findings are summarized in this paper as well as in a
table in the appendix.

Although there are outliers, the ordinances are generally similar in their definitions of
surveillance technology, what government bodies they cover, whether they require reports and
policies, and whether they require an elected body to review and approve new surveillance
technology. The ordinances part ways most drastically in whether they apply retroactively,
whether an independent body assists in implementing the ordinance, and in what exceptions and
enforcement mechanisms exist. Many of the ordinances, for example, have an exception for “exigent circumstances,” but they differ as to how they define this term and the period of time that this exception can last. The ordinances also include a wide variety of additional exceptions and limitations that apply to law enforcement agencies.

A. How is surveillance technology defined?

Fifteen of the ordinances define “surveillance technology.” Almost every definition includes both a type of device that qualifies as surveillance technology and a purpose for which that device must be used to qualify. Oakland, California, for example, which uses a definition typical of the rest, defines surveillance technology as “any software, electronic device, system utilizing an electronic device, or similar, that is used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information associated with, or capable of being associated with, any individual or group.”

Many of the ordinances also list specific technologies that qualify as surveillance technologies, such as cell site simulators, gunshot detection systems, or automatic license plate readers. They also often list exempted technologies, such as manually operated portable digital cameras, audio recorders, and video recorders. Others incorporate a blanket ban on specific technologies, such as facial recognition software.

---


19 § 9.64.010(14) (Oakland).

20 See, e.g., § 23.63(2) (Madison).

21 See, e.g., id. § 23.63(2)(10).

B. Which departments are regulated?

Some ordinances cover more local government departments than others. While some apply to all departments in the jurisdiction, others exempt certain departments from coverage or have special rules for law enforcement. Still others cover only one department.

1. All departments are regulated by the ordinance.

Of the sixteen ordinances, nine regulate every governmental department in the jurisdiction. In these jurisdictions, every department from the police department to the transportation department is covered and must comply with the requirements of the ordinance when seeking to acquire or use qualifying surveillance technology. The BART ordinance is unlike the others in that it applies to a transportation agency that is self-governing, rather than to a municipality. BART’s ordinance does, however, apply across the board; all departments of BART are subject to the ordinance.

2. Some departments are regulated by the ordinance.

Six of the ordinances exempt certain departments from coverage, usually law enforcement agencies, or have special rules for law enforcement.

Some jurisdictions have banned or imposed moratoria on specific surveillance technologies, such as facial recognition software, in a separate ordinance or without additionally passing a surveillance technology oversight ordinance that applies more broadly. Bans, Bills and Moratoria, Elec. Frontier Found., https://perma.cc/6CCG-9H2R (last visited Jan. 5, 2021).


24 See § 17-508(1) (BART).

San Francisco, California has the most clear-cut example of exempting law enforcement and law enforcement-related departments. There, the definition of “City Department” or “Department” covered by the ordinance “shall not mean the District Attorney or Sheriff when performing their investigative or prosecutorial functions, provided that” they certify in a public writing that “acquisition or use of a specific Surveillance Technology is necessary to perform an investigative or prosecutorial function” and certify “either an explanation of how compliance . . . will obstruct their investigative or prosecutorial function or a declaration that the explanation itself will obstruct either function.”

In other jurisdictions, special rules apply to law enforcement agencies when they act pursuant to a lawful search or under other specified circumstances. In Nashville, Tennessee, for example, the surveillance technology oversight ordinance does not cover “acquisition or use of surveillance technology by or on behalf of law enforcement that is used on a temporary basis for the purpose of a criminal investigation supported by reasonable suspicion, or pursuant to a lawfully issued search warrant, or under exigent circumstances as defined in case law.” Cambridge, Massachusetts exempts “[s]urveillance conducted pursuant to a warrant using previously approved Surveillance Technology” where “the Police Commissioner has determined that the release of information pertaining to the surveillance would compromise public safety and security, provided that the information is released in the next Annual Surveillance Report following the Police Commissioner’s determination that public safety and security concerns pertaining to the release of such information no longer exist.” Palo Alto, California’s ordinance states, simply: “The Annual Surveillance Report will not include information that may compromise the integrity or limit the effectiveness of a law enforcement investigation.”

____________________________________________________________________________

performed their investigative or prosecutorial functions,” provided that certain conditions are met); see also Santa Clara Cnty., Cal., Mun. Code § A40-5 (2016) (requiring that the Board not “obstruct the investigative function of the sheriff or the county nor shall it obstruct the investigative and prosecutorial function of the district attorney” in approving or denying use of a surveillance technology).

26 § 19B.1(11) (S.F.).

27 § 13.08.080(E) (Nashville).

28 § 2.128.070(B)(1) (Cambridge); see also § 9.25.080 (Lawrence) (allowing police department temporary use of surveillance technology “when the chief of police finds, subject to approval of the mayor, that compelling circumstances in the public interest warrant use”).

29 Palo Alto, Cal., Admin. Code § 2.30.680 (2018). This is arguably an exception to the annual reporting requirement alone, but we include it here because it applies to law enforcement specifically.
Seattle’s ordinance covers law enforcement agencies but does not apply to the Seattle Municipal Court nor to the Seattle Public Library.\textsuperscript{30}

3. One department is regulated by the ordinance.

Of the sixteen ordinances, only New York City’s ordinance applies to one department alone—the police department.\textsuperscript{31}

C. What reporting and policy requirements do the ordinances establish?

Surveillance technology oversight ordinances generally require city departments seeking to acquire or use qualifying technologies to gain approval for those technologies from a public body that weighs the costs and benefits of acquisition and makes a decision about whether to permit acquisition or use.

When an agency seeks approval for the acquisition of a new surveillance technology, the ordinances often require it to create a use policy to regulate the technology and an impact report to understand how the surveillance technology may affect civil liberties and civil rights. These policies and reports are made public and must be approved before the technology is put to use. The ordinances also typically require a publicly available annual report summarizing surveillance practices and policies from the past year. This section compares the various policy and reporting requirements of the sixteen ordinances studied.

1. Surveillance policies must be created and approved.

Under the surveillance technology oversight ordinances, when an agency seeks to acquire a new surveillance technology, it usually must seek approval from an elected body and propose a surveillance use policy to regulate the new technology. Thirteen of the ordinances studied require these use policies.\textsuperscript{32} In Davis, California, for example, any city department seeking


\textsuperscript{31} N.Y.C., N.Y., Admin. Code § 14-188 (2020).

approval for a new surveillance technology “shall submit to the city council . . . a proposed Surveillance Use Policy . . .”\(^{33}\)

Many of the ordinances define what the proposed surveillance use policies must include. For example, the use policy might need to include the steps a city employee must take prior to using the new technology; the category of individuals who may access the surveillance data generated by the technology; how the data will be protected from unauthorized disclosures, retained, or destroyed; how the data may be accessed by third parties, the public, or criminal defendants; and training mechanisms for those who are authorized to use the new technology.\(^{34}\)

2. The ordinance requires submission of a surveillance impact report.

Twelve of the sixteen ordinances studied require that departments seeking to acquire new surveillance technology prepare and submit a surveillance impact or surveillance acquisition report.\(^{35}\) This report describes the surveillance technology and its likely impact on civil rights and civil liberties. It is usually prepared in addition to a surveillance use policy. The report typically must include, among other things, a description of the technology and how it works; the purpose of the technology; the location where it may be deployed; the fiscal impact of acquiring it; its impact on civil rights and civil liberties; and alternative methods considered before deciding on the proposed technology.\(^{36}\)

3. An annual report on surveillance practices and policies is required.

Of the sixteen ordinances, fourteen require annual issuance of a report detailing all surveillance technology used in the previous year.\(^{37}\) In Oakland, for example, which has a reporting requirement similar to that found in the majority of the ordinances, city staff “must present a written Annual Surveillance Report,” which the City Council will use to “uphold or set aside the previous determination” that the benefits outweighed the costs of acquiring and using the surveillance technology in question.\(^{38}\) These reports generally include information such as a

\(^{33}\) § 26.07.030(c) (Davis).

\(^{34}\) See, e.g., § 2.128.030(D) (Cambridge).

\(^{35}\) See § 2.99.020(3) (Berkeley); § 2.128.020(C) (Cambridge); § 26.07.020 (Davis); § 9.25.040(B) (Lawrence); § 14-188(b) (N.Y.C.); § 9.64.020 (Oakland); § 2.30.680(b) (Palo Alto); § 19B.1(b)(1) (S.F.); § 17-503(4) (BART); § A40-7(d) (Santa Clara); § 14.18.040 (Seattle); § 10-65(b) (Somerville); see also 15-03 § 3 (Grand Rapids).

\(^{36}\) See, e.g., § 2.128.020(C) (Cambridge); § 9.64.010(15) (Oakland).

\(^{37}\) See § 2.99.020(2) (Berkeley); § 2.128.060(A) (Cambridge); § 26.07.060(a) (Davis); § 9.25.090(A) (Lawrence); § 23.63(5) (Madison); N.Y.C., N.Y., City Charter § 803(c-1) (2020); § 9.64.040(1) (Oakland); § 2.30.670 (Palo Alto); § 19B.6 (S.F.); § 17-508(1) (BART); § A40-6(a) (Santa Clara); §§ 14.18.050, 14.18.060 (Seattle); § 10-66(a) (Somerville); § 607.07(A) (Yellow Springs).

\(^{38}\) §§ 9.64.040(1), (2) (Oakland).
description of how the surveillance technology has been used over the past year; how data was shared with other entities; whether there were citizen complaints and what they were; the results of any internal audits; annual costs of the technology; where the technology was deployed; information such as crime statistics that might help the City Council assess the efficacy of the technology; information about any data breaches; and any requests for modifications of the previously submitted use policy.  

Seattle, Washington also requires an annual “Equity Impact Assessment,” which addresses whether the ordinance “is effectively meeting the goals of the Race and Social Justice Initiative, including whether any communities and groups in the City are disproportionally impacted by the use of surveillance technologies” and what can be done to improve in the future.

Nashville and Grand Rapids, Michigan are the only jurisdictions with surveillance oversight ordinances that do not require an annual report.

D. Does an elected body review or approve ordinance reports and policies?

All but one of the sixteen ordinances studied require an elected body to review and approve the reports and policies generated under the ordinance. This is a central feature of the ordinances, which are meant to establish public oversight and approval for surveillance technology. BART, for example, requires “Board of Directors approval at a properly-noticed public meeting” for surveillance technology already in use, for proposals for new use, and of the annual report.

New York City is the only jurisdiction that does not require an elected body to approve policies and reports. It requires only that “the [police] commissioner shall consider public comments and provide the final surveillance technology impact and use policy to the speaker and the mayor,” but not that the City Council approve the policy.

39 See, e.g., § 26.07.020(a) (Davis); § 9.64.010(1) (Oakland).

40 § 14.18.050 (Seattle).


42 § 2.99.030 (Berkeley); §§ 2.128.050(A), 2.128.060(A) (Cambridge); § 26.07.030 (Davis); § 15-03(2) (Grand Rapids); §§ 9.25.030(A), 9.25.040(A), 9.25.050 (Lawrence); §§ 23.63(4)(c), 23.63(4)(d) (Madison); § 13.08.080(C) (Nashville); § 9.64.030 (Oakland); §§ 2.30.660, 2.30.670 (Palo Alto); § 19B.2 (S.F.); § 17-504 (BART); §§ A40-5, A40-6(b), (c) (Santa Clara); § 14.18.020(A) (Seattle); § 10.66 (Somerville); § 607.03 (Yellow Springs).

43 See, e.g., § 2.99.010 (stating the purposes of the Berkeley ordinance and emphasizing the need for oversight and approval by “the City Council as the elected representatives of the City.”)

44 § 17-504(1) (BART).

45 See § 14-188(f) (N.Y.C.).
E. Does the ordinance apply retroactively?

Of the sixteen ordinances, eleven require departments to create policies or reports to govern surveillance technology already in use at the time the ordinance passed.\(^{46}\) For example, in Berkeley, the City Manager must submit to the City Council “a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each Surveillance Technology possessed or used prior to the effective date of this ordinance.”\(^{47}\)

The information required for approval of surveillance technology already in use is generally the same as the information required when seeking approval of a new surveillance technology.\(^{48}\) Different jurisdictions set different lengths of time that departments may continue to use surveillance technology acquired prior to passage before obtaining approval. These deadlines vary from 6 months (in Berkeley and Cambridge) to 60 days (in San Francisco).\(^{49}\)

F. Does the ordinance involve an independent body in reviewing surveillance technology and implementing the ordinance?

Some of the ordinances work in conjunction with internal or independent departments that help implement their requirements. In Oakland, the Privacy Advisory Commission (“PAC”), an independent body, has a significant role in the surveillance technology acquisition and review process. It has the authority to make recommendations on surveillance technology proposals.\(^{50}\) The Oakland ordinance requires city staff to notify PAC before soliciting funds or proposals with non-city entities to acquire, share, or use surveillance technology or the information it provides.\(^{51}\) Upon notification, PAC “shall place the item on the agenda at [its next] meeting for discussion and possible action.”\(^{52}\) PAC may then “make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify the proposal,

\(^{46}\) See § 2.99.050 (Berkeley); § 2.128.050(A) (Cambridge); § 26.07.030(a)(3) (Davis); § 9.25.050 (Lawrence); § 14-188(c) (N.Y.C.); § 9.64.020(3) (Oakland); § 19B.5 (S.F.); § 17-507(1) (BART); § A40.5 (Santa Clara); § 10-64(a) (Somerville); § 607.05(a) (Yellow Springs).

\(^{47}\) § 2.99.050 (Berkeley).

\(^{48}\) See, e.g., id.

\(^{49}\) Id.; § 2.128.050(A) (Cambridge); § 19B.5 (S.F.).


\(^{51}\) Id. § 9.64.020(1)(A).

\(^{52}\) Id. § 9.64.020(1)(B).
or take no action." The PAC review requirements also apply retroactively to existing technologies.

San Francisco’s ordinance references a Committee on Information Technology ("COIT") that is responsible for setting the city’s strategic priorities with respect to technology, for reviewing and approving all technology projects involving expenditures above $100,000, and for making recommendations to the Board of Supervisors about its surveillance technology decisions. COIT is made up of 13 department heads representing the city service areas. As part of its involvement with the surveillance ordinance’s requirements, COIT maintains an inventory of the city’s existing surveillance technologies.

The Seattle surveillance technology oversight ordinance establishes a Community Surveillance Working Group, which includes seven individuals appointed by the Mayor and City Council. At least five of these individuals must “represent equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including Seattle’s diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.” The working group must provide privacy and civil liberties impact assessments to the executive and city council to assist in their assessment of surveillance technologies.

In Berkeley, the Police Review Commission ("PRC") has a chance to review surveillance use policies and surveillance acquisition reports and vote to recommend their approval, object to their contents, or recommend changes. PRC is an independent civilian oversight agency that advises city leaders and the Berkeley Police Department on police practices and investigates complaints by members of the public against police officers. It is composed of nine members

53 Id.
54 Id. § 9.64.020(3).
59 Id. § 14.18.080(A)(3).
60 Id. § 14.18.080(B).
appointed by the mayor and city council.\textsuperscript{63} Although PRC has a chance to provide input on surveillance technology decisions, the ordinance specifies that the review may proceed regardless of whether the PRC objects to or approves of a surveillance technology proposal.\textsuperscript{64}

G. What enforcement mechanisms exist to encourage compliance?

Most of the ordinances include one or more provisions providing a remedy for violations of the ordinance. Across the sixteen ordinances, we observed five different types of enforcement mechanisms. First, some ordinances create a private right of action that allows persons to sue the responsible government body for violating the ordinance. Second, some make it a misdemeanor for an official to intentionally violate the terms of the ordinance. Third, some include a suppression remedy that allows parties in lawsuits to seek to exclude evidence collected in violation of the ordinance. Fourth, some include a provision that imposes discipline on employees who violate the terms of the ordinance. And fifth, some require termination or suspension of contracts that violate the ordinance.

Ordinances may adopt none, some, or all of these approaches. Of the sixteen ordinances, eleven include one or more enforcement mechanism.\textsuperscript{65} The most common mechanism is creating a private right of action, which the majority include.\textsuperscript{66} Lawrence, Massachusetts includes the widest range of enforcement mechanisms, with four available (the one enforcement mechanism excluded is making a violation a misdemeanor).\textsuperscript{67}

\textsuperscript{63} Id.

\textsuperscript{64} § 2.99.030(2) (Berkeley).


\textsuperscript{66} § 2.99.090 (Berkeley); § 2.128.080 (Cambridge); § 26.07.070 (Davis); § 9.25.090 (Lawrence); § 9.64.050 (Oakland); § 19B.8(b) (S.F.); § 17-509 (BART); § A40-10 (Santa Clara); § 14.18.070(B) (Seattle); § 10-67(C) (Somerville).

\textsuperscript{67} §§ 9.25.100, 9.25.110 (Lawrence).
1. The ordinance creates a private right of action in the event of a breach.

Of the sixteen ordinances, ten provide a private right of action when the government fails to correct violations. The Davis ordinance, for example, says: “Any violation of this article constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this article.” But “prior to the initiation of any legal proceeding . . . the City of Davis shall be given written notice of the violation(s) and an opportunity to correct such alleged violation(s) within thirty days of receipt of the notice.” As illustrated by the Davis ordinance, these provisions typically give officials notice and an opportunity to comply with the ordinance before the aggrieved party can sue.

The right of action provisions vary as to the kind of relief they provide. For example, in addition to injunctive relief, the Berkeley ordinance allows a “prevailing complainant in an action for relief [to] collect from the City reasonable attorney’s fees in an amount not to exceed $15,000.” In contrast, the Seattle ordinance does not provide for the recovery of attorney’s fees but allows proceedings for “injunctive relief, declaratory relief, or a writ of mandate.” The Oakland ordinance allows “[a]ny person who has been subjected to a surveillance technology in violation of [the] Ordinance . . . to recover actual damages,” as well as costs and reasonable attorney’s fees.

The provisions also differ as to what a person must prove in court to successfully show actionable harm. The Seattle ordinance, for example, limits recovery to “[a]ny person who is surveilled and injured by a material violation of [the ordinance] that is a proximate cause of the injury.” In contrast, the Somerville, Massachusetts ordinance expressly does not limit the right of action to an injured party, stating that “[a]ny violation of [the ordinance] constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this article.”

---

68 § 2.99.090 (Berkeley); § 2.128.080 (Cambridge); § 26.07.070 (Davis); § 9.25.090 (Lawrence); § 9.64.050 (Oakland); § 19B.8(b) (S.F.); § 17-509 (BART); § A40-10 (Santa Clara); § 14.18.070(B) (Seattle); § 10-67(C) (Somerville).

69 § 26.07.070(a) (Davis).

70 Id. § 26.07.070(a)(1).


74 § 14.18.070(B) (Seattle).

75 Somerville, Mass., Mun. Code § 10-67(c) (2019); see also § 9.64.050(1)(A) (Oakland) (“Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes
2. **The ordinance creates a misdemeanor that can be prosecuted in the event of breach.**

Two jurisdictions—Davis and Santa Clara, California—make breaching the ordinance a misdemeanor.\(^76\) Santa Clara’s relevant provision states:

> It shall be a misdemeanor to intentionally use County-owned surveillance technology (1) for a purpose or in a manner that is specifically prohibited in a Board-approved Surveillance Use Policy, or (2) without complying with the terms of this Division with respect to that County-owned surveillance technology. Unless otherwise prohibited by law, either the District Attorney or County Counsel may prosecute a violation of this Division.\(^77\)

This provision gives the District Attorney or County Counsel the option of prosecuting officials who intentionally violate the ordinance’s requirements.\(^78\) In Davis, it is a misdemeanor to “willfully and maliciously violate” the ordinance.\(^79\)

3. **The ordinance creates a suppression remedy.**

Lawrence and Somerville’s ordinances create a suppression remedy for evidence collected in violation of the ordinance.\(^80\) To illustrate, in Somerville, “[n]o data collected or derived from any use of surveillance technology in violation of this article and no evidence derived therefrom may be received in evidence in any proceeding . . . subject to the jurisdiction of the City of Somerville.”\(^81\) A prosecutor would therefore not be able to introduce evidence obtained in violation of the ordinance at a criminal trial. None of the ordinances from California jurisdictions include a suppression remedy, perhaps because the California Constitution requires special an injury and any person may institute proceedings . . .”). \(^{76}\) But see Cambridge, Mass., Mun. Code § 2.128.080(B) (2018) (stating that “[a]ny person injured by a violation of this Chapter may institute proceedings” without defining “injured”).


\(^{77}\) § A40-12 (Santa Clara).

\(^{78}\) See id.

\(^{79}\) § 26.07.070(c) (Davis).


\(^{81}\) § 10-67(b) (Somerville).
legislative authorization for any suppression remedy beyond what the federal Constitution requires.\(^\text{82}\)

4. Employees who violate provisions can be disciplined.

Three of the ordinances—Oakland, Lawrence, and Yellow Springs, Ohio—provide employment consequences, such as suspension or termination, for government employees who violate the ordinance.\(^\text{83}\) In Oakland, for example, violations by a “city employee shall result in consequences that may include retraining, suspension, or termination.”\(^\text{84}\) The Lawrence ordinance states that “[a]ny municipal employee who violates the provisions of this chapter, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment.”\(^\text{85}\)

5. Contracts that violate the ordinance will be delayed or canceled.

Of the sixteen ordinances, five allow for or require the termination or suspension of contracts that violate the ordinance.\(^\text{86}\) The Yellow Springs ordinance, for example, specifies that “[a]ny contracts or agreements signed before the enactment of this Chapter that violate this Ordinance must be terminated as soon as legally possible.”\(^\text{87}\)

H. Are there exceptions to the reporting and approval requirements?

Almost all the surveillance oversight ordinances include exceptions to the reporting and approval requirements that apply under certain circumstances. There are five main categories of exceptions. First, there is often an exception for exigent circumstances. Second, many ordinances include limited exceptions that apply to certain law enforcement technology or data acquisition from third parties. Third, some ordinances allow surveillance and data collection with consent or when the public has the opportunity to opt-out. Fourth, some ordinances include an exception to approval requirements when city actors update their existing technology. Fifth, one ordinance includes an exception for large-scale events. And sixth, one ordinance exempts sensitive information.

\(^{82}\) Cal. Const. art. I, § 28(f)(2) (“Except as provided by statute hereafter enacted by a two-thirds vote of the membership in each house of the Legislature, relevant evidence shall not be excluded in any criminal proceeding . . .”).


\(^{84}\) § 9.64.050(1)(D) (Oakland).

\(^{85}\) § 9.25.100(B) (Lawrence).


\(^{87}\) § 607.08(a) (Yellow Springs).
1. In exigent circumstances, departments can temporarily bypass approval requirements.

Of the sixteen ordinances, fourteen include an exception for exigent circumstances. If a qualifying emergency need arises, these provisions allow government actors to use surveillance technology typically covered by the ordinance’s restrictions without meeting the ordinance’s usual requirements. The precise definition of exigent circumstances differs between jurisdictions. And some jurisdictions have stricter process requirements than others when government officials rely on the exigent circumstances exception.

The definitions of exigent circumstances vary. The Berkeley ordinance, for example, defines “exigent circumstances” as the “City Manager’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires use of the Surveillance Technology or the information it provides.” In contrast, the Santa Clara definition does not include property damage as a circumstance justifying the exception: “‘Exigent Circumstances’ means the County Sheriff’s Office or District Attorney’s Office’s good faith belief that an emergency involving danger of death or serious physical injury to any person requires use of the surveillance technology or the information it provides.”

---


89 Compare, e.g., § 2.99.020(5) (Berkeley) (“‘Exigent Circumstances’ means the City Manager’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires use of the Surveillance Technology or the information it provides.”), with § A40-7(f) (Santa Clara) (“‘Exigent Circumstances’ means the County Sheriff’s Office or District Attorney’s Office’s good faith belief that an emergency involving danger of death or serious physical injury to any person requires use of the surveillance technology or the information it provides.”).

90 Compare, e.g., § 2.99.040(1) (requiring Berkeley City Manager to notify City Council within 30 days of triggering exception), with § 10-64(a) (requiring Somerville Police Department to notify City Council within 90 days of triggering exception).

91 § 2.99.020(5) (Berkeley).

92 § A40-7(f) (Santa Clara).
The Somerville ordinance ties the exigent circumstances definition to the exigent circumstances exception to the warrant requirement as defined by case law: “Exigent Circumstances means the police chief’s or the police chief’s designee’s good faith and reasonable belief that an emergency involving danger of death, physical injury, or significant property damage or loss, similar to those that would render impracticable to obtain a warrant, requires use of the surveillance technology or the surveillance data it provides.” Under this case law-defined exception, law enforcement may search a person or place without a warrant to prevent the imminent destruction of evidence, to assist persons who are seriously injured and in need of assistance, and under other exigent circumstances.

Once government actors trigger the exigent circumstances exception, jurisdictions also have varying process requirements. The Berkeley ordinance, for example, requires the city manager to notify City Council in writing within thirty days of relying on the exigent circumstances exception and to then seek approval if the city anticipates continued use. In contrast, the Somerville ordinance allows the police department ninety days to give notice to City Council and to then follow normal policy and reporting procedures, although City Council may also grant extensions of the ninety-day period. Yellow Springs has the shortest window for emergency use, requiring Council approval within “96 hours following the declaration of . . . an emergency” and a report within ten days.

Not every ordinance specifies a time limit on emergency use. Madison, Wisconsin’s ordinance, for example, allows emergency use to continue indefinitely as long as the exigent circumstances themselves continue, and Council approval is only required “within thirty (30) days of cessation of the risk that prompted purchase of said Technology.”

---

93 § 10-62 (Somerville) (second emphasis added).
98 Yellow Springs, Ohio, Mun. Code § 607.06(B) (2018); see also Davis, Cal., Mun. Code § 26.07.050(e) (2018) (“Any technology temporarily acquired in exigent circumstances shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the city council for approval . . .”); Oakland, Cal., Mun. Code § 9.64.035(3) (2021) (same); S.F., Cal., Admin. Code § 19B.7(a)(2) (2019) (same).
2. Exceptions made for certain law enforcement technologies and investigations.

In addition to the agency-exemption provisions discussed in Part III(B)(2) and to the exigent circumstances exception, which exempt law enforcement agencies from coverage under certain circumstances, there are two narrower types of exceptions that in practice allow law enforcement to use or acquire unapproved surveillance technology or the data it produces.

The first is an exception for specific technology, such as body-worn cameras or cameras mounted on police cruisers, that law enforcement agencies use. Six ordinances include these kinds of exceptions. The Seattle ordinance, for example, states that “[b]ody-worn cameras” and “[c]ameras installed in or on a police vehicle” “constitute surveillance technology but the [ordinance’s requirements] do not apply to them.” Madison’s ordinance, like many others, creates a limited law enforcement exception in its definition of “surveillance technology” by specifying that the definition does not encompass “Police Department interview rooms, holding cells, and Police Department internal security audio/video recording systems.”

The second is a limited exception that allows third parties to provide information to law enforcement when doing so does not conflict with any other provision of the ordinance. Davis and Oakland’s ordinances include this provision. To illustrate, the Oakland ordinance states: “Notwithstanding any other provision of this section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.” This allows third parties to turn over information to law enforcement that they have collected themselves.


101 § 14.18.030(B) (Seattle); see also § 10-63(b)(4) (Somerville).

102 § 23.63(2)(18) (Madison).

103 § 26.07.030(e) (Davis); § 9.64.030(1)(E) (Oakland).

104 § 9.64.030(1)(E) (Oakland).
3. Exception for data collection to which the public consents or can opt-out.

Six ordinances allow government entities to collect surveillance data where members of the public have consented to the data collection, or where they have been given a chance to opt out of it.\(^\text{105}\) Cambridge, for example, which has a typical provision, excepts “Surveillance Data acquired where the individual knowingly and voluntarily consented to provide the information, such as submitting personal information for the receipt of City services.”\(^\text{106}\) It also includes an exemption for “Surveillance Data acquired where the individual was presented with a clear and conspicuous opportunity to opt out of providing the information.”\(^\text{107}\)

4. Exception for departments to apply technical patches without approval.

Five ordinances relax their approval requirements for technical patches or upgrades to existing surveillance technology.\(^\text{108}\) But these exceptions generally only apply for a limited time and still involve some government oversight. To illustrate, the Cambridge ordinance states that a “City department head may, with approval of the City Manager, apply a technical patch or upgrade that is necessary to mitigate threats to the City’s environment. The department shall not use the new surveillance capabilities of the technology until the [standard approval requirements] are met, unless the City Manager determines that the use is unavoidable; in that case, the City Manager shall request City Council approval as soon as possible.”\(^\text{109}\)

Madison’s ordinance includes a technical patch provision that allows a city department to “apply a technical patch or upgrade that is necessary to mitigate threats to the City’s infrastructure, even if the patch or upgrade materially alters the surveillance capabilities of the technology.”\(^\text{110}\) But, “if such patch or upgrade does materially alter the surveillance capability of the technology, it must be highlighted in the Annual Surveillance Technology Report.”\(^\text{111}\)


\(^{106}\) § 2.128.070(A)(1) (Cambridge).

\(^{107}\) Id. § 2.128.070(A)(2).


\(^{109}\) § 2.128.070(B)(2) (Cambridge).

\(^{110}\) § 23.63(6)(c) (Madison).

\(^{111}\) Id.
5. Exception for large-scale events.

Oakland is unique in that it allows the use of unapproved surveillance technology during a “large-scale event.”\textsuperscript{112} The ordinance defines “large-scale event” as “an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.”\textsuperscript{113}

6. Exception for sensitive information.

Madison’s ordinance also provides a unique exception for “sensitive” surveillance technology information. “Sensitive Surveillance Technology Information” is “any information about Surveillance Technology of which public disclosure would unreasonably expose or endanger City infrastructure; would adversely impact operations of City departments; or may not be legally disclosed.”\textsuperscript{114} The exemption states: “Sensitive Surveillance Technology Information is exempt from the requirements in the ordinance. Departments will provide the basis for exemption to the Information Technology Director. The Information Technology Director will notify the Mayor and Common Council Leadership of the exemption for mayoral approval.”\textsuperscript{115}

IV. Conclusion

This survey of sixteen surveillance technology oversight ordinances reveals a number of core elements these ordinances contain, some similar across the ordinances and others differing significantly. With important exceptions, these ordinances cover most departments in a jurisdiction and set broad requirements for reporting and overseeing the use of surveillance technology. Most of the ordinances provide an exception for government to use surveillance technology in exigent circumstances and at least partially exempt law enforcement agencies from coverage. The greatest points of variance are whether the ordinances apply retroactively, whether an independent body exists to enforce the ordinance, the enforcement mechanisms, and the exceptions. Looking at the text of the ordinances allows for the generation of hypotheses about which ordinances are likely to be more effective at facilitating public input and public oversight of local surveillance technology use, which are likely to be more burdensome to administer, and so forth. A more complete analysis of the effectiveness of these ordinances would investigate and test these hypotheses by looking beyond the text of the ordinances themselves.

\textsuperscript{112} Oakland, Cal., Mun. Code § 9.64.035 (2021).
\textsuperscript{113} Id. § 9.64.010(8).
\textsuperscript{114} § 23.63(2) (Madison).
\textsuperscript{115} Id. § 23.63(6)(d).
<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>California</th>
<th>Massachusetts</th>
<th>Michigan</th>
<th>New York</th>
<th>Ohio</th>
<th>Tennessee</th>
<th>Washington</th>
<th>Wisconsin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Santa Clara County</td>
<td>City of Berkeley</td>
<td>City of Davis</td>
<td>City of Oakland</td>
<td>City of Palo Alto</td>
<td>City and County of San Francisco</td>
<td>City of Lawrence</td>
<td>City of Cambridge</td>
</tr>
<tr>
<td>Does the ordinance define surveillance technology?</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Which departments are regulated?</td>
<td>All departments are regulated by the ordinance.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Some departments are regulated by the ordinance / different rules apply to law enforcement.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>One department is regulated by the ordinance.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>What reports and policies are required?</td>
<td>Surveillance use policies are required.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Surveillance impact report is required.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Annual report on surveillance practices and policies is required.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Does an elected body review or approve ordinance reports and policies?</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Does the ordinance apply retroactively?</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Does the ordinance reference an independent body that assists in reviewing surveillance technology?</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>What enforcement mechanisms exist to encourage compliance?</td>
<td>The ordinance creates a private right of action in the event of breach.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>The ordinance creates a misdemeanor that can be prosecuted in the event of breach.</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>The ordinance creates a suppression remedy.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Employees who violate provisions can be disciplined.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Contracts that violate the ordinance may be delayed or canceled.</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>What exceptions are there to the ordinance’s requirements?</td>
<td>In exigent circumstances, departments can temporarily bypass approval requirements.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Exceptions made for certain law enforcement technologies and investigations.</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Exception for data collection to which the public consents or can opt-out.</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Exception for departments to apply technical patches without approval.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Exception for large-scale events.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Exception for sensitive information.</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>