NEW CCOPS ON THE BEAT

An Early Assessment of Community Control of Police Surveillance Laws

STEVIE DEGROFF, ESQ.
ALBERT FOX CAHN, ESQ.

FEBRUARY 10TH, 2021

STOP SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT
Hogan Lovells

I. Introduction

This report summarizes the current state of local laws governing police use of surveillance technology. An increasing number of state and local municipalities have adopted ordinances which limit or create oversight over the acquisition and use of surveillance technology such as facial recognition software, drones, predictive software, and cellphone tracking. While these ordinances are new, early compliance efforts appear to offer increasing public insight into and municipal control over technologies that many citizens are not aware are even being used in their communities.

Subsequent sections provide a brief overview of local police use of advanced surveillance technology, trends in current local and state laws that limit or regulate the use of surveillance technology by police, and what impact these ordinances have had to date.

II. Background: Local Police Use of Technology

The past few years have seen an explosion in both (a) the application of advanced technologies like artificial intelligence and machine learning in law enforcement contexts as well as (b) increased adoption of such technologies by local police forces. This includes technologies such as facial recognition software, video analytics, social media tracking, predictive policing software, cell phone tracking, drones, and surveillance cameras. This has coincided with a dramatic increase in the market for such technologies. For example, the global facial recognition market was valued at $3.4B USD in 2019 and is expected to expand 14.5% from 2020-2027.[1] Similarly, the video surveillance market is expected to grow from $45.5B USD in 2020 to $74.6B USD by 2025.[2]

The Atlas of Surveillance shows over 6,300 instances of advanced surveillance technology in use by local law enforcement across the United States.[3] This includes everything from body cameras, automated license plate readers, and drones to gunshot detection, predictive policing tools, and facial recognition software. These new technologies are often acquired and used without community input or notice – and can be difficult to uncover even through public record requests.[4] Local police are also increasingly using citizen generated surveillance through applications like Neighbors.[5]

---

[1] Grand View Research, *Facial Recognition Market Size, Industry Report, 2020-2027* (Mar. 2020), *available at* https://www.grandviewresearch.com/industry-analysis/facial-recognition-market.

[2] Markets and Markets, *Video Surveillance Market – Global Forecast to 2025 (Apr. 2020)*, *available at* https://www.marketsandmarkets.com/PressReleases/global-video-surveillance-market.asp.

[3] Atlas of Surveillance, Electronic Frontier Foundation and the University of Nevada, Reno, https://atlasofsurveillance.org/atlas (last visited Dec. 9, 2020).

[4] Conor Friedersdorf, *The Undemocratic Spread of Big Brother*, The Atlantic (May 23, 2018), https://www.theatlantic.com/ideas/archive/2018/05/the-undemocratic-spread-of-big-brother/560999/; Rebecca Heilweil, *Why we don't know as much as we should about police surveillance technology*, Vox (Feb. 5, 2020), https://www.vox.com/recode/2020/2/5/21120404/police-departments-artificial-intelligence-public-records; Clare Garvie, et al., *The Perpetual Line-Up*, Geo. L. Ctr. on Priv. & Tech. (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.

[5] Jamie Siminoff, *Working Together for Safer Neighborhoods: Introducing the Neighborhoods Active Law Enforcement Map*, ring.com (Aug. 28, 2019), https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/ (noting that 405 agencies use the Neighbors Portal to post information about crime events and seek help on active investigation but requesting video recordings from users).

As the use of these advanced surveillance technologies has increased, so has criticism based on the lack of transparency and the potential for bias and abuse.[6] This is particularly true for technologies that rely on algorithms. Extensive research has demonstrated bias in both predictive policing[7] and facial recognition software.[8]

These concerns have been amplified recently as law enforcement deployed these technologies against protestors throughout the United States in 2020.[9] Increasingly, community groups, elected officials, and non-profits are calling for insight into and control over how local law enforcement uses such technology. In 2016, the ACLU proposed sample Community Control Over Police Surveillance (CCOPS) legislation, which would give local city councils control over the purchase and use of such technology, as well as additional insight into the contracts between local police departments and the private companies who develop these technologies.[10] This sample legislation has served as a model in many local municipalities. While not all elements have been adopted wholesale, similar types of regulations have been adopted across the United States.

III. Current Law Enforcement Technology Oversight

As of January 2021, at least 25 municipal government entities have passed legislation governing law enforcement's use of new technology. Of these, 13 have included targeted bans on the use facial

---

[6] *See e.g.* Will Douglas Heaven, *Predictive policing algorithms are racist. They need to be dismantled.*, MIT Tech. Rev. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/; Malkia Devich-Cyril, *Defund Facial Recognition*, The Atlantic (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/; Andrew Guthrie Ferguson, *High-tech Surveillance Amplifies Police Bias and Overreach*, Gov. Tech. (June 12, 2020), https://www.govtech.com/public-safety/High-Tech-Surveillance-Amplifies-Police-Bias-and-Overreach.html; Hannah Devlin, '*We are hurting towards a surveillance state': the rise of facial recognition technology*, The Guardian (Oct. 5, 2019), https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state.

[7] *See e.g.* Rashida Richardson, Jason M. Schultz, & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. 192 (2019), *available at* https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_etal-FIN.pdf; Will Douglas Heaven, *Predictive policing algorithms are racist. They need to be dismantled*, MIT Tech. Rev. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/; Julia Angwin, et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[8] *See e.g.* Claire Garvie, *Garbage In, Garbage Out*, Geo. L. Ctr. on Priv. & Tech. (May 16, 2019), https://www.flawedfacedata.com/; Natasha Singer and Cade Metz, *Many Facial-Recognition Systems are Biased, Says U.S. Study*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html (reporting that the National Institute of Standards and Technology report showed the majority of commercial facial-recognition systems falsely identified African-American and Asian faces 10 times to 100 times more than Caucasian faces.); Joy Buolamwini & Timnit Gebru, *Gender Shades Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research 1-15 (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[9] Katie Schoolov, *As protests over the killing of George Floyd continue, here's how police use powerful surveillance tech to track them*, CNBC (Jun. 18, 2020), https://www.cnbc.com/2020/06/18/heres-how-police-use-powerful-surveillance-tech-to-track-protestors.html.

[10] ACLU, *Community Control Over Police Surveillance (CCOPS)*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance (last visited Dec. 10, 2020).

recognition software[11] and 15 have included more general regulations over the acquisition or use of new technology by local law enforcement.[12] Each of these laws provide some degree of insight into the impact of local control over law enforcement's use of advanced surveillance technologies.

---

[11] Alameda, Cal., Resolution 2019-7533 (Dec. 17, 2019), https://alameda.legistar.com/LegislationDetail.aspx?ID=4273393&GUID=F515A75C-2EB6-4CF8-A0A1-749610C379F8&Options=&Search=; BERKELEY, CAL., MUN. CODE, ACQUISITION AND USE OF SURVEILLANCE TECH., § 2.99.030 ET SEQ., https://www.codepublishing.com/CA/Berkeley/html/Berkeley02/Berkeley0299/Berkeley0299.html; S.F., CAL., S.F. ADMIN. CODE, ACQUISITION OF SURVEILLANCE TECH., CHAPTER 19B ET SEQ., https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320; Bos., Mass., Ordinance Banning Face Surveillance Tech. in Boston, Ordinance 16-62 (effective Jun. 24, 2020), https://www.universalhub.com/files/recognitionban.pdf (at 3); Brookline, Mass., Article 8.39 (Nov. 5, 2019), https://www.brooklinema.gov/DocumentCenter/View/20733/November-2019-Special-Town-Meetings-Supplements-Night-1 (at 12); CAMBRIDGE, MASS., SURVEILLANCE TECH. ORDINANCE, TITLE 2, CHAPTER 2.128 (Nov. 10, 2018), http://cambridgema.iqm2.com/Citizens/Detail_LegiFile.aspx?MeetingID=2399&ID=9847; NORTHAMPTON, MASS., CODE OF ORDINANCES, SURVEILLANCE SYSTEMS, PART II, CHAPTER 290 ET SEQ., https://ecode360.com/13265223; SOMERVILLE, MASS., BAN ON FACIAL RECOGNITION, ORDINANCE NO. 2019-16 (ordained June 27, 2019), *available at* http://somervillecityma.iqm2.com/Citizens/Detail_Meeting.aspx?ID=2941 (agenda item 208142); SPRINGFIELD, MASS., CITY COUNCIL CODE OF ORDINANCES, BANS ON FACIAL RECOGNITION SURVEILLANCE TECH., ORDINANCE , ORD-2020-1 (adopted Feb. 24, 2020), http://springfieldcityma.iqm2.com/Citizens/Detail_Meeting.aspx?ID=4001; S.2963 § 26, 191st Gen. Ct. (Ma. 2020), *available at* https://malegislature.gov/Bills/191/S2963?=11302020; PORTLAND, ME., CODE OF ORDINANCE, §17-1, CHAPTER 17, ARTICLE XI ET SEQ., https://www.portlandmaine.gov/DocumentCenter/View/1083/Chapter-17-Offenses-Miscellaneous-Provisions---Revised-1132020; PORTLAND, OR., PROHIBITS THE ACQUISITION AND USE OF FACE RECOGNITION TECHNOLOGIES BY CITY BUREAUS ORDINANCE, ORDINANCE 190113 (Sept. 9, 2020), *available at* https://efiles.portlandoregon.gov/Record/13945278/.

[12] S.F. Bay Area Rapid Transit Dist., Memorandum from Gen. Couns. to Bd. of Dirs., *Surveillance Tech. Ordinance (2nd Reading)* §4 (Sept. 21, 2018), https://www.bart.gov/sites/default/files/docs/BART%20Surveillance%20Technology%20Ordinance%20%28Second%20Reading%20for%20Ordinance%29.pdf; BERKELEY, CAL., MUN. CODE, § 2.99; DAVIS, CAL., MUN. CODE, SURVEILLANCE TECH., CHAPTER 26, ARTICLE 26.07 ET SEQ., http://qcode.us/codes/davis/view.php?topic=26-26_07; OAKLAND, CAL., CODE OF ORDINANCES, REGULS. ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECH., CHAPTER 9.64 ET SEQ., https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUSSUTE; PALO ALTO, CAL., MUN. CODE, § 2.30.630 ET SEQ., https://codelibrary.amlegal.com/codes/paloalto/latest/paloalto_ca/0-0-0-55386; S.F., CAL., S.F. ADMIN. CODE, ACQUISITION OF SURVEILLANCE TECH., CHAPTER 19B ET SEQ., https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320; SANTA CLARA, CAL., CODE OF ORDINANCES, SURVEILLANCE – TECH. AND CMTY – SAFETY, TITLE A, DIV. A40 ET SEQ., https://library.municode.com/ca/santa_clara_county/codes/code_of_ordinances?nodeId=TITAGEAD_DIVA40SUECCOAF; CAMBRIDGE, MASS., SURVEILLANCE TECH. ORDINANCE, TITLE 2, CHAPTER 2.128 (Nov. 10, 2018), http://cambridgema.iqm2.com/Citizens/Detail_LegiFile.aspx?MeetingID=2399&ID=9847; LAWRENCE, MASS., CODE OF ORDINANCES, SURVEILLANCE TECH., TITLE 9, CHAPTER 9.25 ET SEQ., https://library.municode.com/ma/lawrence/codes/code_of_ordinances?nodeId=TIT9PUPEWE_CH9.25SUTE; SOMERVILLE, MAS., EXEC. POL'Y, POL'Y ON SURVEILLANCE TECH. (Oct.4, 2017), https://www.somervillema.gov/sites/default/files/surveillance-technology-executive-policy.pdf; N.Y.C., N.Y., N.Y.C. ADMIN. CODE, ANN. SURVEILLANCE REPORTING AND EVALUATION, § 14-188 ET SEQ., https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-124303; YELLOW SPRINGS, OHIO, CODE OF ORDINANCES, USE OF SURVEILLANCE TECH., CHAPTER 607 ET SEQ., https://codelibrary.amlegal.com/codes/yellowsprings/latest/yellowsprings_oh/0-0-0-23917#JD_Chapter607; NASHVILLE, TENN., METRO GOV'T OF NASHVILLE AND DAVIDSON CNTY., TENN., TITLE 13, DIV. 1, CHAPTER 13.08.080, https://library.municode.com/tn/metro_government_of_nashville_and_davidson_county/codes/code_of_ordinances?nodeId=CD_TIT13STSIPUPL_DIVIGERE_CH13.08STALSI_13.08.080DESUELDAGADEONPURI-WREMECOAP; SEATTLE, WASH., MUN. CODE, ACQUISITIONS AND USE OF SURVEILLANCE TECH., TITLE 14, CHAPTER 14.18 ET SEQ., https://library.municode.com/wa/seattle/codes/municipal_code?nodeId=TIT14HURI_CH14.18ACUSSUTE;

a. Facial Recognition Bans

In 2019, San Francisco became the first city to ban the use of facial recognition technology by local law enforcement. Eleven cities and one state have since followed suit, with legislation being introduced in Congress to limit federal use of facial recognition technology.[13] While some jurisdictions have passed standalone facial recognition legislation, San Francisco enacted its facial recognition law as a component of a broader CCOPS law. In 2020, 19 state legislatures considered regulations limiting the use of biometrics, like facial recognition software, by law enforcement.[14] While there has been extensive media coverage of the adoption of these laws, many are not full bans. As outlined below, most allow for an exception when information obtained through facial recognition software is shared by a third party, such as the federal government or private businesses. This exception has drawn expanded public criticism from civil rights groups and civil society organizations, with some noting the danger that the use of such third-party facial recognition exceptions could become routine.[15] The majority of these regulations went into effect within the last twelve months. Required reporting on their use and impact, and potential litigation where private rights of action are allowed, is still forthcoming.

Local governments in California and Massachusetts have been particularly active in passing bans on the use of facial recognition technology. In California, four municipalities have banned the use of facial recognition technology. The Berkeley Chief of Police specifically highlighted this policy in a special order, noting that the use of Clearview (a private provider of such technology) was prohibited by the ordinance.[16] Many California municipalizes ban the use of facial recognition technology but allow for the use of information obtained from such technology if it is shared, unsolicited, by a third party and it relates to the investigation of a specific crime. Several California municipalities also require some sort of reporting regarding the information obtained from facial recognition technology. However, as many of these ordinances were passed in 2019, information regarding the use of such technology or receipt of information created by facial recognition technology was not included in the reports produced so far.[17]

MADISON GEN. ORD. § 5.19-5.20, https://madison.legistar.com/LegislationDetail.aspx?ID=4628948&GUID=2AE7E769-4795-4BF3-9D07-1826D08BCEFC&Options=ID%7CText%7C&Search=oversight+board&FullText=1.

[13] Facial Recognition and Biometric Technology Moratorium Act of 2020, S.4084, 116th Cong. (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084; Ethical Use of Facial Recognition Act, S.3284, 116th Cong. (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/3284.

[14] Pam Greenberg, *Spotlight: Facial Recognition Gaining Measured Acceptance*, Nat'l Conf. of State Legislatures (Sep. 18, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx.

[15] Alfred Ng, *Police Say They Can Use Facial Recognition, Despite Bans*, The Markup (Jan. 28, 2021), https://themarkup.org/news/2021/01/28/police-say-they-can-use-facial-recognition-d.espite-bans.

[16] Berkeley, Cal. Police Dept., Policy 1105, Special Order 200-0005 (July 21, 2020), https://www.cityofberkeley.info/uploadedFiles/Police/Level_3_-_General/Special_Order_2020-0005.pdf.

[17] For example, the Berkeley ordinance was passed in October 2019 and the annual surveillance report published in November of 2019 and accepted by the City Council in January 2020 did not include information. City of Berkeley, Cal, *Surveillance Technology Report , Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras* (Nov. 12, 2019), *available at* https://www.cityofberkeley.info/Clerk/City_Council/2019/11_Nov/Documents/2019-11-12_Item_30_Surveillance_Technology_Report.aspx.

In Massachusetts, six municipalities have passed various degrees of bans on facial recognition technology.[18] Many of these ordinances go further than those in California, and specifically call for the exclusion of evidence obtained in violation of these policies. In December 2020, the Massachusetts state legislature passed a bill which, if signed by the governor, will make it unlawful for any public agency in the state to use facial recognition technology or "any computer software that performs . . . remote biometric recognition."[19] However, this measure was later amended and severely curtailed by the Governor.[20] Like the local ordinances in Massachusetts, the law further prevents any information obtained in violation of the law from being used in a judicial proceeding. However, the revised law allows for the use of facial recognition technology under many circumstances. Police may request the Massachusetts registrar of motor vehicles perform a facial recognition search, subject to a warrant or a sworn statement as to the necessity of such search in an emergency, and the registrar of motor vehicles must publish an annual report containing the total number of facial recognition searches conducted on behalf of the police both pursuant to a warrant or in an emergency. However, like many of the local laws in California and elsewhere, this law also makes an exception for receiving third-party facial recognition evidence as long as it was not knowingly solicited.

Outside of these two states, only a few other municipalities have implemented facial recognition bans. Both Portland, Oregon and Portland, Maine allow for a private right of action for violation of their laws, with Portland, Maine providing for penalties up to $1,000 plus attorney's fees for a violation of the regulation.[21] Portland, Oregon allows for citizens harmed by a violation of this ordinance to bring a legal proceeding after giving notice to the City and allowing 30 days to cure the violation. [22] They also require reporting on the current use of facial recognition technology. In December 2020, New Orleans City Council also passed a law banning police use of facial recognition technology as well as predictive policing technology, cell-cite simulators, and characteristic recognition and tracking software.[23] This legislation was pared down from the original version, which would have created comprehensive approval and a reporting process for the use of surveillance technology in the city.[24] While the current law passed without these elements, it does still require the police to designate a Data Protection Officer to ensure compliance.[25]

---

[18] SOMERVILLE, MASS., ORDINANCE NO. 2019-16; Northampton, Mass., Ordinance Prohibiting the Use of Face Surveillance Systems, Ordinance 19.176 (2019), https://www.northamptonma.gov/AgendaCenter/ViewFile/Item/13774?fileID=130290; SPRINGFIELD, MASS., CITY COUNCIL CODE OF ORDINANCES, ORDINANCE , ORD-2020-1; Bos., Mass., Ordinance 16-62; CAMBRIDGE, MASS., TITLE 2, CHAPTER 2.128.

[19] S.2963 § 26, 191st Gen. Ct. (Ma. 2020).

[20] Steph Solis, *Massachusetts Passes Bill With Facial Recognition Rules*, GovTech.com (Dec. 22, 2020), https://www.govtech.com/policy/Massachusetts-Passes-Bill-With-Facial-Recognition-Rules.html.

[21] PORTLAND, ME., CODE OF ORDINANCE, §17-1, CHAPTER 17, ARTICLE XI.

[22] PORTLAND, OR., ORDINANCE 190113.

[23] New Orleans, La., Ordinance 33,021 (passed Dec. 17, 2020), https://cityofno.granicus.com/MetaViewer.php?view_id=&event_id=22991&meta_id=513815) (amended, *see* https://cityofno.granicus.com/MetaViewer.php?view_id=&clip_id=3745&meta_id=518894; https://cityofno.granicus.com/MetaViewer.php?view_id=&clip_id=3745&meta_id=518891).

[24] Michael Isaac Stein, *New Orleans City Council bans facial recognition, predictive policing and other surveillance tech*, TheLensNola.org (Dec. 18, 2020), https://thelensnola.org/2020/12/18/new-orleans-city-council-approves-ban-on-facial-recognition-predictive-policing-and-other-surveillance-tech/.

[25] New Orleans, La., Ordinance 33,021, §159-4(f).

Table 1: Facial Recognition Ban Local Ordinances

Location/Entity	Ban on use of facial recognition software	Exception for information received from third parties	Facial Recognition Reporting required	Private Right of Action	Evidentiary Exclusion
Alameda, CA	X	X			
Berkeley, CA	X	X	X		
San Francisco, CA	X				
Boston, MA	X	X		X	X
Brookline, MA	X	X			
Cambridge, MA	X	X	X		
Northampton, MA	X				
Somerville, MA	X			X	X
Springfield, MA	X				X
Massachusetts	X	X	X		X
New Orleans, LA	X	X			
Portland, ME	X			X	
Portland, OR	X		X	X	

While not a ban, Washington state's regulation concerning the use of facial recognition software requires public notice, at least three community meetings, and the creation of accountability reports before such technology can be adopted by a public agency.[26] The law further requires a warrant to use such technology and limits when and how it can be used by law enforcement, such as prohibiting its use based on sketches or its use as the sole basis to establish probable cause.

b. Acquisition and Use Regulation

As of December 2020, fourteen local governments and one regional government entity have passed legislation regulating the acquisition and use of surveillance technology. The following Table outlines the common elements of acquisition and use regulation municipalities have enacted to date:

Table 2: Surveillance Technology Acquisition and Use Ordinances

Location/Entity	Acquisition Approval	Annual Reports	Use Policy	NDA Ban	Private Right of Action
BART system, CA	X	X	X		X
Berkeley, CA	X	X	X		X
Davis, CA	X	X	X		X
Oakland, CA	X	X	X	X	X

[26] WASH., REVISED CODE OF WASH., FACIAL RECOGNITION, TITLE 43, CHAPTER 43.386, https://app.leg.wa.gov/RCW/default.aspx?cite=43.386.

Location/Entity	Acquisition Approval	Annual Reports	Use Policy	NDA Ban	Private Right of Action
Palo Alto, CA	X	X	X		*banned*
San Francisco, CA	X	X	X		X
Santa Clara County, CA	X	X	X		X
Cambridge, MA	X	X	X		X
Lawrence, MA	X	X	X	X	X
Somerville, MA	X	X	X		X
New York, NY		X	X		
Yellow Springs, OH	X	X	X	X	
Nashville, TN	X	X	X		
Seattle, WA	X	X	X	X	X
Madison, WI	X	X	X		

The vast majority of these ordinances require approval of specific surveillance technologies by the city council or another municipal body. Before adopting a new technology, police departments must submit reports with detailed information about how the technology works, how they intend to use it, and the potential impact on citizens. They are also often required to create and submit use policies as well as annual reports pertaining to any approved technology. These reports are typically required to be made publicly available and are often discussed in public meetings. Each of these provisions not only helps ensure oversight over the acquisition and use of advanced technologies, but also provides citizens with much needed transparency into the technology being deployed in their communities – and an opportunity to voice their support or opposition.

While ten municipalities allow individual citizens to sue for a violation of these ordinances, this right is typically limited and only comes into effect after notice of the violation is provided to local government and some period of time is allowed to cure the violation. Even less common are requirements to ban the use of non-disclosure agreements (NDAs) with private vendors. The majority of this technology is sold to local governments by private companies, which often require NDAs covering various aspects of the technology such as the data used in the creation of the tool. This can become problematic when defendants attempt to question the accuracy of a given tool in court.[27]

IV. Compliance and Impact

As previously noted, both facial recognition bans and more general law enforcement surveillance technology use regulations are relativity new. While many municipalities require approval, public notice and use policies, and annual reporting – these requirements have not yet taken effect. However, for the ordinances that have been in place long enough for reporting and public disclosure to have begun, they appear to have – at least initially – driven increased transparency about and control over local law enforcement use of surveillance technology.

[27] *See e.g.* Taylor R. Moore, *Trade Secrets & Algorithms as Barriers to Social Justice*, Center for Democracy and Technology (August 2017); *Wisconsin v. Loomis*, 371 Wis.2d 235 (Wisc. 2016), *cert. denied*, 85 U.S.L.W 3601 (U.S. Jun. 26, 2017) (No.16-6387); *People v. Superior Court (Chubbs)*, No. B258569, 2015 WL 139069, at *3, *7, *9-10 (Cal. Ct. App. Jan. 9, 2015).

For example, the Bay Area Rapid Transit (BART) system ordinance requires both public notice of a Surveillance Impact Report and draft Surveillance Use Policy before discussion for approval at the board meeting.[28] The process has been followed, with notice and proper documentation made available to the public before the April 25, 2019[29] and October 24, 2019[30] board meetings where surveillance technology was discussed and approved.[31] Additionally, the BART 2020 Annual Surveillance Report covers the initial period through June 30, 2020, and reviews the seven specific surveillance technologies in use by BART.[32]

Similarly, Oakland has reviewed and approved the use of seven technologies, all of which now have publicly available use policies and anticipated impact reports.[33] The use of each technology is discussed in detail at monthly meetings of the Privacy Advisory Commission, and use policies have not been adopted without question. For example, at the February 6, 2020 meeting the commission questioned and requested amendments to the Drone Exigent Use Report due to perceived violations of the ordinance, and referred the Impact Report and proposed Use Policy for the same technology to a special committee for additional review due to concerns about the use of the technology against large crowds.[34] The committee has also rejected reports for lacking detail and transparency.[35] After debates at three different Privacy Advisory Committee meetings, in December 2020 the Oakland City Council approved the Oakland police department drone surveillance policy and use.[36] However, the purchase of drones was limited to those with capabilities allowed in the use policy, and the police department cannot use city funds to purchase any drone devices. At this same meeting, the City Council banned the police use of biometric surveillance and predictive policing technology.

Similar to Oakland, Cambridge's ordinance requires city council approval for any new surveillance technology. Meeting notes do not contain as extended debates as those in Oakland, however the

---

[28] S.F. Bay Area Rapid Transit Dist., Memorandum from Gen. Couns. to Bd. of Dirs., *Surveillance Technology Ordinance (2nd Reading)* §4 (Sept. 21, 2018), https://www.bart.gov/sites/default/files/docs/BART%20Surveillance%20Technology%20Ordinance%20%28Second%20Reading%20for%20Ordinance%29.pdf.

[29] Bay Area Rapid Transit, *Notice of Discussion of proposed technology April* 25 (Apr. 9, 2019), https://www.bart.gov/news/articles/2019/news20190403.

[30] Bay Area Rapid Transit, *Notice of Discussion of proposed technology October 24* (Oct. 24, 2019) https://www.bart.gov/news/articles/2019/news20191009.

[31] S.F. Bay Area Rapid Transit Dist., Bd. of Dirs., Minutes of the 1,851st Meeting (Oct. 24, 2019), https://www.bart.gov/sites/default/files/docs/minutes/10-24-19%20Minutes.pdf; S.F. Bay Area Rapid Transit Dist., Bd. of Dirs., Minutes of the 1,839th Meeting (Apr. 25, 2019), https://www.bart.gov/sites/default/files/docs/minutes/04-25-19%20Minutes.pdf.

[32] S.F. Bay Area Rapid Transit Dist. Board Meeting Agenda (Sept. 10, 2020), https://www.bart.gov/sites/default/files/docs/agendas/09-10-20%20Board%20Packetrev4.pdf.

[33] City of Oakland, Approved Impact Reports and Use Policies, https://www.oaklandca.gov/topics/approved-impact-reports-and-use-policies (last visited Dec. 11, 2020).

[34] City of Oakland, Priv. Advisory Comm., Meeting Minutes (Feb. 6, 2020), https://cao-94612.s3.amazonaws.com/documents/Privacy-Advisory-Commission-Meeting-Minutes-020620.pdf.

[35] City of Oakland, Priv. Advisory Comm., Meeting Minutes (May 2, 2019), https://cao-94612.s3.amazonaws.com/documents/Privacy-Advisory-Commission-Meeting-Minutes-050219.pdf.

[36] Oakland City Council, Special Concurrent Meeting of the Oakland Redevelopment Successor Agency/City Council, Meeting Minutes (Dec. 15, 2020), https://oakland.legistar.com/MeetingDetail.aspx?ID=815803&GUID=ED60E954-69CC-487F-AE1C-894B9BB10F49&Options=&Search=.

Annual Surveillance Reports and Surveillance Technology Surveillance Impact Reports submitted to city council for approval contain extensive detail on technologies used by the city. The second annual report was released on February 28, 2020, and contains 62 pages covering the use of surveillance technology across 23 city departments and over 40 technologies.[37] In the time period covered by the report, the police department reported using 26 different technologies ranging from GPS tracking devices to Shotspotter[38]. For each technology covered, the report contains information on data sharing, complaints, violations of the Surveillance Use Policy, and disproportionate community impact. The technologies in this report are currently under consideration for approval, with the Cambridge City Council Public Safety Committee requesting additional data about several of the technologies after debating their efficacy at an October 2020 meeting.[39] Of note, they have requested:

> *"Shotspotter (broken down by year): number of gunshots reported through ShotSpotter, average response time, resulting arrests, resulting gunshot victims treated, number of gunshots reported by people across the city, number of gunshots reported by people in the ShotSpotter area, gunshots reported by people but not by ShotSpotter in the ShotSpotter area, data retention policies, data on difference in response times between shots reported by Shotspotter and shots reported by humans and data on location pinpoint accuracy; BRIC: Federal agencies that have access to BRIC information, data retention policies; COPLINK: Federal agencies that have access to BRIC information, data retention policies; and any other information that may be deemed helpful and informative to the Council in executing its duties with regard to the Surveillance Ordinance."*

In addition to annual use reporting, municipalities also require the public disclosure of use policies. Several also open either board meetings or city council meetings to open discussion of these policies. As the most recent law as of publication, drafts of the New York police department use policies are posted and open for public comment through February 25, 2021[40] – although no public meetings have been scheduled. At a minimum, these required public disclosures allow local government officials, citizens, and civil society greater insight into the use of surveillance technologies. And where the use of such technology is publicly disclosed, law enforcement has been pushed for greater accountability. However, the full impact of these laws remains to be seen – especially relating to future civil action.

V. Conclusion

Our findings demonstrate accelerating local and state adoption of CCOPS ordinances across the country and a particular focus on facial recognition bans. While adoption has been geographically focused in California and Massachusetts, the trend is truly national in scope, reaching far beyond these two states. There is significant reason for optimism that these ordinances will become a national norm,

---

[37] City of Cambridge, City of Cambridge Departments' second Annual Surveillance Reports (Feb. 28, 2020), https://www.cambridgema.gov/-/media/Files/citymanagersoffice/surveillanceordinancedocuments/secondannualsurveillancereports_combined22820.pdf.

[38] Shotspotter technology is used by law enforcement to detect gunfire through sensors and artificial intelligence. https://www.shotspotter.com/

[39] City of Cambridge, Pub. Safety Committee meeting minutes (Oct. 7, 2020), http://cambridgema.iqm2.com/Citizens/FileOpen.aspx?Type=12&ID=2235&Inline=True.

[40] N.Y.C. Police Dep't, Draft Policies for Public Comment, https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page.

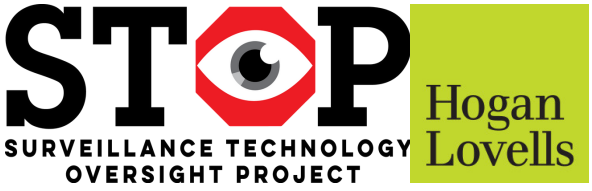
but there is also significant reason for concern that the legislation will not have the entirety of its desired impact.

For facial recognition bans, there is significant risk that the ongoing expansion of private sector facial recognition will dilute the impact of state and local bans. If businesses and members of the public increasingly provide facial recognition evidence to law enforcement at the commencement of an investigation, it could drive police use of facial recognition above pre-ban levels. This pattern has already been documented with large chain retailers, but it could also expand to artificial intelligence-enabled home surveillance products. For those jurisdictions that continue to allow unregulated private-sector use of facial recognition, more must be done to understand and regulate the use of this data by police.

With CCOPS ordinances, there is also reason for concern about the scope of oversight and impact. Many jurisdictions fail to make CCOPS materials readily available to the public, undermining public engagement in the oversight process. Other jurisdictions submit opaque or boiler-plate responses, hiding the details needed for meaningful public engagement. Also, CCOPS often requires sustained investment from civil society to leverage the information provided by localities to advance underlying policy goals.

As CCOPS ordinances require secondary action by the public to have their desired effect (*e.g.,* elimination of invasive tools), they will take additional time to fully evaluate. This preliminary analysis demonstrates that further research will be needed as CCOPS ordinances continue in operation, examining if surveillance transparency leads to increased accountability and reduced surveillance activity.[41]

[41] Nothing in this paper constitutes an opinion of Hogan Lovells or the Surveillance Technology Oversight Project, Inc. ("S.T.O.P."). Hogan Lovells and S.T.O.P do not assume responsibility for the completeness of the information contained in this paper. In addition, Hogan Lovells and S.T.O.P have no responsibility to update this paper for events or circumstances occurring after the date of its publication. This paper has been prepared as a general summary of certain aspects of relevant city and state legislation and should not be treated as a substitute for specific legal advice concerning individual matters, situations or concerns.



Surveillance Technology Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY 10006

www.STOPSpying.org