12-6-2016

Seattle Surveillance Ordinance Memo

Christopher Stevenson

Date: December 6, 2016

To: Shankar Narayan, Technology and Liberty Director, ACLU Washington

Fr: Christopher Stevenson, Member of University of Washington School of Law's Technology and Public Policy Clinic

RE: **Seattle Surveillance Ordinance Memo**

INTRODUCTION

In March 2013, the Seattle City Council ("Council") passed Ordinance 124142 ("Surveillance Ordinance") in order to govern City of Seattle ("City") departments' acquisition and use of surveillance equipment.[1] According to these new rules, departments must submit guidelines for Council approval explaining "how and when surveillance equipment may be used and by whom" prior to any acquisition of new equipment.[2] These "operational protocols" are required to describe the type of equipment to be acquired, where the equipment will be located, and the type of data captured or recorded.[3] They also must address the equipment's potential to endanger privacy rights, as well as propose both a mitigation plan to prevent abuse and a public outreach plan into affected communities.[4] OK

If and when the Council approves the acquisition, before the equipment is deployed the department must draft and submit written protocols about how collected citizen data is to be "retained, stored, indexed and accessed."[5] These "data management protocols" need to set out the period for which data will be retained, who may access the data, the process for authorizing access, storage system infrastructure plans, and methodologies for labeling and indexing data, among other concerns.[6] Unlike the operational protocols, which must be approved by ordinance, the Council has discretion to approve data management protocols without passing a separate ordinance.[7] OK

In the nearly four years since the passage of the Surveillance Ordinance by a 9-0 vote of the Council, no operational protocols for surveillance equipment have been passed via ordinance. Further, the public record indicates that none have even been submitted for Council approval. During that time, in seeming contravention of the Surveillance Ordinance, City departments have acquired technology capable of recording or capturing citizen data on several occasions. For example:

---

[1] Seattle Municipal Code §§ 14.18.10 - 14.18.40, "Acquisition and Use of Surveillance Equipment," (2013)
[2] *Id.*
[3] SMC § 14.18.020
[4] *Id.*
[5] SMC § 14.18.010
[6] SMC § 14.18.030
[7] SMC §§ 14.18.020 - 14.18.030

- In March 2014, the Council voted to authorize funding for the Seattle Police Department (SPD) to implement Booking Photo Comparison Software (BPCS). BPCS is facial recognition technology that will allow SPD to identify criminal suspects by comparing mug shots with photos captured by surveillance cameras. Though the SPD published policy guidelines in the Police Manual defining the limitations of how BPCS may be used and how data collected will be managed, these protocols did not go through the Council approval process.[8]
- In October 2014, the Seattle Police Department (SPD) purchased social media monitoring software from the company Geofeedia without input of the Council. The software is capable of tracking, monitoring, and aggregating the social media activities (Twitter, Facebook, Instagram, etc.) of large groups of people based on where their posts are initiated and what is said.[9]
- In late 2014, Seattle Department of Transportation (SDOT) installed antennas at more than 1,000 intersections throughout Seattle, establishing a Wi-Fi network to track and aggregate data from car sensors (as well as other wireless devices, like phones or tablets) as they pass through intersections, in order to improve SDOT's general understanding of the City's traffic grid and avoid congestion.[10]
- In June 2016, Mayor Ed Murray announced plans to run a pilot program in South Seattle and the Central District for ShotSpotter, a gunshot detection system that utilizes video cameras and microphones to pinpoint the location of gun violence and improve police response time.[11] Good examples of the problem

The stated purpose of the Surveillance Ordinance is to balance the promotion of public safety with the "need to protect privacy and anonymity, free speech and association, and equal protection."[12] Though phrased as a balancing between two opposites, public safety and privacy rights do not need to be mutually exclusive. In fact, a careful consideration in a public forum of how municipal technology acquisitions may implicate privacy and data security concerns can itself be seen as public safety benefit.

---

[8] Keith Wagstaff, *Smile, Seattle! Police Now Can Use Facial Recognition Software*, NBCNEWS.COM, March 12, 2014 (http://www.nbcnews.com/tech/security/smile-seattle-police-now-can-use-facial-recognition-software-n51311); and Josh Sanburn, *Seattle Police to Use Facial Recognition Software*, TIME.COM, March 14, 2014 (http://time.com/25605/seattle-police-to-use-facial-recognition-software/). See also Ordinance 124438 (http://clerk.seattle.gov/~legislativeItems/Ordinances/Ord_124438.pdf) and the SPD's BPCS policy manual (http://clerk.seattle.gov/public/meetingrecords/2014/pscrt20140205_8a.pdf).

[9] Ansel Herz, *How the Seattle Police Secretly - and Illegally - Purchased a Tool for Tracking Your Social Media Posts*, THESTRANGER.COM, Sept. 28, 2016 (http://www.thestranger.com/news/2016/09/28/24585899/how-the-seattle-police-secretlyand-illegallypurchased-a-tool-for-tracking-your-social-media-posts)

[10] David Kroman, *Seattle installs new system to track individual drivers*, CROSSCUT.COM, Sept. 8, 2015 (http://crosscut.com/2015/09/seattles-new-technology-tracks-how-we-drive/)

[11] Elisa Hahn, *Mayor announces gunshot detection pilot program*, KING5.COM, June 2, 2016 (http://www.king5.com/news/local/mayor-murray-and-spd-to-unveil-gunshot-detection-technology/228439762)

[12] Seattle City Council Ordinance 124142 at 1 (2013) (http://clerk.seattle.gov/~legislativeItems/Ordinances/Ord_124142.pdf)

As currently constituted, the ordinance is ineffective in achieving its stated goals because (I) the definition of "surveillance equipment" is imprecise and may be read to exempt relevant acquisitions of surveillance technology by law enforcement; (II) the "exigent circumstances" exception is overly broad; (III) Council review should not be the sole oversight mechanism for all City equipment acquisitions; and (IV) the lack of an enforcement mechanism provides little incentive for compliance. Good description of the problem

DISCUSSION

I. The Definition of "Surveillance Equipment" Should Be Revised to Ensure It Encompasses All Data Collection Technology

One explanation for why the Surveillance Ordinance has been ineffective at encouraging City departments to submit their technology acquisitions for approval is that the definition of "surveillance equipment" is imprecise:

> "Surveillance equipment" means equipment capable of capturing or recording data, including images, videos, photographs or audio operated by or at the direction of a City department that may deliberately or inadvertently capture activities of individuals on public or private property, regardless of whether "masking" or other technology might be used to obscure or prevent the equipment from capturing certain views. "Surveillance equipment" includes drones or unmanned aircraft and any attached equipment used to collect data. "Surveillance equipment" does not include a handheld or body-worn device, a camera installed in or on a police vehicle, a camera installed in or on any vehicle or along a public right-of-way intended to record traffic patterns and/or traffic violations, a camera intended to record activity inside or at the entrances to City buildings for security purposes, or a camera installed to monitor and protect the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.[13]

Notably, the Surveillance Ordinance only concerns itself with "equipment" that is "capable of capturing or recording data," and includes as specific examples of that data "images, videos, photographs, or audio." The term "equipment" coupled with the examples of captured data, while not an exclusive list, suggests surveillance hardware and devices with camera and microphone functionality. Because of this focus, the definition can be read to exclude software applications used to collect and analyze individual data. Good point In addition, the use of the words "capture" and "record" in combination with the explicit references to drone technology in the definition give the impression that the "equipment" under consideration is to be manipulated or tracked in real time for a surveillance purpose. Though it mentions inadvertent capture, the definition seems to be oriented toward traditional notions of surveillance technology, such as video or still cameras, which have a primary intended use of directly monitoring an individual's physical activity. The (eliminate “The”??) Because of this focus, City

[13] SMC § 14.18.010

departments may be under the impression that passive collection of citizen data, such as SDOT's antenna system or via SPD's social media monitoring software, are not subject to the requirements of the Surveillance Ordinance. Who makesz this decision?

For example, the aforementioned SDOT antenna network is capable of tracking any wireless capable device according to the device's media access control (MAC) address.[14] However, SDOT representatives maintain that this data will not be traceable by the City back to individuals or their devices because it will be aggregated and made anonymous by the antenna, and thus SDOT will have no access to the raw, identifiable data.[15] Despite SDOT's dismissal of privacy concerns, a strict application of the definition of "surveillance equipment," suggests that the antennas meet all criteria necessary to make their acquisition subject to the requirements of the Surveillance Ordinance. I agree

The purpose of the antenna network is large-scale data collection: to create a historical database of traffic routes taken on individual streets throughout the City, in order to analyze and eventually improve the traffic grid's ability to adapt.[16] The antennas are pinged every time any wireless device - phone, tablet, or Bluetooth - passes through an intersection. Tracking mobile devices' location as they move through the City by SDOT, especially as part of an initiative to create a massive data archive, is a method of "capturing" the "activities" of individuals within the definition of surveillance equipment.[17] Although they are "installed along a public right-of-way" and "record traffic patterns," they are not "cameras" and thus fall outside the defined exception.

Even though the antennas arguably meet the definition of "surveillance equipment," there is no record that SDOT submitted operational protocols to the Council for approval. Further, even Michael Mattmiller, Seattle's Chief Technology Officer, was unaware of SDOT's antenna network until nearly a year after its installation.[18] Presumably because the equipment was acquired and operated without a specific surveillance goal in mind, unlike a drone with a mounted video camera, SDOT believed that its 'scrubbed' data would not implicate privacy concerns. This borderline situation, where a department presumes that their equipment acquisition is separate and exempt from consideration under the Surveillance Ordinance, yet the acquisition involves a device or technology intended to passively collect data on a large scale, might be avoided if the word "equipment" was revised to read "technology," or if the types of data defined was broadened to include "location" or "electronic or personal information. " Again, who makes this determination/should there be a designated person/entity to do so?

Another possible explanation for SDOT's non-compliance is that the antenna network is owned and operated by a private contractor, Acyclica.[19] A revised definition

[14] Kroman *supra* note 10
[15] *Id.*
[16] *Id.*
[17] SMC § 14.18.010
[18] Kroman *supra* note 10
[19] *Id.*

could easily indicate whether data scrubbing techniques such as those employed by Acyclica are equivalent to the "masking" technologies described in the ordinance, and the requirement that the equipment be "operated by or at the direction of a City department" could be clarified to include or except contractor relationships.

Similarly, in regard to their secret acquisition of the Geofeedia social media monitoring software, the SPD stated: "A department legal review has determined that the use of these tools does not conflict with either the City of Seattle's intelligence or surveillance ordinances."[20] The software in question allowed police to monitor social media posts in real time, place the location of where the post was made on a digital map, and filter through other social media posts in the vicinity.[21] Same as the SDOT network, the software is capable of capturing data about an individual's physical location and does not fall within any defined exception. SPD would likely argue that the Geofeedia software is exempt from the Surveillance Ordinance because it is only analyzing publicly available social media posts and is not capturing new data. However, the definition of "surveillance equipment" is triggered when equipment has the capability of capturing or recording data, not by any requirements of the data's original source. Because the Geofeedia software was advertised to be capable of tracking large events - from protests and professional sporting events to natural disasters - regardless how SPD intended to deploy the technology, its large-scale data recording capabilities should have made it subject to the Council approval provisions of the Surveillance Ordinance. Agree

At a minimum, the following issues with the definition of "surveillance equipment" must be addressed:

- As currently defined, "surveillance equipment" has been read by SDOT and SPD to excuse software applications and passive data collection systems from consideration under the ordinance;
- The degree to which departments may avoid scrutiny for technology that is not strictly acquired but is instead owned and operated by a third-party contractor is not sufficiently described in the ordinance; and
- The meaning of several words and phrases could be clarified. This includes:
    - What "certain views" are contemplated that equipment might be prevented from capturing? Does this provision apply only in the context of describing how security cameras may be designed to obscure the images they capture?
    - What does the term "data" mean? Are the currently listed "images, videos, photographs, and audio" an exclusive list?
    - What is the outer limit of "activities" that are prohibited from being captured or recorded? Does it include location data that may be tracked through social media or mobile devices?

[20] Ryan Yamamoto, *Seattle Police accused of using surveillance software to monitor public online*, KOMONEWS.COM, Sept. 30, 2016 (http://komonews.com/news/local/seattle-police-accused-of-using-surveillance-software-to-monitor-public-online)
[21] Herz *supra* note 9

As a model for how Seattle might revise the "surveillance equipment" definition, the Council could look to the recently passed Ordinance NS-300.897 by the Santa Clara Country Board of Supervisors, which regulates municipal acquisition and operation of surveillance technology.[22] In the first place, the definition uses the term "technology" instead of equipment in order to encompass not only electronic devices but also "[systems] using an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory information specifically associated with, or capable of being associated with, any individual or group."[23] Good By including both a "system" and a "technological tool" within the definition of surveillance technology, the ordinance appears to consider and therefore control the possible acquisition of software applications (such as Geofeedia) and data collection systems (like the SDOT antennas). Secondly, this definition broadens the scope of how the regulated technology is to be used, listing prohibited surveillance actions to include technology that may "collect, retain, process, or share" data, unlike our current Surveillance Ordinance's use of "capture" and "record," which are probably not as effective at controlling devices that subsequently analyze data after being captured by City departments.

Additionally, though it is not contained in the definition, the Santa Clara County Ordinance also requires that Board approval must be obtained for applications related to surveillance separate from the technology's acquisition. Namely, County departments must obtain Board approval when they: (1) seek funds to obtain surveillance technology, such as applying for a federal or state grant; (2) use previously acquired technology for a new purpose or in a new location that has not been approved by the Board; or (3) enter in to an agreement with an entity outside of the County to acquire, share or otherwise use surveillance technology or any information collected therefrom.[24] Adopting or incorporating such specifications about third-party contractors or funding sources would be helpful to clarify the coverage and application of Seattle's Surveillance Ordinance. Agree

II. The "Exigent Circumstances" Exception Is Overly Broad and Inapplicable to Acquisitions of Surveillance Equipment

In some cases, even if a given type of equipment would normally fall within the definition of "surveillance equipment," technology acquisitions of the SPD are exempt from Council approval requirements.[25] More specifically, except in the case of a camera mounted on a drone, equipment acquisitions are exempt from the Surveillance Ordinance if (1) the equipment will be "used on a temporary basis" (2) for a valid law enforcement purpose in "a criminal investigation supported by reasonable suspicion"; "pursuant to a

[22] Santa Clara County, CA - Code of Ordinances §§ A40-1 - A40-12, "Surveillance-Technology and Community-Safety" (2016) (http://15ycf92lfvue3pm0as2w6tec-wpengine.netdna-ssl.com/wp-content/uploads/2016/06/Surveillance-Technology-Ordinance.pdf)
[23] Santa Clara County Code of Ordinances § A40-7(C)
[24] Santa Clara County Code of Ordinances § A40-2(B)
[25] SMC § 14.18.040

lawfully issued search warrant"; or under "exigent circumstances."[26] Under Washington case law, certain warrantless searches are allowable if the court can establish that the search took place under "exigent circumstances" requiring immediate action.[27] The court uses a six-factor balancing test to determine "whether exigent circumstances justify a warrantless entry and search: (1) the gravity or violent nature of the offense with which the suspect is to be charged; (2) whether the suspect is reasonably believed to be armed; (3) whether there is reasonably trustworthy information that the suspect is guilty; (4) there is strong reason to believe that the suspect is on the premises; (5) a likelihood that the suspect will escape if not swiftly apprehended; and (6) the entry is made peaceably."[28] The totality of the situation present in a given case is examined in order to establish exigent circumstances, and failure to meet one of the listed six elements is not, by itself, determinative.[29]

The applicability of the "exigent circumstances" exemption to new technology acquisitions is difficult to square with the rest of the Surveillance Ordinance. The promulgation of operational protocols requires departments to carefully consider the intended purpose and expected uses of equipment that is capable of undermining the privacy rights of Seattle residents prior to its acquisition. Similarly, the creation of data management protocols ensures that departments put in place detailed methodologies for protecting potentially sensitive data after it is captured or recorded. The "exigent circumstances" exemption as applied in other law enforcement contexts, on the other hand, has been found necessary as a narrow departure from constitutionally mandated search and seizure doctrine only when immediate police action is required. While it is imaginable that the use of existing surveillance equipment is necessary under "exigent circumstances" to assist in a pressing police matter, it is harder to create scenarios where the acquisition of new surveillance equipment is necessary to facilitate immediate police action. Even if a scenario arises where the acquisition of such equipment is necessary to immediately resolve an exigent circumstance, the Surveillance Ordinance offers no coherent explanation why operational protocols for the equipment cannot be submitted to the Council retroactively. Furthermore, because the "exigent circumstances" exemption is not defined within the Surveillance Ordinance but instead incorporates the exemption's common law definition, it is subject to unforeseeable adjustment by the courts.

For comparison, the Santa Clara County ordinance also contains an exigent circumstances exception for urgent law enforcement uses but it is limited by several caveats. In particular, after the acquisition of surveillance technology in exigent circumstances, the Santa Clara County Sheriff's or District Attorney's Office must (1) report the acquisition within 90 days; (2) submit the required proposal for a Surveillance Use Policy to the Board of Supervisors within that same 90-day period; and (3) going forward, include the acquired technology in the department's mandatory Annual Surveillance Report.[30] Santa Clara County's approach offers an appealing model for

[26] *Id.*
[27] *State v. Cardenas*, 146 Wash.2d 400, 405 (2002)
[28] *Id.* at 406
[29] *State v. Smith*, 165 Wash.2d 511, 518 (2009)
[30] Santa Clara County Code of Ordinances § A40-9

revision of the Seattle Surveillance Ordinance by retaining the emergency law enforcement exemption, when necessary, but still requiring adherence to the ordinance's goals of transparency and oversight. Good

III. The Surveillance Ordinance May Be Strengthened By Coordinating Council Approval of Equipment Protocols With Existing City Initiatives, Departmental Oversight, and Ordinances

Aside from what was codified into the SMC as Chapter 14.18, the Surveillance Ordinance also required that all departments operating surveillance equipment at the time of its passage (March 18, 2013) should submit applicable operational and data management protocols within 30 days of the effective date of the ordinance.[31] Further, the City Council was meant to review the ordinance's implementation "as it applies to city department use of surveillance equipment" after one year.[32] As stated above, no operational protocols have yet been submitted for Council approval since the Surveillance Ordinance's passage, and if any Council review of the ordinance's implementation occurred, the Council did not inform the public nor have they publicized the review's conclusions. This seeming total lack of compliance indicates that the implicit assumption of the Surveillance Ordinance that departments will self-report their existing surveillance equipment and notify the Council of new acquisitions is badly misguided.

Though the requirements of the Surveillance Ordinance have not been effective in facilitating City departments' transparency about the technologies they deploy, there are other, existing City policies that might facilitate review of new and ongoing departmental projects involving surveillance equipment. The coordination of these programs with the Surveillance Ordinance's requirement of Council approval for surveillance equipment might assist, going forward, in encouraging City departments to comply. In particular, the Surveillance Ordinance might be more effective if it was revised to coordinate with (A) the privacy review process of the City's Privacy Initiative; (B) the Racial Equity Toolkit review of the City's Race and Social Justice Initiative; and (C) the functional duties of the City's Chief Technology Officer in overseeing any department's acquisition of information technology. Good possible solutions

A. Privacy Initiative's "Privacy Review Process"

The City announced via Resolution 31570 in February 2015 their adoption of the City of Seattle Privacy Principles, "related to the City's collection, protection, use, retention, sharing, and disposal of personal information, and committing the City to standards of accountability and transparency."[33] The six Privacy Principles address the value of personal privacy, the scope of the City's collection of personal information, intended uses of personal information after collection, City accountability for protecting

[31] Ordinance 124142 *supra* note 11, at 6
[32] *Id.* at 6
[33] Seattle City Council Resolution 31570 (2015) at 2 (http://clerk.seattle.gov/~legislativeItems /Resolutions/Resn_31570.pdf)

the collected personal information, how personal information might by disclosed by the City, and the City's goal of maintaining an accurate database of personal information.[34]

Later in 2015, the City announced its plans to move forward with a citywide Privacy Initiative based in the guidelines outlined in the earlier-adopted Privacy Principles.[35] As part of the Privacy Initiative, the City proposed a final Privacy Policy that set forth requirements for City departments to observe "when information systems or other forms and applications collect the public's personal information" in the course of City business.[36] The Policy requires that departments not only adhere to the Privacy Principles but also that all projects with "potential privacy impacts" are submitted to the Privacy Program Manager for review so that requirements and recommendations to mitigate these impacts can be put into place.[37] City departments are instructed to use a Privacy Toolkit, which is a collection of review questionnaires and materials, "for direction regarding City privacy policies, standards and the privacy review process."[38]

At a minimum, once it is entirely implemented, the privacy review process will require completion of a Self-Service Assessment by the department to determine the level of privacy risk associated with a City project where personal information will be collected.[39] Next, if the project is found to have a "higher privacy risk," the department will be required to answer additional questions in a Privacy Threshold Analysis, in order to assist the evaluation of potential privacy impacts.[40] If impacts are identified that present a "significant risk," then the department must also complete a Privacy Impact Assessment to facilitate the Privacy Program Manager's further review of the impactful information systems.[41] The Privacy Impact Assessment is automatically triggered if the information being collected is under regulatory control, the technology involved in the collection program involves drones or surveillance cameras, or there is a possibility that the public will perceive the data collection practice negatively.[42] Within the Privacy Impact Assessment, departments must provide a comprehensive overview of their proposed project, including whether the public is notified that their information is collected, how and where the information will be collected, used, retained, or shared, as well as strategies for ongoing monitoring and enforcement of the project.[43]

---

[34] City of Seattle Privacy Principles (https://www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf)
[35] Taylor Soper, *City of Seattle unveils new privacy program to 'build public trust' about use of personal information*, GEEKWIRE.COM, Oct. 12, 2015 (http://www.geekwire.com/2015/city-of-seattle-unveils-new-privacy-program-to-build-public-trust-about-use-of-personal-information/).
[36] City of Seattle Privacy Policy at 1, July 21, 2015 (http://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyPolicyFINAL.pdf)
[37] *Id.* at 1
[38] *Id.* at 1
[39] City of Seattle Privacy Program at 8, October 2015 (http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf)
[40] *Id.* at 8
[41] *Id.* at 8
[42] *Id.* at 23-24
[43] *Id.* at 28-33

There is significant overlap between the project planning requirements placed on City departments in satisfying a privacy review for the purposes of the Privacy Initiative and the submission of operational protocols under the Surveillance Ordinance. It may be feasible to enable the Privacy Program Manager to add surveillance equipment acquisitions as a provision to be completed by departments within the Privacy Threshold Analysis or Privacy Impact Assessment steps of the review process. If so enacted, the Privacy Program Manager should be able to alert the Council of expected equipment acquisitions, as well as facilitate tools to assist the department's drafting of operational protocols for the equipment. Good possible solution

It may also be possible to create entirely separate resources as part of the Privacy Toolkit for departments to utilize in order to comply with the Surveillance Ordinance. These resources could be designed to track the specific requirements of the Surveillance Ordinance, as well as to help departments draft their mandated operational and data management protocols in the ordinance format such that they can be streamlined through the Council review process.

B. Race and Social Justice Initiative's Racial Equity Toolkit

Launched in 2004, the Race and Social Justice Initiative (RSJI) is a citywide policy devoted to eliminating racial disparities and institutional racism throughout Seattle. The Council affirmed the goals and priorities of RSJI by passing Resolution 31164 in November 2009, in which the Council asserted, "City departments should use available tools to work to eliminate racial and social disparities across key indicators of success" including criminal justice, among other factors, "and to promote racial and social equity in the delivery of City services."[44] In furthering this goal, the Council encouraged departments to implement "racial equity tools in budget, program and policy decisions, including review of existing programs and policies."[45]

Additionally, the current mayor, Edward Murray, issued an Executive Order in April 2014 soon after he assumed office in which he also affirmed his administration's commitment to the RSJI, and directed City departments to "expand their use of the Racial Equity Toolkit as part of all program and policy planning processes."[46] The Executive Order also provides that the Mayor will work with the Seattle Office of Civil Rights (SOCR) to implement a Race and Social Justice Assessment Program through which departmental practices and policies may be reviewed for compliance with RSJI goals at the request of the Mayor or by "community request."[47]

The Racial Equity Toolkit is an RSJI resource that assists City departments in assessing their proposed policies, initiatives, and programs for how they impact racial

[44] Seattle City Council Resolution 31164 (2009) at 3 (http://clerk.seattle.gov/~legislativeItems /Resolutions/Resn_31164.pdf)
[45] *Id.* at 4
[46] City of Seattle Executive Order 2014-02 at 2, "Race and Social Justice Initiative" (2014) (http://murray.seattle.gov/wp-content/uploads/2014/04/RSJI-Executive-Order.pdf)
[47] *Id.* at 2

equity.[48] Before policy implementation occurs, the Racial Equity Toolkit requires departments to follow a six step process to identify and define important racially equitable community outcomes related to the program under consideration, involve stakeholders in affected communities, determine the expected racial equity benefit or burden of the program, and develop strategies to minimize unintended consequences and improve accountability.[49] The Toolkit's preemptive review process of department programs may be able to serve as an additional oversight mechanism to improve the effectiveness of the Surveillance Ordinance.

For example, subjecting SPD's BPCS facial recognition proposal to the standards of the Racial Equity Toolkit offers a different angle through which to consider its public impact. At Step 1 of the Racial Equity Toolkit, departments must preliminarily identify which "racial equity opportunity area(s)" will be primarily impacted by their proposed policy.[50] Listed areas are education, community development, health, environment, criminal justice, jobs, and housing. Statistical studies indicate that racial minorities are much more likely to be impacted by unwarranted police monitoring, as well as to be misidentified by facial recognition software.[51] Therefore, BPCS would fall within the Criminal Justice area. If the Surveillance Ordinance were in some way coordinated with the Racial Equity Toolkit, the BPCS' operational protocols could include mitigation strategies for avoiding potential racial inequities. Interesting approach

Similarly, SPD's ShotSpotter pilot program is also implicated. At Step 2 of the Racial Equity Toolkit, departments need to identify "existing racial inequities that influence people's lives and should be taken into consideration" after researching relevant demographic data about and performing outreach into the affected community.[52] Further, Step 3 requires consideration of the benefit or burden of a given departmental program on increasing or decreasing racial equity.[53] The South Seattle and Central District areas targeted by the ShotSpotter program are those in which a majority of the populations are persons of color.[54] In other cities where gunshot detection systems have been implemented, there have been mixed results about the systems' ability to improve police apprehension of criminals. For example, from 2010 to 2013 in Newark, NJ, gunshot detection sensors were set off 3,632 times, more than 75% of which were false alarms, and led to the arrest of only 17 shooters at the scene.[55] In 2016, the police department in

[48] RSJI Racial Equity Toolkit at 1 (http://www.seattle.gov/Documents/Departments/RSJI/RSJI-Racial_Equity_Toolkit-2016.pdf)
[49] *Id.* at 1
[50] *Id.* at 2
[51] Sandra Fulton, *Surveillance Isn't Colorblind*, FREEPRESS.NET, Aug. 10, 2016 (http://www.freepress.net/blog/2016/08/10/surveillance-is-not-colorblind)
[52] RSJI Racial Equity Toolkit at 3
[53] *Id.* at 3
[54] Percentage of the Population Who Are Persons of Color by Census Tract Map, City of Seattle Department of Planning and Development (http://www.seattle.gov/dpd/cs/groups/pan/@pan/documents/web_informational/dpdd016871.pdf)
[55] Sarah Gonzalez, *In Newark, Gunshot Detection System Falls Short of Booker's Claims*, WNYC.ORG, Aug. 9, 2013 (http://www.wnyc.org/story/311533-gunshot-detection-sensors-newark-result-17-arrests-over-three-years/)

Charlotte, NC decided to discontinue their contract with ShotSpotter because the system did not help them make arrests or identify crime victims.[56] The prospect of increased police presence and surveillance in these neighborhoods with majority populations of persons of color, coupled with a system that could be potentially ineffective at achieving its stated goal, should be a concern for the SPD.

Because the ShotSpotter program, like many SPD initiatives, may implicate criminal justice issues germane to RSJI review, the Surveillance Ordinance could be coordinated with the Racial Equity Toolkit in order to identify surveillance programs with racially inequitable impacts.

C. Chief Technology Officer Oversight of Information Technology Acquisitions

In November 2015, the Council passed Ordinance 124920 creating a new Seattle Information Technology Department (SITD) and appointing the incumbent Chief Technology Officer (CTO), Michael Mattmiller, to serve as its director.[57] The SITD was created to manage the City's information technology resources, many of which seem to overlap with technologies that match the definition of "surveillance equipment." Specifically, SITD will be responsible for managing "applications and applications infrastructure" and "computer engineering and operations," systems that will be utilized for data collection and management like "data centers, servers, storage, and backup equipment," as well as resources through which citizens may voluntarily submit data including "citizen engagement portals" and "internal websites."[58]

The CTO position is empowered to administer key information technology functions that read as duplicative of the Surveillance Ordinance's requirement for City departments to promulgate operational and data management protocols for surveillance equipment. Namely, the CTO is granted the authority to "develop, promulgate, and implement City policies and standards governing the acquisition, management, and disposition of information technology resources" and to "develop policies and standards for the management, maintenance and operation of City information technology resources".[59] The CTO is also empowered to "determine the most effective ways of providing information technology resources to City departments, including services and the management thereof, using City or contracted sources," as well as to "execute, administer, modify, and enforce such agreements and instruments as the Chief Technology Officer shall deem both reasonably necessary to implement programs consistent with all applicable laws and ordinances and appropriate for carrying out the responsibilities, functions, and activities of the Department."[60] In concert with the CTO's

---

[56] Cleve R. Wootson, Jr., *Charlotte ends contract with ShotSpotter gunshot detection system*, CHARLOTTEOBSERVER.COM, Feb. 10, 2016 (http://www.charlotteobserver.com/news/local/crime/article59685506.html)
[57] City of Seattle Ordinance 124920 (2015) at 2 (http://clerk.seattle.gov/~legislativeItems/Ordinances/Ord_124920.pdf)
[58] SMC § 3.23.010
[59] SMC § 3.23.030
[60] *Id.*

budgetary responsibilities, these powers could conceivably be aimed at reviewing City departments' compliance with the Surveillance Ordinance.

Perhaps most significantly, the CTO is also empowered to oversee all acquisitions of information technology resources by any City department. The ordinance sets out that "no City officer or employee shall acquire, through purchase, lease, or any form of contract, any information technology resources for the City except through, or in accordance with, policies, guidelines, standards, and procedures established by the Chief Technology Officer."[61] Though this provision does not incorporate the Surveillance Ordinance, it is very possible that some information technology acquisitions subject to CTO oversight might also be classifiable as surveillance equipment. The CTO could establish standards for referring such overlaps between SITD and the Surveillance Ordinance to the Council.

Each of the Privacy Initiative, RSJI, and CTO Ordinance has potential as an oversight mechanism that might serve to encourage City department compliance with the Surveillance Ordinance. Further, while the RSJI's Racial Equity Toolkit is well established and commonly used by City departments, the privacy review process and the CTO's oversight process for information technology acquisitions are very new and their implementation appears to be ongoing. As such, there is an opportunity for supporting materials related to the Surveillance Ordinance to be incorporated into both processes in order to ensure that departmental projects necessitating acquisition of surveillance equipment are referred to the Council for additional approval. Possible but overlapping solutions

IV. The Addition of an Enforcement Mechanism Is Necessary to Improve Departmental Compliance With the Surveillance Ordinance

Though the Privacy Threshold Analysis, Racial Equity Toolkit, and CTO information technology acquisition review all might play a part in providing oversight of department non-compliance with the Surveillance Ordinance, ultimately one major issue with the current system is the lack of an effective enforcement mechanism. Coupled with the fact that producing operational protocols and submitting to the Council review process may be time-consuming and generate negative publicity, departments are not incentivized to comply with the ordinance because there is no risk to non-compliance.

As an example of an alternate approach, the Santa Clara County ordinance contains three provisions to ensure that departments comply with the rules, both in initially acquiring technology and in their continuing use. First, as part of the requirement that all Santa Clara departments must obtain approval for and publicly release a "Surveillance Use Policy" for all surveillance technology they acquire and deploy, the policy must include an oversight provision.[62] More specifically, prior to any acquisition of technology, the acquiring department must explicate the mechanisms by which they

[61] SMC § 3.23.040
[62] Santa Clara County Code of Ordinances § A40-7(E)(10)

will ensure their proposed policy will be followed.[63] Examples given include the identification of personnel assigned to ensure compliance, appointment of an independent person or entity with oversight authority, or sanctions for any violation, among others.[64] The Seattle Surveillance Ordinance, on the other hand, contains only one similar provision ensuring compliance with operational protocols that is much narrower. In fact, it only requires the identification of a "lead department" responsible for "maintaining the equipment and ensuring compliance with related protocols," (as well as personnel within that department given delegated responsibility) when multiple departments coordinate to share surveillance equipment.[65]

Second, the Santa Clara County ordinance also insulates whistleblowers within county departments that make good-faith complaints about a failure to comply with the surveillance regulation.[66] Good idea Specifically, the ordinance provides that any retaliation against a County employee that complains in good faith about a non-compliant acquisition or use of surveillance technology will be grounds for disciplinary action.[67] In contrast, the Seattle Surveillance Ordinance does not instruct or even contemplate how a complaint about non-compliance would be submitted, or who would be eligible to submit one, let along offer protection for City departmental employees.

Third and finally, the Santa Clara County ordinance also includes an explicit enforcement provision that allows a private person or entity that successfully demonstrates violation of the ordinance to obtain injunctive relief and attorney's fees.[68] The ordinance requires the complainant to first provide written notice of the violation, and then if after 90 days, during which the Board may investigate the alleged violation, the department has not remedied the violation, the complainant may seek injunctive relief in court.[69] The complainant may also collect "reasonable attorney's fees" up to $7,500 if they show that the violation was a result of "arbitrary or capricious action" by the County.[70]

Any of the above-listed enforcement provisions would be an improvement to the Surveillance Ordinance as currently constituted. The most simple to impose would be the addition of department oversight procedures to the existing operational protocols requirement, however because of the current lack of compliance with that requirement it also might not be very effective. Adding a whistleblower provision would encourage City personnel to come forward about intentional violations and knowing avoidance of the Surveillance Ordinance, if such a thing exists, but it is also possible that citywide non-compliance is simply due to an overall lack of awareness of the new requirements. The insertion of a right of action against the City would undoubtedly be the most

---

[63] *Id.*
[64] *Id.*
[65] SMC § 14.18.020(J)
[66] Santa Clara County Code of Ordinances § A40-11
[67] *Id.*
[68] Santa Clara County Code of Ordinances § A40-10
[69] *Id.*
[70] Santa Clara County Code of Ordinances § A40-10

controversial addition, though the threat of monetary penalty might also be sufficient motivation to encourage departmental compliance.

Another model for reform may be found in the Seattle Intelligence Ordinance, passed in 1979, which was intended to prohibit SPD's unwarranted collection of intelligence files on citizens' private activities.[71] The Intelligence Ordinance concerns "political surveillance," in that it prohibits any person from becoming the subject of police intelligence gathering based solely on his or her lawful exercise of a constitutional right.[72] SPD is thus forbidden from collecting any "restricted information" about private individuals, including political and religious affiliations and activities, membership or participation in political or religious organizations, and participation in political demonstrations.[73] The police can only collect "restricted information" if it is "reasonably relevant" (A) to someone charged with a crime or accused of an ordinance violation, at the request of the State Attorney General or City Attorney, and in the course of (B) an investigation into government corruption or (C) a background investigation into City government job applicants.[74] In order to ensure compliance with the Intelligence Ordinance, the Mayor has the capacity to appoint a civilian Auditor, who may audit SPD files at unscheduled intervals, at least once every 180 days.[75] The Auditor is empowered to report violations and notify any victim about who restricted information has been collected.[76] Once notified, persons who are injured by the unauthorized collection of restricted information have a right of action against the City.[77]

The Intelligence Ordinance's combination of an Auditor position mandated to notify citizens of violations of the ordinance with a right of action is an effective way to safeguard privacy rights, and this dual setup would greatly improve the Surveillance Ordinance's enforcement. It may be argued, however, that he appointment of a civilian Auditor in the Intelligence Ordinance is reasonable partly because the activities being audited fall entirely within one single department, the SPD. Were a similar position proposed to enforce the Surveillance Ordinance, the Auditor's purview would have to be much wider in order to audit all relevant departments, and as a result they might lack capacity to investigate each department with requisite speed and accuracy. Perhaps more importantly, an Auditor for the Surveillance Ordinance might be infeasible because there is currently little publicly available information about what surveillance equipment is being used or acquired by City departments. As a result, the audits would need to be performed blindly and broadly, at least initially.

---

[71] Seattle City Council Ordinance 108333 (1979); *see also* SMC §§ 14.12.010 - 14.12.400, "Collection of Information for Law Enforcement Purposes" (1982)
[72] Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 CORNELL L. REV. 735, 778 (1984)
[73] SMC § 14.12.030
[74] SMC § 14.12.110
[75] SMC § 14.12.330(A)
[76] SMC § 14.12.340(A)
[77] SMC § 14.12.350

CONCLUSION

Since Seattle passed its Surveillance Ordinance in 2013, ten other cities around the U.S. have proposed or begun discussion about laws similar to Seattle's.[78] Also in that time, people in San Jose and Oakland have mobilized to delay their Police Departments' purchase and use of surveillance technology until it could be ensured that citizens' privacy rights would be protected.[79] Government transparency in the age of technologies that facilitate mass surveillance is crucial, and Seattle's Surveillance Ordinance should be strengthened to ensure that citizens' civil liberties are protected in line with the stated goals of the original ordinance.

As a threshold matter, the definition of surveillance equipment should be broadened to expressly encompass other types of technology that may be used to collect individual data, such as software applications. Next, the exigent circumstances exception should be narrowed such that law enforcement acquisitions of surveillance equipment are not exempted from the ordinance. Finally, the ordinance must be revised to include and enforcement mechanism, either by combining the public approval process for surveillance equipment with existing methods of privacy and criminal justice oversight or by drafting a new provision that gives persons a right of action against the City when departments violate the ordinance.

[78] Catherine Crump, *Citizens need more say over police surveillance technology*, SFCHRONICLE.COM, Nov. 21, 2016 (http://www.sfchronicle.com/opinion/openforum/article/Citizens-need-more-say-over-police-surveillance-10628936.php)
[79] *Id.*