Police Intelligence-Gathering and Surveillance:

Better management needed to protect civil rights

April 2022

PORTLAND CITY AUDITOR
Audit Services

Police Intelligence-Gathering and Surveillance:
Better management needed to protect civil rights

Mary Hull Caballero, City Auditor
KC Jones, Audit Services Director

Audit Team:
Elizabeth Pape, Performance Auditor II
Bob MacKay, Performance Auditor II

Summary

A wave of Black Lives Matter protests swept through Portland in the summer and fall of 2020. Police encountered protesters exercising their right to free speech and others vandalizing property and committing arson. The dynamic conditions of the protests presented a challenge for police to enforce laws while safeguarding people's civil rights.

This audit assessed whether Portland police gathered intelligence and conducted criminal investigations in a manner that protected privacy and civil liberties during the protests. Our inquiry consisted of two parts. The first reviewed whether police working the protests and criminal intelligence officers gathered and maintained information about protesters in a way that protected their civil rights. The second part focused on how the police used surveillance technology, both during protests and more generally.

We reviewed a sample of 40 police reports related to protests and 33 Criminal Intelligence Unit reports and bulletins. We found the Portland Police Bureau provided no guidance for officers at protests about what information they could collect and that the Criminal Intelligence Unit did not limit access to its reports and kept them past their retention schedule.

The Bureau had 37 different surveillance technologies but few policies and procedures to guide their use. We found that officers used social media extensively without direction for appropriate use. Our review of video taken from the Bureau's airplane did not record images that could be used to identify people or vehicles, a finding that may help alleviate protesters' fears of the Air Support Unit.

Intelligence gathering and surveillance is by its nature secretive, but the Bureau should adopt policies to guide officers tasked with collecting it. The policies should set boundaries for acceptable activity and help ease the public's fear of the Bureau's use of intelligence-gathering and surveillance, the collection of which is to make Portland a safer and more secure place to live.

Background

Portland has a lively history of activism and public demonstrations. Portlanders have been especially eager to express their First Amendment rights, from labor organizing in the 1930s, to demonstrations against race discrimination in the 1960s, to the Occupy Wall Street movement in the 2010s. In the Spring of 2020, some people across the nation were shocked by the murder of George Floyd at the hands of a Minneapolis Police officer. His murder led many to question long-standing police practices and direct their anger at law enforcement. Portland erupted into Black Lives Matter protests that swept all quadrants of town and lasted for more than 100 days.

Portland Police have had incidents involving its intelligence-gathering and record-keeping become public controversies. The American Civil Liberties Union of Oregon recently sued the City alleging the Bureau violated state law and a prior agreement with the organization during the Black Lives Matter protests that forbids law enforcement from collecting information about protesters who were not engaging in criminal activity. The Bureau's decision in the 1980s to stop keeping physical files of intelligence information about groups and individuals led a sergeant to store boxes of them in his garage when he retired. The files, which eventually were returned to the Portland Archives and Records Center, included information on a food cooperative, a women's rights organization, and an organization that promoted bicycle repair.

Policing the Black Lives Matter protests was complicated and difficult. Officers often worked overtime shifts and were exhausted. Most of the protesters were law abiding and intent on expressing their opposition to police violence against Black people across the nation. But there were also people in the crowd committing crimes, such as spray-painting buildings, smashing windows, setting fires, barricading streets, and throwing objects at police officers. Police collected evidence to support potential prosecutions of suspected illegal activities.

Collecting information that involves Constitutionally protected speech comes with risks. Surveillance and intelligence-gathering without safeguards can:

- Stifle free speech and association;
- Create irrelevant information and harm innocent people;
- Generate of a sense of vulnerability;
- Allow for abuse; and,
- Make communities less safe.

Research shows these effects are particularly acute for people of color because of the historical use of intelligence-gathering to suppress civil rights movements and over-policing of Black communities.

The Police Bureau group responsible for intelligence-gathering is called the Criminal Intelligence Unit. The unit also provides security for dignitaries and investigates threats against Portland officials and those involving workplace violence. The team consists of one sergeant, four officers, and one administrative support staff. It reports directly to the Chief. The unit's budget was $1.4 million in Fiscal Year 2019-2020.

Officers collected information about protesters without documenting reasons

Law enforcement officers should not collect information about the political, religious, or social views or associations or activities of individuals, businesses, or groups without reasonable suspicion of criminal activity, according to Oregon Revised Statute 181A.250. Collecting information about protesters without documenting criminal activity has the potential to stifle free speech.

Dave Killen, Oregonian. May 2021. A detective stored this photo of peaceful protesters in police records.

Portland officers collected personally identifiable information about protesters in police records without documenting suspected criminal activity. We reviewed a random sample of 40 police reports related to protest activity and found five examples of officers collecting information about protesters without the required documentation.

One example involved an officer who recorded a video of protesters with a personal phone. The officer told his supervisors that he made the recording for his own use and not because the protesters were engaged in criminal activity. The protesters became angry when they noticed the officer recording them. This prompted the officer to notify his supervisor, who asked him to document the incident in a report.

We observed four other examples in our sample of officers recording personal information about protesters without documenting suspected criminal activity, including:

- A photo of protesters;
- A video of people presumed to be protest organizers;
- A report by an officer who recorded license plates of vehicles near a protest; and,
- Photos and videos from a protest saved from publicly available social media posts.

The presence of the information is why officers need clear direction from the Bureau to ensure they comply with the law. The First Amendment protects people's right to protest, and street protests can be complex events for the police to manage. The Bureau had no directives or instructions for officers specific to investigating criminal activity during First Amendment events. Without guidance, officers used their individual discretion to decide how and what type of information to collect during the 2020 protests.

Other cities, such as San Francisco and the District of Columbia, have policies that direct how officers should conduct investigations when policing activity associated with First Amendment events. Their policies include how investigations are authorized, who can gather evidence, and whether invasive investigative techniques can be used. They also include guidelines for information validation, access, and retention.

Bureau held protected information without safeguards

Unlike officers policing protests in real-time, the Criminal Intelligence Unit has standard operating procedures intended to ensure the Bureau complies with state law when gathering information related to political and religious activity. According to its procedures:

- When a report comes to the Criminal Intelligence Unit, it should be placed in a working file for review;
- If it is determined there is no reason to suspect criminal activity, the information should not be retained longer than 30 days; and,
- Access to the reports should also be limited to staff in the intelligence unit and those with the appropriate permission to view them.

We reviewed a sample of 33 Criminal Intelligence Unit work products to determine if the unit protected political or religious information that was not associated with criminal activity. We found six work products related to political activity that had no substantiated criminal activity. Those should not have been retained beyond the 30-day limit. They also were widely available throughout the Bureau despite the access limitation that applies to sensitive information.

For example, one report described a person suspected of surveilling a Police Bureau building during the Black Lives Matter protests. The report included the person's vehicle license plate number. A few days later, an officer assigned to the Criminal Intelligence Unit determined the person's conduct was not criminally suspicious and closed the case.

We observed five other examples that did not appear to comply with procedures:

- A report and bulletin about a person planning to protest actions by the Oregon Attorney General;
- A bulletin from Vancouver Police describing a vehicle playing anti-law enforcement music;
- A report about a perceived social media threat to the Multnomah County District Attorney;
- A report about assistance provided to a New Jersey law enforcement agency regarding political activity from a Portland internet address; and,
- A report about a person who expressed concern to a third-party about antisemitic activity within the Portland Police Bureau.

The continued existence of the reports raises risks for the people described in them. Any officer from any agency that searches the Bureau's records system using the names will have access to the case information. Such searches commonly are conducted during routine traffic stops. Studies have shown that police officers are more likely to view people as dangerous when they also view them as disrespectful. Officers might perceive drivers to be a threat during traffic stops if they access reports that say drivers were involved in Black Lives Matter protests or played music perceived to be anti-police. Officers also are poorly served when unfounded information remains in the system while making decisions in the field.

The records exceeded the retention limit and were widely available because the Criminal Intelligence Unit does not have a process for protecting political or religious information that was not related to criminal activity. Officers saved reports in the Bureau's central records management system, known as RegJIN, which state law requires be retained for at least 20 years. The system is accessible by all sworn Bureau members as well as officers from partner agencies, such as Lake Oswego and Scappoose.

Bureau's surveillance technology vulnerable to misuse

There's tension between the promise that technology offers to make people safer and more secure and the threat of invasive surveillance. Technology can be both beneficial and harmful at the same time. We found the Bureau had tools capable of gathering information about people but did not have accompanying data governance policies to comply with the City's privacy principles.

> The use of technology can improve policing practices and build community trust and legitimacy, but its implementation must be built on a defined policy framework with its purposes and goals clearly delineated. Implementing new technologies can give police departments an opportunity to fully engage and educate communities in a dialogue about their expectations for transparency, accountability, and privacy.
>
> *- President's Taskforce on 21st Century Policing*

The Bureau provided a list of 37 types of technology capable of collecting sensitive information. Some, such as the online reporting portal, are not what jump to mind when thinking about intelligence-gathering and surveillance. Policy-setting criteria suggests, however, that technology intended for a purpose other than surveillance but that can be used for that activity should be regulated.

People interviewed for this audit said they feared the Bureau was using technology for inappropriate surveillance. Their concerns ranged from license plate readers, aircraft, cell phone data extraction, predictive policing tools, and facial recognition software. There was a particular fear that data might be shared with U.S. Immigration and Customs Enforcement. Community members offered ideas that would make them more comfortable with the Bureau's technology, such as ensuring that data is secure, evaluating the dollar and societal costs of surveillance technology against its public safety benefits, and creating rules about sharing data with third parties, including other law enforcement agencies.

The Fourth Amendment places restrictions on how law enforcement collects information without probable cause that a person committed a crime. The City's Privacy and Information Protection Principles include high-level values statements to provide further protections for Portlanders, but do not include specific practices. The principles relate to transparency, accountability, and equitable and ethical data management.

Of the Bureau's 37 types of technology that could be used for intelligence-gathering or surveillance, 16 had associated policies, including license plate readers, body wires, and cell phone data extraction software. With one exception, the policies addressed basic concepts, such as authorized uses and required training. Some, however, were missing other important components, such as guidance for data collection and safeguarding.

Policies were absent for 21 types of technology that can be used for surveillance. Many of them were used for tactical awareness by the Special Emergency Response Team, Crisis Negotiation Team, and Bomb Team.

The Bureau documented its use of three of 37 types of technology: license plate readers, traffic cameras, and the online reporting portal. Usage reports assessed the effectiveness of the technology but were missing other elements. For example, reports about license plate readers and the online reporting system did not address community members' complaints about the technology and were not readily available to the public. None of the reports addressed cost or whether any improvements or modifications were needed. Only the traffic camera report was available online.

Neither Council nor Bureau managers provided overall direction for adopting and using surveillance technology. The City Council of Oakland, Calif., adopted an ordinance that outlines rules for adopting technology, using and maintaining data, and sharing information. Oakland's Council must authorize surveillance technology purchases and use and seeks advice from a privacy commission. Oakland's ordinance requires staff to draft use policies for each type of surveillance technology, including who has access and how data is collected, protected, and shared. Staff also must submit a report to the privacy commission that includes information about how all surveillance technology is used, its effectiveness, and recommendations for changes in use. The President's taskforce on 21st Century Policing also recommended involving community advisory committees in the adoption of new technology.

Officers used social media without direction

Social media is becoming an essential law enforcement tool. The Urban Institute and the International Association of Chiefs of Police found in a 2016 survey that 91 percent of law enforcement agencies used social media to notify the public about safety concerns, 89 percent for community outreach, 70 percent for intelligence gathering, and 59 percent had contacted a social media company to obtain evidence.

Law enforcement can use social media for several investigative purposes, such as:

- Overt investigations that use publicly available information, such as Twitter;
- Discrete investigations similar to wearing plain clothes or patrolling in an unmarked car. An example is using a private internet service provider to read a blog; and,
- Covert investigations similar to undercover activities, such as using a fictitious account or getting a court order to intercept data.

Oregon Revised Statute 181A.250 prohibits law enforcement officers from collecting information about the political, religious, or social views or associations or activities of individuals, businesses, or groups without reasonable suspicion of criminal activity. Reasonable suspicion is a lower bar than probable cause. Social media presents the opportunity to collect information on multiple people networks of personal associations are inherent to the format. The American Civil Liberties Union noted that monitoring social media can silence discourse by making people afraid they will be punished for expressing views and targeted for threatening existing power structures.

Social media can also be used to track innocent speech that may be hyperbolic or misunderstood by police. For example, an Oregon Department of Justice investigator investigated the Black director of its civil rights division after the director posted to the BlackLivesMatter hashtag on Twitter. The investigator also mistook a hip-hop group's logo in the director's personal newsfeed for an anti-police slogan. The director sued, saying the surveillance operation violated his civil rights. The case was settled, but the legal agreement also required the director to leave his job.

Social media is used extensively across the Police Bureau. Officers, Detectives, and Supervisors said they used social media for investigations by reviewing publicly available information and creating fictitious accounts with assumed identities to view private accounts. Officers also could get a warrant for more comprehensive access to social media accounts.

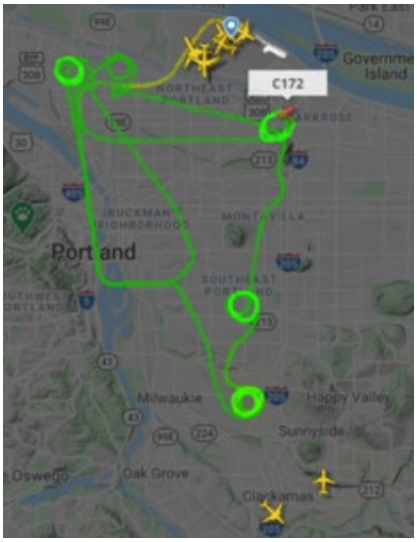
The Bureau's social media directive did not include instructions about how to use social media during investigations. Instead, it was focused on officers' personal use. The Justice Department's Bureau of Justice Assistance recommends key investigative elements that should be included in social media policies, such as authorization requirements for different types of social media use and how evidence will be validated and stored.

We reviewed a sample of 25 instances in which Criminal Intelligence Unit officers used social media. Seven instances were appropriately documented. Sixteen instances did not have documentation of suspicion of criminal activity. Examples included:

- three instances in which subjects were not associated with any active criminal cases;
- four instances in which inquiries came from other agencies but were not documented as such; and,
- nine instances in which work products did not include documentation of suspected criminal activity.

Transparency may assuage public's fear of airplane surveillance

The Bureau's use of aircraft evoked fear in more community members and protesters interviewed and surveyed for this audit than other intelligence-gathering or surveillance tools. People were concerned the Bureau used its airplanes to collect information on individual protesters.



Source: www.flightradar24.com. This screen shot shows the flight path of the Bureaus airplane on 4/8/21 at 9:20 PM.

In contrast to the level of concern, we found no evidence in a sample of recordings created by the Air Support Unit during the 2020 protests of information of individuals' political activity. One of 20 recordings we reviewed was related to a protest, and it included evidence of criminal activity. The technology did not appear capable of capturing images in enough detail to identify individuals or vehicles. We rode in the plane to observe what pilots could see from the air and could not identify individual people or vehicles. We also did not find any evidence that indicated that Portland officers used Stingray technology, which community members suspected Air Support used to remotely access information from cell phones.

The Bureau's Air Support Unit flies a fixed-wing plane about 1,200 hours a year. It is staffed by one full-time sergeant, who oversees others assigned to help when needed. Its budget was $500,000 in Fiscal Year 2020-21.

Source: Audit Services. The Air Support Unit's airplane.

Air Support has policies that forbid recording political activities unless there is evidence of a crime. The policy directs crewmembers to avoid recording protest events unless an incident commander asks them to, or the crew observes criminal activity. The unit does not report publicly about its activities but was developing an online dashboard to share information internally. The Bureau missed an opportunity to alleviate the community's fears about the intrusiveness and use of the plane by not sharing the information publicly.

To view Air Support Unit videos online, visit our report: www.portland.gov/police-intelligence-gathering

- Protests video: https://youtu.be/j0jTuCj7Qeg
- Aerial video: https://youtu.be/tVl6fn4YGFo
- Patrol video: https://youtu.be/nx39AmFOxhI

Recommendations

To improve the quality of information gathered and trust with Portlanders, the Police Commissioner and Chief should:

1. Adopt a directive related to investigating First Amendment activity that provides guidance for the appropriate collection of information to protect people's civil rights.
2. Create a procedure that limits access to sensitive information and promotes compliance with state law about collecting and maintaining political, religious, and social information that is not associated with criminal activity.
3. Adopt a technology directive that includes Council authorization of surveillance technology, advice from a privacy commission, and requirements for policies and reporting.
4. Add to the social media directive guidance for its use for investigations and a requirement to document the law enforcement purpose for searching individuals and groups.
5. Publish public reports on the Bureau's use of surveillance technology to ease the public's concerns about inappropriate intelligence-gathering and how devices are managed to prevent it.

The Police Commissioner and Police Chief generally agreed with our recommendations

View the responses to the audit from Mayor Ted Wheeler and Portland Police Chief Chuck Lovell at the end of this report.

How we did our work

Our audit objective was to determine whether privacy and civil liberties were protected in 2020 by Portland Police conducting investigations related to Black Lives Matter protests. A second objective was to determine whether the Bureau applied data governance standards for surveillance technology.

To accomplish our objectives, we

- Interviewed police managers, detectives, and officers involved in investigating protest-related cases; Criminal Intelligence Unit, Air Support Unit, and technology support staff; other City employees with expertise in open data, technology, law, and finance;
- Interviewed community members and representatives from the American Civil Liberties Union Oregon, Council on American Islamic Relations Oregon, Coalition of Communities of Color, Future of Privacy Forum, Imagine Black, Latino Network, PDX Privacy, Portland Copwatch, Secure Justice, Technology Association of Oregon, Unite Oregon, Western States Center, and Word is Bond;
- Reviewed rules related to intelligence gathering and surveillance technology, including Oregon Revised Statute 181A.250 and Bureau directives and standard operating procedures.
- Compared Portland's policies and practices to those in other jurisdictions, including policing First Amendment events in San Francisco and the District of Columbia; surveillance technology use in Oakland; and social media criteria developed by the Bureau of Justice Administration;
- Reviewed reports and evidence collected by police officers related to protests, including a random sample of 40 reports out of a population of 1,503. Our findings cannot be generalized to the population;
- Reviewed reports, bulletins, and tactical assessment generated by the Criminal Intelligence Unit, including a random sample of 33 products from a population of 471. Our findings cannot be generalized to the population;

- Inventoried surveillance technologies and their associated policies; compared them to best practices;
- Reviewed social media use by Criminal Intelligence Unit officers. We drew a random sample of 25 social media searches from the 114 people officers looked up between Aug. 8, 2021 and Oct. 15, 2021. Our findings cannot be generalized to the population;
- Reviewed a random sample of recordings take by the Air Support Unit. We reviewed recordings from 20 flights out of a population of 157. Our findings cannot be generalized to the population. We reviewed video from an additional four flights that occurred during large protests. We rode in the airplane for direct observations on September 1, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Office of Mayor Ted Wheeler
City of Portland

April 1, 2022

Mary Hull Caballero
City Auditor
1221 SW 4th Avenue, Ste. 310
Portland, OR 97204

Dear Auditor Hull Caballero,

Thank you for the opportunity to review and respond to your audit of police intelligence gathering. The people of Oregon have placed strong privacy protections on the ways in which law enforcement can collect and use information about the citizenry. I support these protections because of the very real history of shameful and biased surveillance practices by some law enforcement agencies in our state and nation. This history cannot be forgotten as we forge ahead with efforts to improve policing and work to earn trust between law enforcement and our community.

As Police Commissioner, my team and I will work with PPB to enact all five of audit recommendations, four in full and one in part. PPB's Policy Development Team will lead efforts to engage subject matter experts to ensure that all policies, existing or new, accurately reflect legal and procedural requirements. My administration will also continue to work with PPB to ensure these policies are implemented without delay.

Auditor, I appreciate your team's efforts and thoughtful consideration in making these assessments. Thank you for the important work you do.

Sincerely,

Mayor Ted Wheeler

1221 SW Fourth Avenue, Suite 340 ♦ Portland, Oregon 97204
MayorWheeler@PortlandOregon.gov

CITY OF PORTLAND, OREGON

Bureau of Police
Ted Wheeler, Mayor
Charles Lovell, Chief of Police
1111 S.W. 2nd Avenue • Portland, OR 97204 • Phone: 503-823-0000

Integrity • Compassion • Accountability • Respect • Excellence • Service

March 26, 2022

Dear Auditor Hull-Caballero:

We have reviewed the recent audit by your office regarding Police Intelligence Gathering and Surveillance. While we agree, fully or in part, to the five recommendations, we would like to provide critical, clarifying information in addition to our recommendation responses.

As we discussed with your team, the application of a Criminal Intelligence Unit (CIU) Standard Operating Procedure (SOP) to the five police reports was incorrect as the reports cited were not criminal intelligence (a sixth was an outside law enforcement agency bulletin). These reports were filed appropriately, in RegJIN, in accordance with Portland Police Bureau Directive 900.00 General Reporting Guidelines. The retention of such reports is bound by State Public Records Law. This information was shared with the audit team but this assertion remained in the final report. A new directive regarding criminal intelligence will address the overall concerns expressed by the audit regarding the safeguarding of information.

In addition, the audit uses the term "searching" when referring to the use of social media by investigators. It's important to note that while common vernacular might include the terms "searching the internet" or "searching social media," the term "search" has a specific meaning under the law. The City Attorney's Office pointed out the constitutional significance of the word "search" and, moreover, that various court opinions have held that viewing open source social media does not constitute a "search" under the Fourth Amendment. For clarity, when viewing publicly available social media information, it should not be labeled a "search" but instead a "query" or "viewing." The term "search," as it relates to viewing social media, should only be used to describe police accessing private information after obtaining a subpoena, search warrant, or court order.

As you will see the Portland Police Bureau is in the process of implementing several of the recommendations provided by your office as we continue to improve our transparency and trust building.

The following is our response to each of the audit's recommendations.

1. Adopt a directive related to investigating First Amendment activity that provides guidance for the appropriate collection of information to protect people's civil rights.

Agree, in part. Current Portland Police Bureau (PPB) Directive 635.10 Crowd Management/Crowd Control defines Freedom of Speech as: "The right to speak, associate,

assemble, and petition the government; speech that is protected by the First Amendment to the United States Constitution and Article I, sections 8 and 26 of the Oregon Constitution. For the purposes of this Directive, the rights issuing from both the federal and state Constitutions are collectively referred to as First Amendment rights."

Under the directive's policy section it states:

1. "The purpose of this Directive is to provide guidance for demonstrations, special events, the managing of crowds during demonstrations, and controlling crowds during civil disturbances."

2. "Freedom of speech, association, assembly, and the right to petition the government are subject to reasonable restrictions on the time, place, and manner of expression; the content of the speech does not provide the basis for imposing limitations on First Amendment rights."

3. "The Portland Police Bureau recognizes that the City of Portland has a tradition of free speech and assembly. It is the responsibility and priority of the Portland Police Bureau not to unduly impede the exercise of First Amendment rights and to provide for the safe and lawful expression of speech, while also maintaining the public safety, peace and order. A police response that impedes otherwise protected speech must be narrowly tailored to serve a significant government interest."

4. "While the First Amendment provides broad protections for the expression of speech, it does not provide protection for criminal acts including, but not limited to, riot, disorder, interference with traffic upon the public streets, or other immediate threats to public safety, peace or order."

This directive is currently under review. The Policy Development Team and subject matter experts will look to provide additional guidance on the appropriate collection of information, in accordance with Oregon Revised Statute (ORS) § 181A.250 (Specific information not to be collected or maintained), and in accordance with other Directives including but not limited to Directive 900 Report Writing, and Directive 660.00 Management of Criminal Intelligence Files (DRAFT).

All PPB members will be required to sign and acknowledge understanding the directive.

2. Create a procedure that limits access to sensitive information and promotes compliance with state law about collecting and maintaining political, religious, and social information that is not associated with criminal activity.

Agree. Directive 660.00 Management of Criminal Intelligence Files (DRAFT) provides definitions, policy, and procedures specific to criminal intelligence, including ORS § 181A.250. Upon adoption of this directive, all PPB members will be trained on the directive (including refresher training on ORS § 181A.250) and will be required to sign and acknowledge understanding the directive.

3. Adopt a technology directive that includes Council authorization of surveillance technology, advice from a privacy commission, and requirements for policies and reporting.

Agree, in part. Currently PPB follows the current state law that governs surveillance.

In accordance with ORS § 181A.250, members shall not collect or maintain information about the political, religious, or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

Furthermore, PPB Directive 344.05 Bias-Bases Policing clearly states:
"Bureau members are committed to respecting and preserving the constitutional rights of all individuals. Members are prohibited from taking or refraining to take any police action motivated by bias or prejudice and should, when appropriate, strive to engage community members in a positive manner."

Furthermore, "members shall not profile or discriminate against any individual who is a member of a legally protected class. Legally protected classes, as defined by federal or state statute, as well as case law, include an individual's race, color, national origin, citizenship, ethnicity, religion, sex, pregnancy, sexual orientation, gender identity, age, actual or perceived mental or physical disability, language (spoken or signed), marital or familial status, veteran status or any other protected status under law."

PPB will draft a Standard Operating Procedure (SOP) that more specifically governs the use and reporting of electronic surveillance technology.

More specifically, the SOP prohibits the use of electronic surveillance technology (EST) to:

- Conduct random or indiscriminate mass surveillance activities.
- Target a person based solely on individual characteristics, such as, but not limited to race, ethnicity, national origin, religion, disability, economic source or status, housing status, gender or sexual orientation.
- Harass, intimidate or discriminate against any individual or group.
- Conduct personal business of any type.
- To be combined with any type of facial recognition technology.

Authorized use of EST includes the following:

- Ongoing and current criminal investigations, where the investigator has reasonable suspicion to believe that person(s) to be surveilled, have committed a crime, or about to commit a crime, or are involved in the commission of a crime.
- Pursuant to a court order authorizing it's use in an investigation if required by law.

- With consent from the person(s) to which the EST is monitoring (900 Alarms, Threats / Safety).
- In instances where there is an imminent threat to life / safety where exigent circumstances exist.
- All uses of EST will follow current local, state and federal laws as to the use, placement, monitoring, and reporting.

As part of the SOP, the authorization of EST will be at the direction of the Commissioner in Charge of the Police Bureau. PPB must obtain Commissioner in Charge approval prior to any of the following:

- Accepting state or federal funds for surveillance technology.
- Acquiring, purchasing, or using new electronic surveillance technology.

4. Add to the social media directive guidance for its use for investigations and a requirement to document the law enforcement purpose for searching individuals and groups.

Agree. Current PPB Directive 311.40 Personal Use of Social Media does not govern the official use of social media and states that official uses will be governed by a separate directive.

The PPB Policy Development Team will work with subject matter experts (SMEs) to create a directive governing the official use of social media resources to include definitions, policies, and procedures. The directive may include policy and procedure on documenting the law enforcement purpose, if applicable and legally required.

5. Publish public reports on the Bureau's use of surveillance technology to ease the public's concerns about inappropriate intelligence-gathering and how devices are managed to prevent it.

Agree. As part of the PPB annual report, PPB will report the use of EST which will include the following:

a. Description of the technology was used, and the purpose of its use.
b. A general geographic area where the technology used.
c. Record of any community complaints in the use of the specific surveillance technology.
d. Any violations of Directives or Operating Procedures.
e. Overall effectiveness of the technology, or problems identified.
f. Any recommendations to the policy.

Chief of Police

Police Intelligence-Gathering and Surveillance:
Better management needed to protect civil rights

April 2022, Report #547

View this report online: www.portland.gov/police-intelligence-gathering

Audit Services
We audit to promote effective, efficient, equitable, and fully accountable City government for the public benefit. We assess the performance and management of City operations and recommend changes to the City Council and City management to improve services.

We follow Government Auditing Standards and have strict internal quality control procedures to ensure accuracy. We also operate the Auditor's Fraud Hotline and coordinate the City's external financial audit.

Audit Services | 1221 SW 4th Avenue, Room 310, Portland, OR 97204