SEATTLE CITY COUNCIL
CENTRAL STAFF

February 6, 2023

MEMORANDUM

To: Economic Development, Technology and City Light Committee
From: Lise Kaye, Analyst
Subject: Council Bill 120501 - Authorizing approval of uses and accepting the surveillance impact report for the Seattle Police Department's use of Computer, Cellphone, and Mobile Device Extraction Tools

On February 8, 2023, the Economic Development, Technology and City Light Committee will discuss Council Bill (CB) 120501. This CB would approve the Seattle Police Department's (SPD's) continued use of Computer, Cellphone, and Mobile Device Extraction Tools and accept the Surveillance Impact Report (SIR) and an Executive Overview for these technologies. The bill is intended to meet the requirements of Seattle Municipal Code Chapter 14.18, Acquisition and Use of Surveillance Technologies, which requires City of Seattle departments intending to acquire surveillance technology to obtain advance Council approval of that acquisition and of a surveillance impact report (SIR).[1] Departments must also submit a SIR for surveillance technology in use when Ordinance 125376 was adopted in 2017 (referred to in the ordinance as "retroactive technologies"), but failure to approve an ordinance for a retroactive technology does not require SPD to discontinue its use. Councilmembers may choose to amend the ordinance to request additional information or to request that SPD develop new and/or revised operational policies, which, if implemented, could restrict or modify the application of certain technologies.

This memorandum describes SPD's use of Computer, Cellphone, & Mobile Device Extraction Tools, summarizes recommendations from the Community Surveillance Working Group, describes whether and how each recommendation is addressed in the SIR and/or by current law, and summarizes responses by the Chief Technology Officer (CTO) and/or SPD. Finally, the memorandum identifies two policy issues for Council consideration.

Computer, Cellphone, & Mobile Device Extraction Tools

SPD uses the Computer, Cellphone, & Mobile Device Extraction Tools covered by this SIR to recover digital information or data from computers, cell phones, and mobile devices as part of criminal investigations. Two units in SPD manage these devices: the Sexual Assault and Child Abuse Unit and the Technical and Electronic Support Unit. Tools that extract information from computer devices take a photo of a computer's hard drive, preserving the entirety of digital information on the hard drive at a point in time. Additional tools include software that bypasses, deciphers, or disables a password and saves extracted files to a different device. Extracted information may include contact lists, call logs, text and multi-media messages, and Global Positioning System (GPS) locations.

[1] The Executive Overview summarizes SPD's allowable uses of Computer, Cellphone, & Mobile Device Extraction Tools. See also the memorandum summarizing process for developing a Surveillance Impact Report (SIR), consistent with Ordinances 125376 and 125679 and Ordinance 108333, Seattle's "Intelligence Ordinance," adopted in 1979 and amended in 1982 via adoption of Ordinance 100572.

Extraction may at times be done covertly, but SPD's policies allow use of these tools only after obtaining appropriate consent and/or legal search warrant authority. The SIR does not disclose the specific tools used by SPD to avoid the risk of countermeasures that could compromise ongoing and future investigations. SPD reports that the department mitigates potential civil liberties risks, including the risk of unlawful surveillance and the risks of racial or ethnicity-based bias from the use of these systems and associated data sharing, storage and retention through its warrant parameters, evidence procedures, and anti-bias policies. The Racial Equity Toolkit does not identify metrics to be used as part of the CTO's required annual equity assessments.

Surveillance Working Group Recommendations and CTO Response

The Community Surveillance Working Group's Impact Assessment for Computer, Cellphone, & Mobile Device Extraction Tools makes 10 recommendations to Council. The CTO's response finds that the "policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this technology." The CTO's response does not specifically address the Working Group's recommendations, but it identifies relevant citations from the SIR relative to the "key concerns" raised by the Working Group.

Table 1 summarizes which recommendations have been addressed in the SIR and/or are a matter of state law, and which would require a revised SPD policy and/or procedure. Attachment 1 provides additional detail on whether the SIR as drafted or current law addresses the Working Group's recommendations as well as relevant responses from the CTO and/or SPD.

Table 1. Surveillance Working Group (SWG) Recommendations Addressed in SIR and/or State Law

Addressed in SIR or State Law	SWG Recommendation(s) – Abbreviated
Would require revised SPD policy and/or procedure and updated SIR	#2. Restrict use to serious and violent offenses involving a non-property crime #3. Publicly disclose equipment information and contract documentation #4. Prohibit SPD from signing a non-disclosure agreement with technology manufacturer, vendor or reseller #5. Provide a monthly report of deployments #6. Destroy within 30 days information unrelated to a warrant #7. Ensure clear recordkeeping functions, detailed audit logs and automatic screen recording
Would be inconsistent with state law	#1. Prohibit consent searches on computer, cell phone, and mobile devices #8. Delete data if charges are dismissed or result in a conviction
See citations in Attachment A	#2. Define purpose and allowable uses. #5. Register each use of the tools #9. Provide strong access controls #10. Provide adequate training, including a privacy component

Policy Considerations

Central Staff has identified the following potential policy considerations and options.

1. Annual equity assessment metrics.

   SPD has not yet finalized metrics to be used in evaluating use of Computer, Cellphone, & Mobile Device Extraction Tools as part of the CTO's annual equity assessments. These assessments are intended to play a key role in determining whether the City's surveillance legislation is meeting the goals of the Race and Social Justice Initiative.

   Options:

   A. Request a report on the proposed metrics by a date certain.

   B. Take no action.

2. Mitigation of Civil Liberties Impacts.

   The SIR provides only a boilerplate reference to SPD's general anti-bias policing policies as providing mitigation against the risk of disproportionate surveillance and/or civil liberties impacts. In the absence of data tabulating the frequency of use of the Computer, Cellphone, & Mobile Device Extraction Tools and the corresponding incident types, it is not possible to evaluate whether the Systems are being used inequitably.

   Options:

   A. Request that SPD report on deployment of Computer, Cellphone, & Mobile Device Extraction Tools by incident type and location for the past three years and identify any disproportionate impacts.

   B. Take no action.

Attachment:

1. Surveillance Working Group Working Group Recommendations: SIR Citations, Current Law, and CTO and SPD Responses

cc: Esther Handy, Director
Aly Pennucci, Deputy Director
Brian Goodnight, Supervising Analyst

SEATTLE CITY COUNCIL
CENTRAL STAFF

Attachment 1: Surveillance Working Group Working Group Recommendations: SIR Citations, Current Law, and CTO and SPD Responses

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
1. Prohibit the use of consent searches on computer, cell phone, and mobile devices.	**SIR §1.1** These technologies are utilized only with the device owner's consent or pursuant to search warrant authority. **CTO Response:** The conditions under which the devices are used are clearly outlined in the SIR and are further regulated by RCW 9.73.
2. The purpose and allowable uses of Mobile Device Forensic Tools must be clearly defined, and any SPD use must be limited to that specific purpose and those allowable uses. The specific incident types for which these tools may be used must be clearly specified, e.g., use should be restricted to violent or serious offenses involving a non-property crime..	**SIR §1, 2 and 4 provide this information.** *SMC 14.12 (the "Intelligence Ordinance) governs the collection of data for a criminal investigation.* *The SIR does not limit the use of these tools to specific incident types.*
3. Vendor names, model numbers, purchase orders, and contracts must be publicly disclosed.	*SPD has requested not to publicly disclose this information to avoid the risk of countermeasures that could compromise ongoing and future investigations.*
4. SPD must be prohibited from signing a non-disclosure agreement with any manufacturer, vendor, or reseller of these tools.	Not addressed in the SIR. *SPD is not aware of having signed any such non-disclosure agreement.*
5. Register each use of these tools and provide a monthly transparency report detailing the deployments.	**SIR §3.1** The Sexual Assault Unit (SAU) keeps a log of device uses, including the date, case number, detective assigned, device information and warrant parameters. The Technical and Electronic Support Unit (TESU) logs each deployment and maintains all request forms. *SPD's operational policies do not currently require a monthly report.*
6. Destroy any information unrelated to the purpose of a warrant within 30 days.	**SIR §3.1** If no data is collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order warrant (as determined by the judge), the device is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file

Working Group Recommendation	Whether/How Addressed by SIR, CTO or SPD and/or Current Law
7. These tools must have clear recordkeeping functions, detailed audit logs and automatic screen recording.	Not addressed in the SIR. **CTO Response:** SPD has existing audit functionality with the Office of Inspector General, unit supervisors, or the federal monitor. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, the Surveillance Ordinance does mandate yearly auditing of these technologies by the Office of Inspector General and the IT department in some circumstances. *Per SPD, there are limited internal logs in the operating systems/software, but these are temporary and not utilized by SPD for audit/tracking purposes. All data on a case is forwarded to the case detective and handled by them with regards to disposition and retention.*
8. All data from these tools must be promptly deleted if charges are dismissed or do not result in a conviction.	Not addressed in the SIR. *Per SPD, all data is processed with the case so retention and handling of the data is dictated by the current department policies on digital evidence processing and retention. The examiner does not retain the data once they are done assisting with the case.*
9. Require strong access controls for licensed workstations and extracted data.	**SIR §3.1** The technology requires a personal password to log onto the device and a separate password from the login to access extracted data. SAU data is stored on a separate secured server with access limited to authorized SPD SAU users.
10. Provide adequate training for all personnel who use these tools, including a privacy component.	**SIR §3.3** Select users in the SAU and TESU units are trained in the use of data extraction devices. These users must attend extensive training and vendor certification prior to being authorized to perform extractions and continuing training re-certification that is available through the technology provider. **SIR 7.2** SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training.