June 2, 2022

Seattle Information Technology
700 5th Ave, Suite 2700
Seattle, WA 98104

RE: ACLU of Washington Comments on Group 4b Surveillance Technologies

AMERICAN CIVIL LIBERTIES UNION
Washington

P.O. Box 2728
Seattle, WA 98111-2728
(206) 624-2184
aclu-wa.org

Michele Storms
*Executive Director*

On behalf of the ACLU of Washington, we write to offer our comments on the surveillance technologies included in Group 4b of the Seattle Surveillance Ordinance implementation process.

The six Seattle Police Department (SPD) technologies in Group 4b are covered in the following order:

1. GeoTime
2. Mobile Device Extraction Tools
3. Camera Systems
4. Remotely Operated Vehicles
5. Crash Data Retrieval Tool
6. Tracking Devices

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of important questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology. Answers to these questions should be included in the updated SIRs provided to the Community Surveillance Working Group and to the City Council prior to their review of the technologies.

## GeoTime

### I. *Background*

GeoTime is a geospatial analysis software that visually maps data over space and time. It raises serious privacy and civil liberties concerns. These concerns are three-fold. First, GeoTime's data aggregation and analysis features are incredibly invasive. They enable law enforcement to gather and

create correlations between large amounts[1] of personal data from numerous sources at a time, including call detail records, mobile forensic data, GPS, location-tracking data, and social media data, creating very detailed, personalized maps of people's lives.[2]

Secondly, GeoTime's capabilities are excessively broad and intrusive. It creates links between people and reveals "patterns of behavior and relationships between seemingly unconnected events and entities,"[3] producing a dragnet that potentially captures the private data of those not involved in the crime or event being investigated. It may therefore implicate innocent individuals in a crime.

Lastly, and relatedly, GeoTime may be used to surveil and ultimately chill constitutionally protected activities concerning religion, expression, and assembly. For example, GeoTime advertises a "Trip Counter" feature, which enables users to "find new locations of interest [e.g. a mosque, an abortion clinic, or the site of an anti-police violence rally] and get quick answers. Who visited? How many times? When was each visit?"[4]

SPD has access to a potentially wide variety of undisclosed GeoTime products with various surveillance functionalities. GeoTime is owned by UnCharted Software, which sells a number of GeoTime products with various surveillance functionalities. The SIR does not disclose which GeoTime products SPD owns. At the 5/18/22 public engagement meeting with SPD, following up from a question asked at the first public engagement meeting on 4/18/22, the SPD representative stated that SPD owns two GeoTime Desktop licenses on computers secured in the Intel Unit and seven GeoTime Glimpse licenses that allow web access to the portal.[5] According to the SPD representative, three detectives have access to GeoTime and there is one detective who accesses it regularly.[6]

Though the SIR does not disclose GeoTime Desktop's functionalities or how they work,[7] there is evidence that SPD can use GeoTime to analyze

---

[1] On its website, GeoTime advertises that its "Enterprise" product can "handle millions of records at once." "GeoTime Enterprise," *GeoTime,* Accessed May 12, 2022, http://www.geotime.com/enterprise.

[2] The GeoTime website advertises that its "Desktop" product can "layer datasets to provide a comprehensive picture of activity." See "GeoTime Enterprise."

[3] "GeoTime for Analysis of Behavior in Time and Geography," *Oculus Info Inc.,* 2011, Accessed May 12, 2022, https://www.uncharted.software/assets/GeoTime_Overview.pdf.

[4] "GeoTime Desktop," *GeoTime*, Accessed May 12, 2022, https://www.geotime.com/desktop.

[5] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2," Accessed June 1, 2022, https://www.seattle.gov/event-calendar?trumbaEmbed=view%3Devent%26eventid%3D159435131

[6] Ibid.

[7] Seattle Police Department, "2022 Surveillance Impact Report: GeoTime," Accessed May 12, 2022,

social media data. At the 5/18/2022 public engagement meeting, the SPD representative, following up from a question at the first public engagement meeting, stated that SPD does not use the social media analysis functionality of GeoTime.[8] However, it remains unclear which of the remaining functionalities SPD does use. It should be noted that although SPD states they do not use the social media analysis functionality, it is unclear whether they can still input social media data into GeoTime in order to gain insights via the other functionalities such as the mobile device forensic analysis functionality. This functionality ostensibly analyzes data extracted from people's phones, which SPD has the capability to do with their mobile device extraction tools.[9] This strongly suggests that even without the social media analysis functionality, analysis of social media data is nevertheless something SPD can capably do with GeoTime, given that 99% of people access their social media from their mobile phone.[10] It is noteworthy that GeoTime Desktop can import data from Cellebrite,[11] one of the mobile device extraction tools that public records show SPD owns or has owned in the past.[12]

In general, SPD provides a very general and vague explanation of GeoTime's capabilities in the SIR that does not meaningfully convey the vast number of sources of personal and private data that SPD can aggregate and analyze within GeoTime, and the kinds of outputs it generates. The GPS analysis functionality alone, for example, can use the following data sources: automated license plate readers, transit pass, automated toll pass, crime incident data, witness/informant statements, in-vehicle GPS system, Google location history, Uber/Lyft location reports, and on-board vehicle data (e.g., odometer, speed, location logs, saved locations/routes, connected devices/media, call logs), among others.[13]

Despite how powerful this tool is, the SIR does not indicate use cases for GeoTime, or define limitations on the kinds of data sources that SPD can input. There is also a lack of clarity on the oversight measures in place, such as whether GeoTime has audit logs and what data those logs might collect. When asked at the 5/18/22 public engagement meeting about the last time

---

https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20%20Geotime.pdf.

[8] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

[9] Seattle Police Department, "2022 Surveillance Impact Report: Computer, Cellphone, & Mobile Device Extraction Tool," Accessed June 1, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Computer%2C%20Cellphone%2C%20%26%20Mobile%20Device%20Extraction%20Tools.pdf.

[10] Dean, Brian, *BackLinko*, "Social Network Usage & Growth Statistics: How Many People Use Social Media in 2022?, 2021, https://backlinko.com/social-media-users.

[11] "GeoTime Desktop."

[12] On file with the author.

[13] Khamisa, Adeel, "GeoTime: GPS Data Analysis – Tips and Best Practices," *GeoTimeInfo,* October 10, 2021, https://www.youtube.com/watch?v=oOUKjwDKCVo.

an audit was conducted, the SPD representative referred the question-asker to the Office of Inspector General (OIG), which strongly suggests that no audit has been done by OIG, and certainly no audit conducted by SPD's Audit, Policy, and Research Section (APRS—SPD's auditing body) or the federal monitor.[14] Moreover, the SIR does not indicate there are any validation measures for the data inputs, or outputs such as images, animated videos, or PowerPoint files of mapped data. When asked at the 5/18/22 public engagement meeting whether there are measures in place to verify the accuracy of GeoTime data and analyses, the SPD representative stated that this verification is part of the normal investigative process, and an SPD officer will validate GeoTime data and analyses.[15] This is troubling, given that GeoTime enables SPD to annotate maps/graphics & edit visualizations used as the output. It is also concerning because one of the supported file formats for imported data is an Excel file format, which can be edited.[16] This means SPD can modify or fabricate records that GeoTime analyzes. Without a way to track SPD's movements inside the application, it is hard to know whether data or the output has been tampered with or manipulated. This has high costs given that outputs are shared in court presentations, used as evidence, etc.

Another concern is the lack of clarity regarding how SPD obtains the data that GeoTime analyzes. For example, the SIR states that the data are obtained by investigators "under the execution of court ordered warrants, including data from cellular providers and from data extracted from mobile devices," and it cites to the Mobile Device Extraction Tools SIR.[17] However, this contradicts what is actually written in the Mobile Device Extraction Tools SIR, which is that mobile device forensic data can also be obtained via consent agreement with the mobile device owner.[18] Clarity is needed as to whether data can be obtained based on consent alone, what data can be obtained under consent agreement as opposed to search warrant, and under what circumstances. Moreover, there must be policies in place

Finally, there is a lack of clarity about who at SPD has access to GeoTime data inputs and outputs, with which entities outside SPD those data are shared (including law enforcement agencies outside the state), and how those data are shared. When asked about this at the 5/18/22 public engagement meeting, the SPD representative stated that SPD does share case info with other law enforcement agencies as it relates to

[14] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[15] Ibid.
[16] "Frequently Asked Questions," *GeoTime*, Accessed May 12, 2022, https://www.geotime.com/frequently-asked-questions.
[17] SPD, "GeoTime," 6.
[18] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 3.

investigations.[19] This is a particularly pressing issue given recent indications that the US Supreme Court is poised to overturn *Roe v. Wade*, and that states are ready to pass legislation criminalizing abortion.[20] Our state recognizes the individual right to abortion care and it is anticipated that Washington will see an influx of people from neighboring states seeking abortion services here.[21] GeoTime may be used to surveil these people and it is critical that there be restrictions on the ability of SPD to share these data and analysis with law enforcement and other agencies outside the state. Moreover, for any data that are shared, there should be stringent data storage, retention and transfer/sharing safeguards in place to protect the data.

Given the lack of adequate policies described by the SIR and the number of unanswered questions that remain, we have concerns that SPD's use of GeoTime may infringe upon people's civil rights and civil liberties.

## II. *Specific Concerns*

a. **Lack of Clarity on How Often GeoTime is Deployed and Who Determines Whether Deployment Will Occur.** According to the SIR, "GeoTime is utilized frequently by investigators during the investigation of crimes." Conversely, at the public engagement meeting on 4/27/22, SPD representative stated that SPD "rarely" used GeoTime. At the public engagement meeting on 5/18/22, the SPD representative stated that it is used 1-2 times a week by one detective.[22] It remains unclear how often GeoTime is deployed (e.g., how many times a week? For how many cases?). In addition, the SIR provides no information about who determines in which cases/when to use GeoTime.

b. **Lack of Clarity on What Data SPD Inputs Into GeoTime.** Regarding data that SPD manually inputs into GeoTime to produce visualizations, the SIR refers variously to "geodata, such as latitude

[19] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[20] Almanza, Emily Galvin, "The Criminalization of Abortion: What to Expect in a Post-Roe United States," May 6, 2022, https://www.teenvogue.com/story/criminalization-of-abortion-laws-roe.
[21] Ahmed, Tasnim, "As States Move to Restrict Abortion Access, Neighboring States Prepare for Surges in Demand, *CNN,* April 13, 2022, https://www.cnn.com/2022/04/13/health/neighboring-states-abortion-bans/index.html.
[22] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

and longitude" (4) and "location information," (4) "cell records," "cell site locations," (4) "criminal information," "data from cellular providers and from data extracted from mobile devices" (6), and "Personally Identifiable Information" (14). It does not provide a comprehensive list of data sources that GeoTime aggregates and analyzes.

c. **Lack of Clarity on How SPD Obtains the Data it Inputs into GeoTime.** The SIR states: "The data analyzed using GeoTime is obtained by investigators under execution of court ordered warrants, including data from cellular providers and from data extracted from mobile device."[23] This contradicts the Computer, Cellphone, & Mobile Device Extraction Tools SIR, which states that extraction tools are "used only with the device owner's consent, pursuant to search warrant authority or in certain circumstances outlined in RCW 9.73.210."[24] The implication is that search warrants are not the only means through which data are obtained. Relatedly, when asked at the 5/18/22 public engagement meeting about whether any private information without a warrant or any public data are ever added to GeoTime, the SPD representative stated that SPD does input public data.[25] He did not respond to the part of the question asking whether any private information without a warrant is added to GeoTime.

d. **Lack of Clarity on How SPD Accesses GeoTime and What Access Controls are in Place for GeoTime.** The SIR states that GeoTime can be accessed via licensed workstations and through an online internet portal.[26] It later states that "access to the application is limited to SPD personnel via password-protected login credentials. Data is securely input and used on SPD's password-protected network with access limited to authorized users."[27] It's unclear from this explanation: (1) what software-level security controls (authentication, authorization, logging, etc.) are in place for *both* the GeoTime workstations and for the portal; (2) whether they are the same access control mechanisms for both the portal and the workstations; and (3) where the internet accessible portal can be accessed from (e.g. can it be accessed from a cell phone?). Without

[23] SPD, "GeoTime," 6.
[24] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 5.
[25] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[26] Ibid., 5.
[27] Ibid., 9.

this information, it is difficult to assess the privacy risks and suggest measures to mitigate them.

e. **Lack of Clarity on Which SPD Personnel/Units and How Many Have Access to GeoTime.** In one part of the SIR, it states, "Only trained, backgrounded, and CJIS certified SPD detectives have access to GeoTime."[28] In a different part, it states that log-in credentials "are granted to employees with business needs to access GeoTime" without any elaboration on which employees and the definition of "business needs" (8). At the 5/18/22 public engagement meeting, an SPD representative stated that three detectives have access to GeoTime, and one of those three uses it regularly.[29] However, it remains unclear whether these are the only individuals in SPD who have access to GeoTime via both the licensed workstations and the internet portal. There is a large discrepancy between the number of licenses for the internet portal (7 GeoTime Glimpse licenses) and the number of people who purportedly have access (3).

f. **Lack of Clarity on Which SPD Personnel Have Access to Data Output Generated from GeoTime.** The SIR states that GeoTime is "used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files."[30] However, the SIR does not state which SPD employees has access to those exported files created by GeoTime and how many SPD employees have access to them.

g. **Lack of Clarity About Data Storage, Safeguards, and Retention.** In response to data storage and retention questions, the SIR states that GeoTime "does not collect information or data…No information is saved inside the GeoTime tool."[31] While it may be the case that technically GeoTime does not "collect" data, SPD manually inputs data into GeoTime to generate maps and other visualizations and that data must be hosted/stored somewhere. However, that location is not provided in the SIR. At the 4/27/22 public engagement meeting, the SPD representative stated the internet accessible portal is hosted by GeoTime (i.e., UnCharted Software) but the data that GeoTime uses are not

[28] Ibid., 5.
[29] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[30] SPD, "GeoTime," 7.
[31] Ibid.

hosted there and that he would have to check on where the data are stored.[32] The SIR also does not indicate for how long the data are stored/hosted in that location, what safeguards are in place to protect it, who has access to the data, including whether UnCharted Software stores or has access, and when that data must be deleted.

h. **Lack of adequate policy and practices for validating the accuracy of the data and the analysis that GeoTime provides.** In the SIR, SPD evades the question of how GeoTime checks the accuracy of the information collected by stating: "GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators an exports complex geospatial maps…"[33] This response does not address what measures SPD takes to ensure that the data it inputs into GeoTime is accurate. It also does not address what steps it takes to validate the accuracy of the GeoTime data output/analysis. GeoTime is a powerful tech that purports to help investigators, among other things, "dispute an alibi or demonstrate criminal intent."[34] Without validation of its analyses, it could have deleterious impacts on the lives of the people whose data is inputted, including implicating the wrong person in a crime.

i. **Inadequate Oversight Policies.** In response to the question about safeguards in place for protecting data and to provide an audit trail, the SIR states the entities authorized to conduct audits but it does not address whether there are self-audits, third-party audits, or review. It also does not address whether GeoTime has an audit log or not, what that log contains if they in fact have one, and whether that log is sufficient to conduct an audit investigation. At the 4/27/22 public engagement meeting, the SPD representative expressed uncertainty about whether there is a direct audit log about what actions each user takes inside the application.[35] At the 5/18/22 public engagement meeting, when asked about the last time an audit was conducted on SPD's use of GeoTime, the SPD representative referred the questioner to OIG, which strongly suggests no audit has been conducted by OIG or any other entity, including APRS and the federal monitor.[36] Without detailed auditing capabilities, or regular auditing, it is not possible to have sufficient

[32] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[33] Ibid., 13.
[34] "Frequently Asked Questions."
[35] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #1," Accessed June 1, 2022, https://www.seattle.gov/event-calendar?trumbaEmbed=view%3Devent%26eventid%3D159435112.
[36] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

oversight into how SPD uses GeoTime and whether they are complying with policy.

j. **Lack of Clarity and Transparency on What Other Tech GeoTime Interfaces With.** The SIR does not specify which other tech, if any, GeoTime interfaces with. SPD stated at the 4/27/22 public engagement session that it doesn't interface with PredPol, Crime View or other predictive policing utility, yet when a member of the public asked if SPD would include that in the SIR, SPD's response was that it was "not a tenable option" for SPD to list all the tech that GeoTime does not interface with.[37] Without this information, it is difficult to adequately assess the privacy risks that GeoTime poses.

k. **Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not fully explain use cases for GeoTime and does not include policies placing limits on its uses.
    i. **Visualization vs. Predictive Policing.** Without clearer usage limits, analyses provided by GeoTime might be used for predictive policing.
    ii. **Data.** There are ostensibly no policies governing limits on the kinds of data sources that can be manually input into GeoTime.
    iii. **Type of crime.** In response to the question of "what are acceptable reasons for access to the equipment and/or data collected?" the SIR states: "Data is only accessed as part of ongoing criminal investigations or under the City of Seattle Intelligence Ordinance."[38] It is not specified if there are limits to the type of events (e.g. First Amendment protected demonstrations) or crimes that SPD will investigate via GeoTime (e.g. petty crimes like graffiti and trespassing). At the 4/27/22 public engagement meeting, the SPD representative indicated there is no policy governing the incident types for which SPD may use GeoTime but claimed that "SPD doesn't have time to apply" GeoTime to "lower-level offenses."[39] The implication is that with more time and resources, there is nothing stopping SPD from using GeoTime to investigate more offenses, even minor ones.

[37] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #1."
[38] SPD, "GeoTime," 8.
[39] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #1."

l. **No Policies Restricting Use of GeoTime's Additional Surveillance Features.** The SIR does not provide sufficient information about what components of GeoTime SPD uses and doesn't use. For example, during the 4/27/22 public engagement meeting, when asked about SPD's use of GeoTime's Social Media Analysis functionality, the SPD representative stated SPD does not use this feature of GeoTime.[40] He claimed this fact was in the SIR, which it is not.[41] There also don't appear to be any policies restricting SPD's use of Social Media Functionality. Without a full accounting of the features of GeoTime that SPD uses, it is impossible to assess all the potential privacy risks. With regard to the Social Media Analysis Functionality in particular, social media data will include the private information of non-targeted people so if SPD is using it, measures are necessary to ensure those data are protected and not misused in the GeoTime analysis.

m. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share GeoTime data and analyses with outside entities[42] but does not address whether SPD maintains a record of those disclosures. It only addresses recording of public disclosure requests made pursuant to the Public Records Act and the City of Seattle Intelligence Ordinance. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

n. **Inadequate Data Sharing Policies.** The SIR offers only an extremely general description of who might receive GeoTime data and analyses and how such data would be shared. Neither security protocols for transferring data nor for ensuring that shared data are properly deleted are explicated in the SIR. Indefinite retention of data and insecure sharing processes could lead to exposure of sensitive data, with manifold consequences for those whose data is inputted into GeoTime.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

[40] Ibid.
[41] SPD, "GeoTime."
[42] Ibid., 11.

a. Which GeoTime functionalities does SPD use?
b. Which SPD units have access to GeoTime? How many SPD employees have direct access to GeoTime, both via GeoTime Glimpse (internet portal) and GeoTime Desktop (workstations)?
c. Which SPD units have access to the files (e.g. maps and other visuals) generated by GeoTime? How many SPD personnel have access to those files? What other agencies or groups outside of SPD that have access to GeoTime files?
d. What other technology does GeoTime interface with?
e. What are all the data sources that SPD inputs into GeoTime?
f. Can data manually input into GeoTime be obtained without a warrant and based on two-party consent alone? If so, under what circumstances may the data be obtained without a warrant and what rules set the parameters for GeoTime's use?
g. How often is GeoTime deployed? How many times/for how many investigations a week is it deployed?
h. Who determines whether GeoTime should be deployed?
i. What is the criteria for deployment? Can any detective determine based on their own discretion that deployment of GeoTime is necessary for their investigation? Is supervisor approval required?
j. What software-level security controls are in place for both the GeoTime workstations and for the internet accessible portal? Are they the same access control mechanisms? Where can the internet accessible portal be accessed from (i.e., a mobile device)?
k. Where does SPD store/host the data it manually inputs into GeoTime? Is there a difference in where the data are hosted or stored when GeoTime is accessed via the portal vs. via a workstation?
l. How long are the data stored there? When are the data deleted?
m. What safeguards are in place to protect the data that is inputted into GeoTime (is the data encrypted? What are the access control mechanisms?)
n. How does SPD validate the accuracy of the data it manually inputs into GeoTime, as well as GeoTime data outputs/analyses?
o. Which SPD personnel have access to the data output/files generated from GeoTime? How many SPD personnel have access to the GeoTime data outputs?

p. What is the nature of the training that SPD personnel receive on GeoTime? How many hours of training do they receive? What does the training cover? Do they receive periodic updated training? Are they provided privacy training specific to the privacy risks associated with GeoTime?
q. Does GeoTime have an audit log? If so, what does it contain/what information does it collect? Does it log what actions each user takes inside the application?
r. How often is SPD's GeoTime subject to an audit? When was the last audit of SPD's GeoTime conducted and by which entity (APRS, OIG, or the federal monitor)? Where are the audit reports located?
s. Does SPD maintain a record of all disclosures of GeoTime data and analyses/output, including those to outside entities?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of GeoTime. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- There is a specific and restricted purpose of use. There must be a policy defining clear limits on GeoTime's uses, including narrow parameters for: (1) using data that were obtained via consent agreement as opposed to a search warrant; (2) using GeoTime in conjunction with other technology; (3) the use of all of GeoTime's surveillance features; and (4) the event type or crime type that GeoTime is used for.
- The use of GeoTime's social media analysis functionality must be prohibited.
- The use of GeoTime for predictive policing must be prohibited.
- People whose data is obtained via consent agreement must be informed, as part of the consent process, that their data will be inputted into GeoTime.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for both the GeoTime licensed workstations and for the internet accessible portals, as well as for access to GeoTime outputs and analyses.
- Any data inputs or outputs must be securely shared with third parties and properly deleted.

- SPD must disclose/log to whom and under what circumstances GeoTime data inputs and outputs are shared.
- There must be adequate training for all personnel who use GeoTime and the training must include a privacy component specific to the risks inherent to using GeoTime as an investigative tool.
- There must be a detailed direct audit log of user actions within GeoTime, and SPD must produce a publicly available annual audit report about its use of the technology.
- Any data inputs hosted by UnCharted Software or data outputs created via GeoTime are not owned by, used by, or retained by UnCharted Software, and any data inputs and data outputs are properly secured.
- There must be measures in place to validate the accuracy of GeoTime data inputs and outputs/analyses.

## Computer, Cell Phone, and Mobile Device Extraction Tools

### I. *Background*

A computer, cell phone, and mobile device extraction tool, also known as mobile device forensic tool (MDFT),[43] is a powerful software technology that allows police to circumvent most security features on a person's device to easily extract all the data on the device—including call logs, contacts, text messages, emails, social media posts, photographs, location information, search history, and financial transactions—and systematically search and analyze it. As such, this tool "represent[s] a dangerous expansion in law enforcement's investigatory powers."[44] Its use by SPD raises serious privacy concerns, given the sheer amount of personal, sensitive information stored on people's smartphones. Eighty-five percent of U.S. adults own a smartphone,[45] and they generally keep it on their person wherever they go. The implication is that the vast majority of people are vulnerable to having their phones invasively searched by law enforcement. This risk is particularlyacute and the privacy infringement is particularly egregious for

[43] National Institute of Standards and Technology, "Mobile Security and Forensics," Accessed May 17, 2022, https://csrc.nist.gov/Projects/Mobile-Security-and-Forensics/Mobile-Forensics.
[44] Koepke, Logan, et al. "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," *UpTurn,* October 20, 2020, https://www.upturn.org/work/mass-extraction/.
[45] Pew Research Center, "Demographics of Mobile Device Ownership and Adoption in the United States," April 7. 2021, https://www.pewresearch.org/internet/fact-sheet/mobile/?menuItem=d40cde3f-c455-4f0e-9be0-0aefcdaeee00.

the many low-income people who rely exclusively on their smartphone to access the internet.[46]

The use of MDFTs by SPD also raises serious civil liberties concerns. This technology enables police to conduct an excessively broad and intrusive search. It provides access that "can be disproportionately invasive compared to the scope of evidence being sought and poses an alarming challenge to existing Fourth Amendment protections."[47] Without limitations on use cases and narrowly defined parameters around, for example, what data can be extracted and for what purpose, the use of this tech is rife for misuse. In particular, the ACLU-WA is concerned about the use of MDFTs by SPD to surveil and ultimately chill constitutionally protected First Amendment activities concerning religion, expression, and assembly. Furthermore, use of MDFTs by SPD likely tracks with disparities in SPD policing practices[48] and statewide criminal legal system outcomes.[49] Therefore, it likely disproportionately impacts marginalized groups, including Black people, people of color, and people experiencing poverty or houselessness.

SPD does not disclose in the SIR which vendor provides its MDFT tools, which products it uses, and how many licenses it has for each product. When asked about its MDFT vendors at the 5/18/22 public engagement meeting, the SPD representative stated that SPD will not disclose what vendors they use because this information "could hinder investigative efforts."[50] In particular, the representative cited concerns that having this information would help people create so-called "counter-measures."[51] Without vendor information though, it is challenging to assess the privacy and civil liberties impacts of the technology. It is also antithetical to the

---

[46] "As of early 2021, 27% of adults living in households earning less than $30,000 a year are smartphone-only internet users—meaning they own a smartphone but do not have broadband internet at home." Vogels, Emily A., "Digital Divide Persists Even As Americans with Lower Incomes Make Gains in Tech Adoption," June 22, 2021, https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption.

[47] Koepke, et al., "Mass Extraction."

[48] See, e.g., Kasakove, Sophie, "Seattle Bike Helmet Rule is Dropped Amid Racial Justice Concerns," *New York Times*, February 18, 2022, https://www.nytimes.com/2022/02/18/us/seattle-bicycle-helmet.html; "Report Finds Racial Disparities in Stops, Arrests, Use-of-Force by Seattle Police Officers," *KOMO News*, July 15, 2021, https://komonews.com/news/local/report-finds-racial-disparities-in-stops-arrests-use-of-force-by-seattle-police-officers.

[49] "Race and Washington's Criminal Justice System: 2021 Report to the Washington Supreme Court," *Fred Korematsu Center for Law and Inequality, Seattle University School of Law*, https://law.seattleu.edu/media/school-of-law/documents/centers-and-institutes/korematsu-center/initiatives-and-projects/race-and-criminal-justice-task-force/task-force-20/2021-race-and-washingtons-criminal-justice-system-report.pdf.

[50] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

[51] Ibid.

spirit and purpose of the Seattle Surveillance Ordinance process, which was established in part to create transparency about Seattle agencies' use of new and old technology.

Via Public Records Act disclosures, the ACLU-WA is aware that SPD uses or has used a variety of device extraction tools, including but not limited to: Cellebrite[52] (and Cellebrite's Advanced Investigative Services, or CAIS); Black Bag Forensic Software; GrayShift GrayKey; Octoplus; Medusa Pro; MSAB Incorporated aka Micro Systemation, and XRY Office Version.[53] It's noteworthy that law enforcement often purchase tools from multiple vendors in order to maximize the types of devices they can extract data from (e.g., iPhone, Android, etc.).[54]

***Concerns with Data Extraction and Analysis***

MDFTs can reliably access and extract some, if not all, data from most phones, with very few exceptions.[55] According to the SIR, there are very few hurdles to SPD officers or detectives using this technology, despite how easily it provides full access to device data. The SIR states that in order to use MDFTs, investigators must fill out a request form that includes a copy of consent or search warrant authorizing the extraction.[56] The SIR further states that "unit supervisors are responsible for screening all technology deployments to ensure that the appropriate authorities are in place before approving deployment of tracking technology."[57] However, the SIR does not specify any criteria for determining whether MDFTs should be deployed in the first place—i.e., what constitutes a case where the deployment of MDFTs is considered necessary?

The SIR does not adequately convey this invasiveness and the implications for privacy rights and civil liberties. It describes the data extraction process in the following way: "Extracting information from computer devices involves taking a snapshot of a computer's hard drive, preserving the entirety of digital information on the hard drive at a particular point in time."[58] This description does not explicitly communicate the wide range of data sources and the sheer amount of data that MDFTs can extract and analyze, which is troublingly vast. On the most basic level, MDFTs can extract photographs taken from smartphones along with the metadata from

---

[52] Hvistendahl, Mara and Sam Biddle, "Use of Controversial Phone-Cracking Tool is Spreading Across Federal Government," *The Intercept,* February 8, 2022, https://theintercept.com/2022/02/08/cellebrite-phone-hacking-government-agencies/.
[53] On file with the author.
[54] Koepke et al., "Mass Extraction."
[55] Ibid.
[56] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 6.
[57] Ibid., 8.
[58] Ibid., 5, DRAFT SIR - Computer, Cellphone, & Mobile Device Extraction Tools.pdf (seattle.gov)

those photos, such as the GPS coordinates of where a photo was taken and the time and date it was taken, thereby providing a "geographic record of the person's movements," as well as the movements of anyone else in those photos.[59] MDFTs can also extract app data and access location information, in-app communications, and in-app photos from those apps.[60] Cellebrite software tools, for example, can extract and interpret data from at least 181 apps on Android's operating system and at least 148 apps on Apple iPhones.[61] These can include everything from social media apps like Instagram, Facebook, Snapchat, and Twitter; navigation apps like Google Maps; web browsers like Chrome and Firefox; and dating apps like Tindr, Grindr, and OkCupid.[62] They can even extract data from encrypted messenger apps like Signal and Telegram.[63] MDFTs are also frequently updated by the vendor in order to be able to extract data from an ever growing number of apps.[64]

Many apps are account-based, i.e., data are stored on the cloud as opposed to directly on the device, and can be accessed remotely. MDFTs, including Cellebrite, often have specific features or products that provide law enforcement access to those data as well.[65] Google's Location History is an example of a particularly rich cloud-based data source that MDFTs enable access to. Any user with their location history turned on in their Google account will have years' worth of precise location records stored online in their Google Account, which can be extracted with MDFTs.[66]

In addition to app data, MDFTs can access "deleted" data from phones, as well as phone meta data, i.e., data about how people use their phone (e.g., when certain applications were installed and deleted, how often an application was used, when a device was locked or unlocked, when a message was viewed, etc.).[67]

MDFTs commonly extract all these user data by circumventing the device's security features using various tactics that exploit the device's security flaws or built-in diagnostic or development tools. For example, since March 2016, Cellebrite has added lock-bypass support for about 1500 devices, which exploits device vulnerability to force the phone to skip the passcode-checking step when it turns on.[68] Moreover, to get around encryption, MDFTs can repeatedly guess the decryption key, which is usually based on

[59] Koepke et al., "Mass Extraction."
[60] Ibid.
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.

the phone's log-in password, to identify the correct one, thereby enabling the MDFT to decrypt the phone's contents.[69] It's been estimated by John Hopkins professor and security technologist Matthew Green that this password-guessing process would take at most 13 minutes for a 4-digit passcode (average 6.5 minutes), 22 hours for 6 digits (average 11.1 hours), and 92 days for 8 digits (average 46 days).[70] iPhones (which are the device used by 45% of smartphone users) default to a six digit passcode. With GrayKey or Cellebrite Premium (both of which SPD has owned or owned in the past), law enforcement can decrypt the data on an iPhone in less than a day, and on, average less than half a day.[71]

Even without an encryption key though, MDFTs can still extract plenty of phone data because phones don't encrypt all data on a device.[72] There are also many phones that don't encrypt user data, or that have encryption schemes that can be dismantled. If all else fails, law enforcement can install on the device a spyware tool, such as the one provided by Grayshift (a vendor SPD uses), which enables phone access by recording future password entries[73]

If law enforcement is unable to access and extract data from a device in house, they can send it to the vendor for "Advanced Services." At the 5/18/22 public engagement meeting, SPD stated they use "white glove" services which entails sending the phone to the vendor and having them extract the data.[74] Public records confirm SPD utilizes these services. They show, for example, that in 2018, SPD purchased 20 "vouchers for service that unlocks, extracts, and decrypts data from cellular phones" for over $33,000."[75] Emails from Cellebrite's Advanced Services Team to an SPD detective show Cellebrite unlocked iPhones within days or weeks.[76]

In addition to data extraction capabilities, MDFTs also provide powerful analysis tools that allow law enforcement to quickly sort, search, examine, and ultimately make meaning out of the vast trove of data they now have at their fingertips. These details are also omitted from the SIR. Data analysis tools include data visualization functionalities that can, for example, show

---

[69] Ibid.
[70] Green, Matthew [matthew_d_green], "Guide to iOS estimated passcode cracking times (assumes random decimal passcode + an exploit that breaks SEP throttling): 4 digits: ~13min worst (~6.5avg) 6 digits: ~22.2hrs worst (~11.1avg) 8 digits: ~92.5days worst (~46avg) 10 digits: ~9259days worst (~4629avg)," *Twitter,* April 16, 2018, https://twitter.com/matthew_d_green/status/985885001542782978.
[71] Koepke et al., "Mass Extraction."
[72] Ibid.
[73] Ibid.
[74] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[75] Koepke et al., "Mass Extraction."
[76] Ibid.

full text conversations as a chat instead of as individual messages or create a network map using contact data in order to reveal connections and relationships.[77] Moreover, they include data searching functions like basic keyword search but also more advanced options like Cellebrite's "search by face" function that enables law enforcement to compare an image of a person's face to all the other images of faces found on the phone.[78] With Cellebrite, law enforcement can also input their own images into the software and search for similar images on the device.[79] These visualization functionalities can be applied to data from multiple phones to discern connections between people, through, for example, shared contacts, call or text correspondence, or account information.[80]

Despite the power MDFTs give SPD to broadly access people's most sensitive data, it is not clear from the SIR how often MDFTs are utilized and for what kinds of cases. The SIR cites that SPD uses these tools to investigate internet crimes against children, via their Sexual Assault and Child Abuse (SAU) Unit).[81] It further states that the Technical and Electronic Support Unit (TESU) "manages extraction tools for other SPD investigations"[82] but it is unclear what those "other" SPD investigations. An extensive report written by UpTurn on the use of MDFTs by law enforcement agencies across the country, including SPD, found that MDFTs are used as "an all-purpose investigation tool for a broad array of offenses."[83] In other words, the use of MDFTs by law enforcement is routinely used for a variety of different kinds of investigations. During their investigation, UpTurn received "hundreds of cellphone extraction request forms" as part of a public records request to SPD. ACLU-WA's analysis of SPD's logs of extractions records found that between September 19, 2016 and March 20, 2017, a six-month period, SPD attempted at least 194 extractions, 67 which were failures and 127 that were successful. This is a conservative estimate, given that these records are likely incomplete and ostensibly don't include any extractions sent to the vendor for "Advanced Services."

***Concerns with Consent Searches***

[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid.
[81] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 6.
[82] Ibid.
[83] Koepke et al., "Mass Extraction."

Relatedly, there are inadequate policies that govern and ultimately limit SPD's use of this technology. According to the SIR, MDFTs are "utilized only with the device owner's consent or pursuant to search warrant authority"[84] and these measures mitigate privacy risks, such as "concerns that data may be accessed out of scope."[85] However, there are several reasons to believe that the consent requirement is not rights protective and will not sufficiently limit the misuse of MDFTs.

Firstly, there is an inherent power imbalance between police officers and members of the public,[86] given that police are armed and act with state authority. That imbalance is arguably greater when the interaction is between police and Black people or people of color, who are disproportionately the targets of violent police practices and may feel pressure to "consent" to a phone search because of fear of being harmed by police if they do not consent.[87] In this context, "consent" is obtained under duress and is arguably coerced, not voluntary.

In addition to the power imbalance, the notion of a consent agreement is problematic because of the significant information asymmetry between police officers and members of the public about MDFTs. It is reasonable to assume that the vast majority of people have very little if any knowledge of MDFTs and their capabilities, or much if any understanding of how much of their personal, private and often sensitive data are stored on their phones and can be easily and quickly accessed via this technology. Any consent process is unlikely to adequately convey these things and fix the information deficit, especially in the absence of legal counsel. Arguably, no one can really know what they are consenting to, so truly informed, meaningful consent is not possible.

This is especially the case in situations where the device owner is a juvenile or a non-English speaker. At the 5/18/22 public engagement meeting, when asked how the consent process is different for non-English speaking people, the SPD representative stated SPD would "try to have an interpreter on site or use a language line to make sure we have informed consent."[88] This statement is troubling because it implies that it is not standard practice to provide non-English speakers a translator and a consent form in their language during the consent process. Any consent obtained without interpretation would be constitutionally invalid.

---

[84] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 3.
[85] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 15.
[86] Nadler, Janice, "No Need to Shout: Bus Sweeps and the Psychology of Coercion," *The Supreme Court Review,* vol. 2002, 2002, pp. 153-222.
[87] Strauss, "Reconstructing Consent."
[88] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

Lastly, even if consent processes provide for interpretation, consent searches are problematic because consent agreements generally do not define adequate parameters limiting the phone search, so police have huge amounts of discretion about what data they extract with MDFTs, the scope of the data they extract, and what they do with those data. For all these reasons, SPD's reliance on consent agreement to conduct phones searches with MDFTs is extremely problematic and concerning. This concern is exacerbated by SPD's heavy reliance on consent agreement to deploy MDFTs; according to UpTurn's report, "approximately one third of the phones the Seattle Police Department sought to extract data from were consent searches."[89]

Finally, it is unclear who within SPD and which entities outside SPD have access to extracted data and how those data are protected. The SIR states: "Extraction is conducted in-house and data is provided to the requesting Officer/Detective for the investigation file. TESU then purges all extracted data. No data is stored by a vendor, as the necessary tools are maintained entirely offline and on-premises."[90] Further down, the SIR states "All data extracted is stored securely within SAU—not accessible to any vendor."[91] However, this contradicts evidence, cited earlier, that SPD relies on the vendor to unlock phones they can't unlock themselves on premises. Moreover, during the 5/18/22 public engagement meeting, the SPD representative stated that has it sent devices to the King County Sheriff's Office in the past for "Chip-Off" extraction.[92] The implication then is that extraction is not always conducted in house, that extraction may be conducted by the vendor or another law enforcement agency, and therefore that vendor and the law enforcement agency have access to the data. However, the SIR does not specify the policies or practices that govern how the data extracted by the vendor are safeguarded while it is in the possession of the vendor.

### *Concerns with Data Sharing*

Moreover, the SIR states that "data obtained from the system may be shared outside SPD with other agencies, entities, or individuals within legal guidelines or as required by law."[93] The sharing of data extracted via MDFTs with law enforcement agencies outside Washington state is particularly troubling given that many states have signaled they are ready to criminalize abortions in the wake of a US Supreme Court draft leak which indicates the high court is ready to overturn Roe v. Wade. Our state remains a safe haven for people to exercise their reproductive rights and it

[89] Koepke et al., "Mass Extraction."
[90] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 6
[91] Ibid.
[92] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[93] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 12.

is anticipated that Washington will see an influx of people from neighboring states seeking abortion services here.[94] MDFTs may be used to surveil these people and it is critical that there be restrictions on the ability of SPD to share these data with law enforcement and other agencies outside the state. Moreover, for any data that are shared, there should be stringent data storage, retention and transfer/sharing safeguards in place to protect the data.

Given the lack of adequate policies described by the SIR and the number of unanswered questions that remain, we have concerns that SPD's use of MDFTs may infringe upon people's civil rights and civil liberties.

## II. *Specific Concerns*

a. **Lack of clarity about MDFT vendor names, product names, and the number of licenses SPD owns.** The SIR does not disclose vendor names, product names or the number of licenses. At the 5/18/22 public engagement meeting, the SPD representative stated that SPD would not share information about vendor names because this information "could hinder investigative efforts."[95] Without this information, it is challenging to comprehensively assess the impacts of MDFTs on privacy rights and civil liberties, as well as SPD's need for this technology.

b. **Lack of Clarity and Transparency on What Other Tech MDFTs Interface With.** The SIR does not specify which other tech, if any, SPD uses in conjunction with MDFTs. MDFTs are capable of interfacing with a host of other technologies, including ones owned by SPD such as GeoTime. GeoTime states on their website that that their technology can import data from Cellebrite software tools, which public records show SPD owns or has otherwise owned in the past. Without this information, it is difficult to adequately assess the privacy risks that MDFTs pose.

c. **Lack of Clarity on Which SPD Personnel and How Many Have Access to MDFTs and How Often They are Deployed.** The SIR does not specify how many SPD personnel

[94] Ahmed, "States Move to Restrict Abortion Access."
[95] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

are trained and certified in the use of MDFTs and/or otherwise have access to MDFTs. It also does not indicate how often MDFTs are deployed. Without this information, it is difficult to adequately assess the impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

d. **Lack of Clarity on Which SPD Personnel and How Many Have Access to Extracted Data.** The SIR states: "Only authorized SPD users can access the device or the extracted/imaged data while it resides in the extraction/imaging software" and that when the data are moved to an investigative file, access to it there is again "limited to authorized detectives and identified supervisory personnel." However, it does not specify who qualifies as an "authorized" user or detective. Therefore, it remains unclear which SPD personnel and how many have access to data that has been extracted via MDFTs.

**e. Lack of Clarity on How SPD Mitigates Potential for Inadvertent or Unauthorized Data Collection**. In response to the question of how SPD minimizes improper data collection, the SIR states, in part, that "[u]se of extraction tools is constrained by consent or court order providing the legal authority."[96] This is a vague statement that does not describe the measures SPD takes to ensure that the data extracted via MDFTs is narrowly tailored to the needs of the investigation.

f. **Legitimacy of Consent-Based Use of MDFTs and Lack of Clarity on How Consent is Obtained.** It is unlikely that consent-based use of MDFTs is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals may fear that refusing to give their consent to police will lead to deadly consequences. Additionally, the SIR does not describe the process by which officers obtain consent from witnesses or confidential informants. It is unclear if this process is standardized.

**g. Lack of Clarity on Vendor Access to Data.** According to the SPD representative at the 5/18/22 public engagement meeting,

[96] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 8.

SPD relies on vendors to extract data from devices that it cannot do itself in-house with off-the-shelf MDFT tools.[97] This is corroborated by UpTurn's extensive report on MDFTs, which examined public records from SPD. This contradicts the SIR, which states that all extraction is done in-house and that vendors do not have access to data. The implication is that vendors do have access to device data. This is extremely concerning because it increases the risk of those data being exposed or otherwise misused.

h. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share extracted data "with other agencies, entities, and individuals" outside of SPD, which presumably includes agencies from outside the state. However, it does not specify under what circumstances data would be shared or the policies and practices in place that govern data storage, retention and transfer/sharing to protect the data. It also does not indicate whether these disclosures are documented, and how.

i. **Low Threshold for MDFT Deployment.** The SIR states: "As it relates to extraction tools themselves, use is authorized, and constrained, only by consent or search warrant."[98] There is no indication there are any criteria for determining whether use of MDFTs is warranted or appropriate in the first place, despite the invasiveness of the technology and the lack of limitations on the scope of data collection via these tools. This suggests the barrier to using extraction tools is very low, even though the privacy infringement is incredibly egregious.

j. **Lack of Clarity on Safeguards in Place to Protect MDFTs and Extracted Data From Unauthorized Access.** The SIR states, regarding SAU extraction requests, that a personal password is needed to log onto the device.[99] A separate password is required to access extracted data and that same password is required to move the extracted data from the device to a portable USB.[100] No access controls are specified for TESU extraction requests or data extracted by TESU. Once data has been extracted, the MDFT can "either save the files to

[97] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[98] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 15.
[99] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 7
[100] Ibid.

removable physical storage (like a USB drive or similar media) or a computer workstation. These extracted data files are then accessed using the specialized installed software," which enable the user to examine and search the data.[101] However, the SIR does not specify what access control mechanisms are in place for accessing this software and the data on it, including whether data are encrypted. This is extremely concerning as it puts private data at risk of being improperly accessed and searched.

k. **Lack of Clarity About Data Storage, Safeguards, and Retention.** The SIR provides only a vague description of how extracted data are stored, safeguarded, and for how long they are retained. It states that "once the data has been extracted and provided to the investigating detective for inclusion in the investigation file, all data is purged from the extraction devices." This leaves out critical details about what access control mechanisms are in place to safeguard the data and how long data there are retained. The SIR also states that the data are sometimes saved to "removal physical storage (like a USB drive or similar media) or a computer workstation"[102] but it does not specify what policies and practices govern data storage, safeguards and retention on those mediums.

l. **Inadequate Data Sharing Policies.** The SIR offers only an extremely general description of who might receive device data extracted with MDFTs and how such data would be shared. Neither security protocols for transferring data nor for ensuring that shared data are properly deleted are explicated in the SIR. Indefinite retention of data and insecure sharing processes could lead to exposure of sensitive data, with manifold consequences for those whose data is collected.

m. **Lack of Clarity on Use of MDFTs to Search the Phones of Minors.** The UpTurn report on MDFTs provides evidence via public records that SPD uses MDFTs to extract data from the device of minors.[103] However, the SIR does not mention this fact. When asked at the 5/18/22 public engagement meeting

---

[101] Ibid., 5.
[102] Ibid.
[103] Citing to a King County Search Warrant, the report states that SPD "[o]fficers were looking for a juvenile who allegedly violated the terms of his electronic home monitoring. Officers eventually located the individual, and, after a 'short foot pursuit…he threw several items to the ground,' including a phone. Officers located the phone and sought to search it for evidence of escape in the second degree." Koepke et al., "Mass Extraction."

about what percentage of devices SPD extracts belong to minors, SPD claimed they don't have that data, which suggests SPD does not collect data on the demographics of the people whose phones they search. The use of MDFTs to search the phones of minors is very concerning, given that minors are a vulnerable population and are entitled under law to extra protections to safeguard their rights. Moreover, the lack of data collection on MDFT use makes it challenging, if not impossible, to detect whether there is bias in SPD practices.

**n. Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not fully explain use cases for MDFTs and does not include policies placing limits on its uses.

i. **Scope of data collection**. The SIR states that "[a] certified user within TESU conducts the extraction and provides the entirety of the data to the requesting Officer/Detective for the investigation file."[104] The SIR also states that improper data collection is limited through the consent agreement or a search warrant[105] but does not specify how these create limitations on data collection if in fact the detective is given the entire contents of a device. Arguably there are no measures that constrain or minimize inadvertent or improper data collection since virtually everything is collected.

**ii.** **Type of offense or investigation**. According to the SIR, SPD's SAU uses MDFTs to investigate internet crimes against children[106] and the TESU "manages extraction tools for other SPD investigations"[107] without elaboration on what those "other investigations" are. Furthermore, the SIR does not specify if there are limits to the type of events (e.g. First Amendment demonstrations) or offenses that SPD will investigate (e.g. petty crimes like graffiti and trespassing).

**iii.** **Tools MDFTs interface with.** The SIR does not specify any limitations on the technology that MDFTs can interface with.

---

[104] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 7.
[105] Ibid., 8
[106] Ibid., 6.
[107] Ibid.

o. **Lack of clarity about oversight.** The SIR states that both TESU and SAU "maintain logs of deployment,"[108] "all deployments of extraction tools are documented,[109], and "logs of collected information are available for audit,"[110] but it does not specify what information is collected exactly. When asked at the 5/18/22 about the last time an audit was conducted, SPD did not have a response and referred participants to OIG for an answer, strongly suggesting there has is no history of auditing. Without detailed auditing capabilities, or regular auditing, it is not possible to have sufficient oversight into how SPD uses MDFTs and whether they are complying with policy.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

a. Which vendor(s) provide SPD the extraction tools they use?
b. Which extraction tools and how many does SPD currently own?
c. How many licenses does SPD have for each MDFT product?
d. What is the cost to obtain and maintain each? What funding source(s) does SPD use to cover these costs/expenditures?
e. With what frequency/how often does SPD use extraction tools?
    a. How many times a week/for how many investigations a week is it used?
f. Besides child sexual assault and child abuse investigations, what kinds of investigations are extraction tools used for? Describe the range of investigations and what kinds of investigations they are mostly used for.
g. How often are extraction tools used in the field vs. at a unit work station? Under what circumstances are they used in the field vs. at a unit work station?
h. What does the training and certification for these extraction devices entail?
    a. How many hours of training do they receive? What does the training cover?
    b. Do they receive periodic updated training?
    c. Is there a privacy component to the training that is specific to the privacy risks of this tech? (response to 7.2 indicates no.)

[108] Ibid., 16
[109] Ibid., 8
[110] Ibid., 10

i. What does the process of obtaining consent from the phone owner look like?
    i. In what context does an officer/detective typically ask a person for consent to access their phone?
    ii. At the 5/18/22 public engagement meeting, the SPD representative indicated that a person can consult a lawyer before signing the form. Is that something the person is explicitly informed of?
    iii. Is there a script that officers/detectives follow when obtaining consent? If so, what does that script say?
    iv. What information is the phone owner provided about how their data will be extracted and what data? Is the person informed both verbally and in writing that the extraction tool will extract a full copy of data from their device—all emails, texts, photos, location, app data and more—which can then be programmatically searched?
    v. Does policy require that non-English speakers be taken through the consent process in their native language?
    vi. Does policy permit SPD to seek consent from minors to search their device with MDFTs? If so, how does that process differ, if at all, from the process used for non-minors?
j. When an officer/detective makes a request to a supervisor to use a data extraction tool, are they required by policy to articulate something they are specifically looking for?
k. What policies and practices and/or procedures limit the scope of data SPD extracts with MDFTs?
l. How does SPD safeguard the data of people on the device who are not under investigation (i.e., smart phones usually contain the private data of other people, such as location data from photos or social media pages)?
m. What policies and practices and/or procedures minimize improper or inadvertent data collection?
n. Question 4.10 of the SIR asks about safeguards in place for protecting data from unauthorized access and to provide an audit trail. SPDS's response is not very detailed or satisfactory. What safeguards are in place for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (view logging, modification logging, etc.)?
o. How are device data safeguarded when the device is sent to the vendor for extraction? How does SPD ensure that vendors

providing "Advanced Services" don't receive improper/unauthorized access to device data?

p. How often is a deployment audit performed? How often is a request audit performed? When was the last time an audit was performed for each?
q. The SIR states: "Once the data has been extracted and provided to the investigating detective for inclusion in the investigation file, all data is purged from the extraction devices." How much time is data typically stored on an extraction device before it is downloaded to the investigation file? Is it immediate? Is deletion of data on the extraction device also immediate? Is that reflected in the training?
r. What other technologies, if any, do MDFTs interface with? What policies, if any, limit the technologies that MDFTs interface with?
s. Who has access to the data on the extraction device? What constitutes an "authorized user"? How many "authorized users" within SPD have access to the data?
t. Who within SPD has access to the data once it has been downloaded out of the extraction tool? How many people have access?
u. Which agencies, entities and individuals outside of SPD can SPD share extracted data with? Are these disclosures documented? If so, where and how?
v. What data storage, retention and transfer/sharing safeguards in place to protect the data?
w. Are data obtained via extraction tools subject to the PRA?

## IV. ***Recommendations for Regulation***

Pending answers to the questions above, we can make only preliminary recommendations for regulation of Computer, Cell Phone, and Mobile Device Extraction Tools. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The use of consent searches of mobile devices must be prohibited.
- The plain view exception for digital searches must be abolished.
- There is a specific and restricted purpose of use. There should be policy defining clear limits on the use of MDFTs, including narrow parameters for: (1) data collection (2) using MDFTs in conjunction with other technology; (3) the event type or offense type that MDFTs are used for.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for licensed workstations as well as for access

to extracted data on whatever medium they exist, including removable physical storage like a portable USB drive.

- Any device data extractions must be securely shared with third parties and properly deleted.
- SPD must create and abide by robust data deletion and sealing policies.
- SPD should disclose/record to whom and under what circumstances extracted device data are shared.
- There is adequate training for all personnel who use MDFTs and that the training includes a privacy component specific to the risks inherent to using MDFTs as an investigative tool.
- There must be a detailed and direct public audit log of user actions within MDFT software, and these logs must be easy to understand. SPD must produce a publicly available annual audit report about its use of the technology.

## Camera Systems

### I. *Background*

Camera systems are a surveillance technology that enables law enforcement to monitor and record video and the sound of people's activities. SPD uses their camera systems in a "covert" manner, so that those who are the target of this surveillance (and ostensibly all others in proximity) are unaware they are being surreptitiously recorded. According to the SIR, "these covert cameras are disguised and used to record specific events related to an investigation."[111] They are either concealed on a person or hidden in or on objects.[112] The SIR states they are used by SPD to record activities "in plain view" where there is no reasonable expectation of privacy, and to record activities in a setting where a reasonable expectation of privacy exists.The SIR also indicates that SPD uses cameras "for video recording in the presence of a confidential informant or undercover officer as allowed by law." [113]

[111] Seattle Police Department, "2022 Surveillance Impact Report: Camera Systems," Accessed May 23, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Camera%20Systems.pdf.
[112] SPD, "Camera Systems," 6.
[113] Ibid.

The use of undercover or covert cameras raises serious privacy and civil liberties concerns. Research shows that law enforcement disproportionately target certain groups with camera surveillance, namely Black people, people of color, young people, and people living in poverty. One study out of Great Britain showed that Black people were surveilled at a rate one-and-a-half to two-and-a-half times higher than their representation in the public.[114] In general we expect the use of camera surveillance to track or mirror racial and socio-economic disparities in police practices more broadly,[115] so that neighborhoods that are over-policed to begin with are targeted for surveillance.[116] Covert camera systems may also be used to surveil and ultimately chill constitutionally protected First Amendment activities concerning religion, expression, and assembly. For example, the SIR explicitly mentions the use of camera systems to surveil "places of worship that have been seriously vandalized or whose congregants have been threatened."[117] Given the recent history of racialized surveillance of Muslims and mosques under the mantle of "homeland security" and "counter-terrorism,"[118] the use of this technology to potentially monitor religious minorities and their communities may chill the free exercise of religion and raise concerns about discrimination and racial profiling.

The SIR does not specify the vendor or product names of the camera systems SPD uses, nor does it provide much of any detail about the capabilities of those cameras. When asked about it at the 5/18/22 public engagement meeting, the SPD representative stated that SPD would not share information about vendor names because this information "could hinder investigative efforts."[119] Without this information, it is challenging to adequately assess all the privacy and civil liberties impacts of this technology, and SPD's need for it.

Camera systems vary widely in their complexity, interconnectivity, and capability. They may be able to tilt, pan, and/or zoom. Some capture high-

---

[114] Norris, Clive and Gary Armstrong, *CCTV and the Social Structuring of Surveillance,* Routledge, 2006, p. 162.
[115] Kasakove, "Seattle Bike Helmet Rule is Dropped Amid Racial Justice Concerns."
[116] See, for instance, Hitchcock, Ben, "You're Being Watched: Police Quietly Deploy Cameras Near Public Housing," *cvill.com,* January 15, 2020, https://www.c-ville.com/youre-being-watched-police-quietly-deploy-cameras-near-public-housing/ C-VILLE Weekly; Todd, Gracie, "Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore, November 19, 2020, https://cnsmaryland.org/2020/11/19/police-cameras-disproportionately-surveil-nonwhite-areas-of-dc-and-baltimore-cns-finds/.
[117] SPD, "Camera Systems," 5.
[118] Khan, Saher and Vignesh Ramachandran, "Post 9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear," *PBS.org,* September 16, 2021, https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear.
[119] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

definition images so even small details can be detected. They can be panoramic or otherwise wide-angle, enabling wide-area coverage with a single camera. They may also be remotely operated and/or have a feed that can be monitored. Some cameras may also record at nighttime or in low light, and may even use infrared or heat vision for dark areas where night vision is not sufficient. They may rely on motion sensors or are otherwise motion-activated. SPD's fixed location covert cameras appear to be motion-activated, since the SIR states "they are most often set to record only when motion is detected."[120] Camera systems may have audio capabilities, too. According to the SIR, SPD's covert camera systems "capture images only, not sound,[121] but it is not clear whether audio is a setting that is turned off or if the cameras do not have the capability to record sound at all. In response to a question on the SIR asking about data retention policies, SPD writes: "Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, investigational conversation recordings are retained 'for 1 year after transcribed verbatim and verified OR until disposition of pertinent case file, whichever is sooner, then Destroy" (LE06-01-04 Rev. 1)."' This appears to contradict earlier statements that audio is not recorded.

Some camera systems can be paired with other technologies, including automated license plate readers (ALPRs)[122] and facial recognition,[123] which renders the technology even more invasive. However, the SIR does not specify whether their camera systems have any of these features or otherwise interface with these other technologies.

Based on the SIR, there appear to be few barriers to SPD officers and detectives using covert camera systems, and the few hurdles that exist are very low. The Technical and Electronic Support Unit (TESU) manages, maintains, deploys and/or installs the covert camera systems that SPD uses.[124] An SPD officer or detective that wants to use a covert camera for their investigation must submit a request form to TESU that "outline[s] the equipment requested and the case number." It's noteworthy that in a different part of the SIR, it states that officers or detectives make a verbal request to the TESU and TESU personnel will complete a form for them.[125] All requests are screened by a TESU supervisor but the SIR does

---

[120] SPD, "Camera Systems," 6.
[121] Ibid.
[122] "Automated License Plate Readers," *ACLU,* Accessed May 30, 2022, https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers
[123] "Face Recognition Technology," *ACLU*, Accessed May 30, 2022, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.
[124] SPD, "Camera Systems," 7.
[125] Ibid., 8.

not specify what that screening process entails.[126] In addition to the form, to request a camera that will record in plain view, officers or detectives have only to show reasonable suspicion, which is a very low bar, ostensibly giving officers plenty of discretion to determine when, where, and against whom to deploy cameras. SPD's decisions around where to deploy cameras, for example, may reflect biases that already exist about which neighborhoods are considered "high crime" (i.e., neighborhoods that are already over-policed). It may also open the door to a fishing expedition, where officers aren't looking for anything in particular but plan to deploy cameras in the hopes of capturing criminal activity.

In general, "plain view" settings, which are an exception to the search warrant requirement under the Washington state constitution, are not defined in the SIR. SPD's characterization of plain view settings versus settings where there is a reasonable expectation privacy is vague and lacks nuance. SPD appears to use "plain view" as a proxy for "public area" without accounting for the multitude of scenarios in a public setting where there is a reasonable expectation of privacy. This raises concerns that SPD officers/detectives may be defining the plain view exception more broadly than permitted by law, especially as applied to a very intrusive technology.

To request a camera that will record in places where there is a reasonable expectation of privacy, a warrant or consent is required. The use of consent agreement in lieu of a warrant is concerning because of the power and information differential between police and members of the public, which could lead to a person consenting to the use of a camera system under duress (resulting in coerced consent).[127]

Moreover, with both consent agreements and the use of reasonable suspicion, it's unclear how the scope of data collection is narrowly tailored to the investigation (e.g. where cameras are installed, what data they collect, how long cameras are installed for, etc.) to ensure both that more data is not collected than necessary for the investigation, and that improper data collection (inadvertent or otherwise) doesn't occur (including the capture by cameras of the activities of people who are not under investigation). In general, it's unclear from the SIR how the scope of data collection is constrained in contexts where a warrant is not required. The SIR also does not specify what proportion of camera use is for plain view recording versus recording in a setting where there is a reasonable expectation of privacy, and for the latter, what proportion of cameras are deployed on the basis of a warrant versus a consent agreement.

[126] Ibid.
[127] Strauss, "Reconstructing Consent."

While the SIR lists some of the event types or investigations that camera systems may be deployed for, it does not provide a comprehensive list, nor does it specify any policies that limit use cases. Thus it's unclear whether camera systems are used for serious offenses as well as more minor/petty offenses (e.g. graffiti, trespassing). The SIR also does not specify any criteria SPD applies to determining whether hidden cameras are necessary and appropriate in the use of an investigation. A UN Office of Drugs and Crime report on the current practice of electronic surveillance for investigating serious crime provides useful guidance. Interestingly, the SIR quotes from this report to extoll the benefits of cover camera surveillance,[128] but does not mention this guidance. The report states that law enforcement's use of electronic surveillance "should not be an investigative tool of first resort" and that "its use should be considered when other less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence." In particular, this report cites to four principals or policy considerations that should inform the decision to deploy electronic surveillance (including hidden cameras): (1) the use of this form of data gathering is necessary to obtain the evidence required; (2) that there are mechanisms in place to protect the confidentiality of the information obtained, including the privacy of third parties that are not the subject of the investigation; (3) that the process of evidence gathering is overseen by a judge "or independent other of a certain requisite and specified authority"; and (4) that the privacy infringement is proportionate to the seriousness of the suspected offense and the evidence that will be collected.[129] However, none of these principles or policy considerations are reflected in the SIR as part of SPD's calculus for deploying covert cameras or limiting their use.

II. *Specific Concerns*

a. **Lack of clarity about Camera System Vendor and Product Names, and the Number of Camera Systems SPD Owns.** The SIR does not disclose vendor or product names of the camera systems it uses, or the number of camera systems it owns. At the 5/18/22 public engagement meeting, the SPD representative stated that SPD would not share information about vendor names because this information "could hinder

[128] SPD, "Camera Systems," 5.
[129] United Nations Office on Drugs and Crime, "Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime," 2009, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.

investigative efforts."[130] Without this information, it is challenging to know the capabilities of these camera systems and comprehensively assess their impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

b. **Lack of Clarity About How SPD Defines the Plain View Exception.** The SIR does not define the plain view exception to the search warrant requirement. It appears to cast plain view settings as a proxy for "public area" without explaining that even in a public area, there are situations where people have a reasonable expectation of privacy under the law. This is concerning because it suggests SPD is interpreting the plain view exception more broadly than permitted by the law, especially as applied to a very intrusive technology.

c. **Legitimacy of Consent-Based Use of Covert Camera Systems and Lack of Clarity on How Consent is Obtained.** It is unlikely that consent-based use of cover camera systems is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals may fear that refusing to give their consent to police will lead to deadly consequences. Additionally, the SIR does not describe the process by which officers obtain consent from witnesses or confidential informants. It is unclear if this process is standardized and if there is a separate consent process for confidential informants.

d. **Lack of Clarity on How Many SPD Personnel Have Access to Camera Systems and How Cameras are Secured to Prevent Unauthorized Access.** The SIR indicates that camera systems are managed and maintained by SPD personnel within TESU but does not specify how many SPD personnel are trained and certified in the use of camera systems and/or otherwise have access to them. It also does not provide information about how cameras are secured to prevent unauthorized access, especially for body-worn cameras (the ones that can be concealed on a person), which are ostensibly

[130] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

small and discrete and therefore can be surreptitiously moved around. The SIR states that "access to the systems/technology is limited to TESU personnel via password-protected login credentials" but that doesn't account for how cameras are physically secured.[131]

e. **Lack of Clarity on Safeguards in Place for Protecting Data from Unauthorized Access.** The SIR states that for fixed location cameras, data is stored directly on the device, and must be returned to TESU, which extracts the data onto a thumb drive or external hard drive and provides this copy to the requesting Officer/Detective for inclusion in the investigation file. The investigation file is kept on SPD's password-protected server which is "limited to authorized detectives and identified personnel" but does not specify who qualifies as an "authorized detective and identified personnel." Moreover, the SIR does not specify who has access to the data on the thumb drive or to the investigation file, or what the access controls are for the those. For fixed location cameras, recorded data are stored on an SPD-owned server and requesting officers or detectives must log into the server to extract the data. Similarly, the SIR does not specify who has access to the data on the server or what access control mechanisms are in place for the data. Without adequate access control mechanism, private data are at risk of being improperly accessed.

f. **Lack of Clarity About Data Storage and Retention.** The SIR provides only a vague description of how extracted data are stored and for how long they are retained. It also does not specify what policies and practices govern data storage and retention on these mediums.

g. **Lack of Clarity on How Often Cameras are Deployed**. The SIR does not indicate how often camera systems are deployed, or the proportion of camera deployments that are concealed on a person versus installed in a fixed location. It also does not provide information about what proportion of cameras installed in a setting where a reasonable expectation of privacy exists are deployed based on consent agreement versus a warrant. Without this information, it is difficult to adequately assess the

[131] SPD, "Camera Systems," 11.

impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

h. **Lack of Clarity and Transparency on What Other Tech Camera Systems Interface With.** The SIR does not specify which other tech, if any, SPD uses in conjunction with camera systems. Camera systems are capable of interfacing with a host of other technologies, such as automated license plate readers, facial recognition, or otherwise augmented with other forms of artificial intelligence.

**i. Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not explain all of the use cases for camera systems and does not include policies placing limits on its uses.

i. **Scope of data collection**. The SIR does not indicate how the scope of data collection is limited, especially in situations where the cameras are recording in plain view and all that is needed to deploy a camera system is reasonable suspicion, which is a very low bar.

**ii. Type of offense or investigation**. The SIR does not specify if there are limits to the type of events (e.g., First Amendment protected demonstrations) or offenses that SPD will investigate (e.g., petty crimes like graffiti and trespassing) using camera systems.

**iii. Tools camera systems interface with.** The SIR does not specify any limitations on the technology that camera systems can interface with.

j. **Inadequate Oversight Policies.** The SIR states that TESU maintains logs of requests (including copies of request forms and/or warrants) and extractions that are available for audit.[132] However, it is unclear if SPD has measures to prevent or detect the use of a covert camera system being used outside of the bounds of a case or legal investigation. It's also unclear how often audits on the use of camera systems are conducted and if there are any policies governing the frequency with which audits are done.

[132] Ibid., 12

k. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from covert camera systems with outside entities[133] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

a. What are the manufacturers, vendors, model names and numbers of the fixed location cameras and body cameras?
b. The SIR states: "Covert cameras may only be issued/deployed by TESU detectives. All TESU staff that deploy these cameras have received vendor training in their use." Do the SPD personnel who request to use camera systems from TESU for their investigation, and who ostensibly are involved with the camera system operation, also receive training?
c. What is the nature of the training that TESU personnel receive around camera systems?
    i. How many hours of training do they receive? What does the training cover?
    ii. Do they receive periodic updated training?
    iii. Are they provided privacy training specific to camera systems?
    iv. Is the training standardized and documented?
d. Are camera systems capable of capturing and recording audio?
e. How many fixed location cameras does SPD own? How many are currently deployed?
f. Where are fixed location cameras deployed (i.e., what neighborhoods)?
g. What is the distribution of fixed location cameras across these neighborhoods?
h. How many fixed location cameras are currently deployed in locations where there is a "reasonable expectation of privacy"?
i. Where are these deployed (e.g., what neighborhoods and blocks)?
j. What is the distribution of fixed location cameras across these neighborhoods?

[133] Ibid, 14

k. In general, where are the kinds of places that these cameras are covertly placed? Urban areas? Rural? Residential? Intersections? Etc.
l. How long are they typically deployed for? Days? Months?
m. How sophisticated are fixed location cameras? What capabilities do they have (e.g., can they zoom, pan, pivot)? Can they transmit video in real time? Is there a feed that can be monitored? Can the camera be remotely operated?
n. How many covert body-worn cameras does SPD own?
o. Are fixed location and body cameras used in conjunction with other tech?
p. What safeguards/access control mechanisms are in place to protect data stored on the SPD server, camera device, investigative file or USB drive and limit access to authorized users only?
q. What is the data retention policy for data on these various mediums?
r. What are the policies governing when data must be deleted or otherwise purged from these mediums?
s. How often are audits of covert camera use conducted? Is there a policy governing how often audits occur?
t. When was the last time a request audit and deployment audit were conducted by APRS or OIG?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of covert camera systems. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The names of the manufacturers, vendors, model names, and model numbers are publicly disclosed.
- There is a policy defining the incident types for which SPD may use covert camera systems, and how they may be used.
- Covert camera systems are only used with authorization of a court-ordered warrant.
- The following are made publicly available: The frequency with which covert camera systems are used; the average and median length of time covert camera systems are deployed; how many camera systems SPD has; and how many people have access to the camera systems.

- There must be strong access controls (authentication, authorization, logging, etc.) in place for accessing data collected via covert camera systems, regardless of the medium they are stored on.
- There is a clear data retention policy.
- SPD should disclose/record to whom and under what circumstances camera system recordings are shared.
- There is adequate and standardized training for all personnel who use covert camera systems and the training includes a privacy component specific to the risks inherent to using covert camera systems as an investigative tool.
- There must be a detailed direct audit log of user actions with covert camera systems and SPD must produce a publicly available annual audit report about its use of the technology.

## Tracking Devices

### I. *Background*

Tracking devices are location-tracking tools that allow SPD to track vehicles electronically via interconnected hardware and software. Physical tracking devices are placed on or in a targeted vehicle and they report latitude and longitude coordinates on a pre-determined schedule that can be adjusted by users remotely. SPD uses a connected online portal that collects the information captured by the tracking device to map the locations and movement of vehicles.

Tracking devices raise serious privacy and civil liberties concerns because they can be used to comprehensively track and plot the movements of individual cars over time. These devices can be used to target individuals who visit sensitive places such as places of religious worship, protests, union halls, immigration clinics, or health centers. While SPD states that it uses tracking devices only with a warrant or after obtaining consent, data collected via these devices may be combined with other SPD data and analyzed with other invasive tools used by SPD such as GeoTime or IBM i2 iBase that can create very detailed, personalized maps and analyses of people's lives—even if they are not involved in a crime or an event being investigated.

Additionally, we have concerns about whether consent-based tracking is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law

enforcement, and as noted by one scholar, "many African Americans, and undoubtedly other people of color, know that refusing to accede to the authority of the police, and even seemingly polite requests—can have deadly consequences."[134]

## II. *Specific Concerns*

a. **Lack of Information on What Specific Tracking Devices are Used.** The public has not been provided the names of the manufacturers and the specific model numbers and names of the tracking devices used by SPD. Without this information, it is difficult, if not impossible to meaningfully review all the functions and capabilities of the tools in use and provide recommendations on how each tool should be regulated.

b. **Lack of Clarity on Usage Limitations and Types of Incidents for Which Tracking Devices are Used.** While the SIR states that officers/detectives will provide written consent and/or a court approved warrant for all vehicle-tracking technology deployments, it does not describe the incident types for which tracking devices are used. Especially with consent-based uses of tracking devices, it is unclear from the SIR how the use of tracking devices is constrained (whereas a judicial warrant would articulate formal parameters around data collection, such as time frame). Additionally, it is unclear whether SPD has a policy limiting the use of geolocation trackers to vehicles.

c. **Legitimacy of Consent-Based Tracking and Lack of Clarity on How and From Whom Consent is Obtained.** It is unlikely that consent-based tracking is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals

[134] "Given this sad history, it can be presumed that at least for some persons of color, any police request for consent to search will be viewed as an unequivocal demand to search that is disobeyed or challenged only at significant risk of bodily harm." Strauss, Marcy, "Reconstructing Consent." *Journal of Criminal Law and Criminology*, vol. 92, no. 1, 2001, pp. 242-243.

may fear that refusing to give their consent to police will lead to deadly consequences. Additionally, the SIR does not describe the process by which officers obtain consent from witnesses or confidential informants. It is also unclear from whom consent is being sought—the vehicle owner, driver, and/or passengers. Lastly, it is unclear if this process is standardized.

d. **Lack of Clarity About Data Storage, Safeguards, and Retention.** It is unclear whether the data collected via the physical tracking devices ever leaves SPD-owned equipment. The SIR states that "data is securely stored by the vehicle tracking technology vendor and will be transferred to the case investigator only via Seattle Police Department owned and authorized technology. At that time, vehicle tracking data collected by the tracking device is downloaded from the vendor software and resides only with the investigation file."[135] It is unclear if the data is within the SPD network on-premises or if it flows to a vendor providing Software-as-a-Service. Additionally, the SIR does not state if any data retention policy exists. The SIR states that SPD deletes tracking device data from the software and hardware after the conclusion of a tracking schedule, but it does not state how long the data are kept after being moved to an investigation file.

e. **Lack of Clarity on if TESU Personnel Training is Standardized and Documented.** The SIR states, "TESU personnel are trained by the vendor in the use of the hardware and software. When an Officer/Detective requests and deploys a tracking device from TESU, TESU personnel train the Officer/Detective in the tracker's use." It is unclear how the vendor trains the TESU personnel and how consistency in this training is ensured.

f. **Lack of Clarity on Which SPD Personnel/Units and How Many Have Access to Tracking Devices.** The SIR states "Only authorized SPD users can access the vehicle tracking devices or the data while it resides in the system," that "only SPD personnel involved in the investigation have

[135] Seattle Police Department, "2022 Surveillance Impact Report: Tracking Devices," Accessed May 23, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Tracking%20Devices.pdf, 9.

access to this information, and "[o]nly Technical and Electronic Support Unit personnel have access to vehicle tracking equipment and services" but it is unclear which units and how many people in total have access to the tracking devices.

g. **Lack of Clarity on Frequency of Usage of Tracking Devices.** It is unclear how many cases per year use tracking devices, how many deployments there are per year, and the average and median length of time tracking devices are deployed.

h. **Inadequate Oversight Policies.** The SIR states that no formal audits exist for tracking device deployments. It is unclear if SPD has measures to prevent or detect the use of a tracking device being used outside of the confines of a case or legal investigation.

i. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from tracking devices with outside entities[136] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

a. What are the manufacturers, vendors, model numbers, and model names of the tracking devices in use by SPD?
b. Is there any policy defining the incident types for which SPD may use tracking devices?
c. What is the process of getting consent?
d. Is the "online portal" hosted within the SPD network on-premise, or is it hosted on the vendor's website?
e. Does the data collected via the tracking device ever leave SPD-owned equipment
f. Are the trackers placed anywhere other than a vehicle?
g. Is the TESU personnel training standardized and documented?

[136] Ibid., 10

h. What is the retention period for data collected by tracking devices?
i. How many cases per year use tracking devices?
j. How many deployments of tracking devices are there per year?
k. How long is the average and median length of time tracking devices are deployed?
l. How many tracking devices does SPD have?
m. How many people have access to SPD's location tracking devices?
n. How many times has SPD deployed a tracking device on a vehicle either not owned by the suspect or owned by the suspect but also frequently used by other individuals?
o. Are there measures in place that would prevent or detect the use of a tracking device outside the confines of a case or legal investigation?
p. Have there been any audits of SPD's use of tracking devices? If so, when was the last audit and where can that audit report be found?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of tracking devices. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The names of the manufacturers, vendors, model names, and model numbers are publicly disclosed.
- There is a policy defining the incident types for which SPD may use tracking devices, and how they may be used.
- Tracking devices are only used with authorization of a court-ordered warrant.
- Data collected via the tracking device never leaves SPD-owned equipment.
- The following are made publicly available: The frequency with which tracking devices are used; the average and median length of time tracking devices are deployed; how many tracking devices SPD has; and how many people have access to the tracking devices.
- There must be strong access controls (authentication, authorization, logging, etc.) in place tracking devices.
- There is a clear data retention policy.
- SPD must disclose/record to whom and under what circumstances tracking device data are shared with third parties.

- There is adequate and standardized training for all personnel who use tracking devices and the training includes a privacy component specific to the risks inherent to using tracking devices as an investigative tool.
- There must be a detailed direct audit log of user actions with tracking devices and SPD must produce a publicly available annual audit report about its use of the technology.
- There must be measures in place to validate the accuracy of the data collected by tracking devices.

## Remotely Operated Vehicles

### I. *Background*

Remotely Operated Vehicles (ROVs) are unarmed remote controlled vehicles with mounted cameras. Three SPD units use ROVs: SWAT, Arson/Bomb, and Harbor. These units use ROVs to access areas that are potentially dangerous for personnel to physically enter. The ROVs operated by the SWAT and Arson/Bomb units are wheeled vehicles while the ROV operated by the Harbor unit are designed as submersible underwater vehicles.

There are 14 ROVs used in total.

- The SWAT unit has 7 ROVs. Two are manufactured by Robotex, four are manufactured by Recon Robotics, and one is manufactured by Tactical Electronics.
- The Arson/Bomb unit has 5 ROVs. They are manufactured by TeleRob, Andros, ICOR, Talon, and PointMan. Each of these ROVs has a camera which transmits back to the handheld control unit.
- The SPD Harbor unit has 2 submersible ROV units. One unit is manufactured by Deep Ocean Engineering and has onboard video and sonar recording capability. The other ROV is manufactured by Seabotix and has onboard video and sonar recording capability as well as two interchangeable remotely controlled articulated arms.

ROVs pose privacy and civil liberties concerns because they may be used to surveil members of the public via cameras and may be used to carry weapons and deliver lethal force. In 2016, Dallas police officers used a bomb disposal remote control vehicle armed with explosives to kill a

man.[137] Given that SPD's ROVs are equipped with cameras and remotely controlled arms, these technologies have the potential to cause serious harm to members of the public.

## II. *Specific Concerns*

a. **Lack of Clarity on Usage Limits.** While the SIR explains some use cases for ROVs, it does not include specific policies placing limits on its uses. For example, the SIR does not describe any policies in place prohibiting the use of ROVs to surveil members of the public or to carry or deploy weapons.
b. **Lack of Clarity on if There are Auditable Logs of the Deployment of ROVs.** The SIR does not clearly answer what processes are required prior to each use or access to ROVs, such as a notification, or check-in, or check-out of the equipment. The SIR only states, "Authorized members of the SPD SWAT, Arson/Bomb, and Harbor units are given training in the appropriate use and application of these ROVs."[138] Lack of a check-in/check-out procedure is concerning because there may be no logs that could be audited of the deployment of the ROVs.
c. **Lack of Clarity on the Number of Cases for Which ROVs are Used.** The SIR does not make clear for how many cases per year the SWAT, Arson/Bomb, and Harbor units use ROVs, and the average and median length of time ROVs are deployed.
d. **Lack of Clarity on Whether SPD has Ever Used ROVs to Deploy Weapons.** Some ROVs can support recoilless disrupters that can shoot diverse types of projectiles which are intended to remotely disable an improved explosive device (IED), i.e., a bomb However, some ROVs, such as the SWORDS TALON ROV, support a diverse range of weapons.[139] A 12-gauge shotgun can also be mounted onto

---

[137] Sidner, Sara and Mallory Simon, "How Robot, Explosives Took Out Dallas Sniper in Unprecedented Way," *CNN*, https://www.cnn.com/2016/07/12/us/dallas-police-robot-c4-explosives/index.html.
[138] Seattle Police Department, "2022 Surveillance Impact Report: Remoted Operated Vehicles (ROVs)," Accessed May 30, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20ROVs.pdf, p. 6.
[139] Qinetiq, "Multi-Mission Explosive Ordnance Disposal Robot," https://www.qinetiq.com/en/what-we-do/services-and-products/talon-medium-sized-tactical-robot

the Pointman ROV.[140] The purpose of mounting weapons onto ROVs would be to harm or kill humans—not to disable an IED. SPD uses both TALON and Pointman ROVs and it is unclear whether SPD has ever used ROVs to deploy weapons or if SPD has a policy prohibiting the use of weapons with ROVs.

e. **Inadequate Data Storage, Safeguards, and Retention.** The SIR states that Harbor unit personnel delete the data on the hard drives inside the ROV only periodically when the software informs the users that it is nearing capacity.[141] It is unclear why there is no policy requiring the deletion of recorded data from the Harbor unit's ROVs when a deployment is finished. It is also unclear whether the statement that no images or data are stored or retained by ROVs used by SWAT and Arson/Bomb units also applies to SPD-provided cell phones, personal cell phones, or remote controllers and tablets that may also support recording data.

f. **Lack of Clarity on if ROV Training is Standardized and Documented.** The SIR states, "Authorized members of for the SPD SWAT, Arson/Bomb, and Harbor units are given training in the appropriate use and application of these ROVs. Unit commanders are responsible to ensure usage of the technology falls within the appropriate usage."[142] It is unclear if there is a standardized and documented training process.

g. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from ROVs with outside entities[143] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

- Is there any policy defining usage limits for SPD's use of ROVs?
- Is there a procedure for SPD personnel to get access to the ROVs?

---

[140] i-HLS, "Pointman Tactical Robot, Surveillance Systems Assist Law Enforcement in Urban, Security Ops," *Defense Update,* 2013, Accessed June 1, 2022, https://defense-update.com/20130504_new-tools-for-border-security.html

[141] SPD, "ROVs," 8.

[142] SPD, "ROVs," 6.

[143] SPD, "ROVs," 10.

- Is there an auditable log of the deployment of ROVs?
- For how many cases per year does the SWAT unit use ROVs?
- For how many cases per year does the Arson/Bomb unit use ROVs?
- For how many cases per year does the Harbor unit use ROVs?
- Is the training for members of the SPD SWAT, Arson/Bomb, and Harbor units standardized?
- Is there a policy requiring the deletion of recorded data from the Harbor unit's ROVs when a deployment is finished?
- Is there a policy prohibiting SPD personnel from recording data using SPD-provided cell phones or personal cell phones, or remote controllers or tablets that may be connected to the ROVs wirelessly?
- Has SPD ever used an ROV with weapons or for lethal force?
- Have there been any audits of SPD's use of ROVs? If so, when was the last audit and where can that audit report be found?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of ROVs. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- There is a policy defining the incident types for which SPD may use ROVs, how they may be used, and what the usage limits are.
- A court ordered warrant is required to use ROV to surveil any members of the public.There is a prohibition on the use of ROVs to deploy weapons.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for ROVs.
- Any data collected via ROVs that is not needed for an investigation is deleted immediately.
- Data collected via ROVs never leaves SPD-owned equipment.
- The following are made publicly available: The frequency with which ROVs are used; the average and median length of time ROVs are deployed; and how many people have access to the tracking devices.
- SPD must disclose/record to whom and under what circumstances ROV data are shared with third parties.
- There is adequate and standardized training for all personnel who use ROVs and the training includes a privacy component specific to the risks inherent to using ROVs as an investigative tool.

- There must be a detailed direct audit log of user actions with ROVs and SPD must produce a publicly available annual audit report about its use of the technology.

## Crash Data Retrieval

### I. *Background*

Crash Data Retrieval (CDR) tools are used to reconstruct traffic collisions by connecting to a vehicle's Event Data Recorder (EDR) and translating the raw EDR data to a PDF format readable report. Nearly all passenger vehicles sold in the US since 2013 have an onboard EDR, which automatically records technical information during a critical event such as a collision. While the type of data collected by an EDR varies by manufacturer, the types of data that are recorded include GPS, throttle, brake pedal position, steering angle, and speed. After airbags are deployed, these data are saved permanently and can only be accessed through the vehicle's onboard diagnostics port.

CDR tools pose privacy and civil liberties concerns because EDRs can be used to track people's locations and record other sensitive information without their knowledge. In 2011, OnStar, a company that uses EDRs to track vehicle location and other operational data, changed it user contract terminology without notifying customers, in order to track people's driving habits and sell the information to third parties.[144] While the policy was eventually reversed due to public pressure, entities such as auto insurance companies may use increasingly powerful tracking systems to monitor policyholders, and that data may be accessed by law enforcement.

The SIR's lack of clarity on SPD's policies and the specific CDR tools in use raises concerns about SPD's use of this technology.

### II. *Specific Concerns*

a. **Lack of Information on What Specific CDR tools are Used.** The SIR does not provide the names of the manufacturers and the specific model numbers and names of the CDRs used by SPD. Without this information, it is difficult, if not impossible, to meaningfully review all the

[144] David Kravets, "OnStar Tracks Your Car Even When You Cancel Service," *Wired,* 2011, Accessed June 1, 2022, https://www.wired.com/2011/09/onstar-tracks-you/

functions and capabilities of the tools in use and provide recommendations on how each tool should be regulated.

b. **Lack of Clarity on Usage Limits.** While the SIR explains the general use case for CDR tools, it does not describe if SPD seeks to use CDR tools to gather EDR data every time an accident occurs, regardless of whether a citation has been issued or a crime has occurred.
c. **Lack of Clarity on the Breadth of Warrants to Collect Vehicle Data.** It is unclear if the warrants used by SPD specify that only EDR data are collected or if these warrants permit SPD to extract any data from the vehicle, including information from a car's system such as phone contacts and location history from past trip navigations.
d. **Lack of Clarity on if There are Audits on the Deployment of CDR Tools.** It is unclear if SPD has logs of CDR use and if there has been an audit of SPD's usage of CDR tools.
e. **Lack of Clarity on the Number of Cases for Which CDR Tools are Used.** The SIR does not make clear for how many cases per year CDR tools are used, and the average and median length of time CDR tools are deployed.
f. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from CDR tools with outside entities[145] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

h. What are the manufacturers, vendors, model numbers, and model names of the CDR tools in use by SPD?
i. Is there any policy defining usage limits for SPD's use of CDR tools?
j. Are the warrants to get access to vehicle data after a crash limited to EDR data?
k. Are the audits on SPDs use of CDR tools?
l. For how many cases per year does SPD use CDR tools?

[145] Seattle Police Department, "2022 Surveillance Impact Report: Crash Data Retrieval Tool," Accessed May 30, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20%20Crash%20Data%20Retrieval.pdf, 9.

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of CDR tools. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The names of the manufacturers, vendors, model names, and model numbers are publicly disclosed.
- There is a policy defining the incident types for which SPD may use CDR tools, how they may be used, and what the usage limits are.
- There is policy requiring warrants sought for CDR use are narrowly tailored to only extract EDR data, and no other data from the vehicle.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for CDR data.
- The following are made publicly available: The frequency with which CDR tools are used; the average and median length of time CDR tools are deployed; and how many people have access to the CDR tools.
- SPD must disclose/record to whom and under what circumstances CDR data are shared with third parties.
- There must be a detailed direct audit log of user actions with CDR tools and SPD must produce a publicly available annual audit report about its use of the technology.

Sincerely,

Jennifer Lee
Technology and Liberty Project Manager

Mina Barahimi Martin
Policy Analyst