Upturn
Toward Justice in Technology

June 02, 2022

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

RE: Upturn's Comments on "Computer, cellphone and mobile device extraction tools" in Group 4b Surveillance Technologies

On behalf of Upturn, I write to offer our comments on one technology included in Group 4b of the Seattle Surveillance Ordinance implementation process.

Upturn is a nonprofit organization based in Washington, D.C. that works in partnership with many of the nation's leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of technology. One of Upturn's priorities is to ensure that technology does not exacerbate or entrench mass incarceration and racial inequity in the criminal legal system.

We write to comment specifically on Seattle Police Department's (SPD) use of mobile device forensic tools (MDFTs) — tools that allow police to extract and search a cellphone for every text, photo, piece of location data, online search history, and more.[1] In 2020, Upturn published *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (attached). Based on more than 110 public records requests, more than 12,000 pages of documents, and more than two years of research, this report is the most comprehensive examination of law enforcement's use of mobile device forensic tools to date.[2] Among the report's findings is that more than 2,000 law enforcement agencies have

[1] Under Group 4b the Seattle Surveillance Ordinance process describes these tools as "Computer, cellphone and mobile device extraction tools." We use the terminology "mobile device forensic tools" as we believe it is most technically accurate — regardless, this is the same technology that the Seattle Police Department uses.

[2] Our records requests asked law enforcement agencies for three common records: purchase records, records of use (describing in what cases and how often law enforcement agencies use mobile device forensic tools), and policies governing use. We supplemented our research through publicly available reporting; various open databases from city, county, and state governments; federal grantmaking databases; and GovSpend, a database of government contracts and purchase orders. In order to assess the technical capabilities of current mobile device forensic tools, we examined technical manuals, software release notes, marketing materials, webinars, and digital forensics blog posts and forums. We also visited the office of one of the few public defenders in the US with these forensic tools (and forensic staff) in-house.

purchased these tools in all 50 states and the District of Columbia. State and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant. Few departments have detailed policies governing when and how officers can use this technology. The report also documents the existing technical capabilities of today's mobile device forensic tools, finding that the tools provide sweeping access to personal information on a phone. *Mass Extraction* documents a dangerous expansion in law enforcement's investigatory power.

In these comments, we highlight four issues with law enforcement use of mobile device forensic tools. We believe that MDFTs are simply too powerful in the hands of law enforcement and should not be used. Recognizing that MDFTs are already in widespread use across the country, we conclude with recommendations that we believe can, in the short term, reduce the use and harm of MDFTs.

1. Mobile device forensic tools are designed to be invasive. They are a dangerous expansion of law enforcement's investigatory power.

Every day, law enforcement agencies across the country search thousands of cellphones using MDFTs. MDFTs are a powerful technology that allows police to extract a full copy of data from a cellphone — all emails, texts, photos, location data, app data, and more — which can then be programmatically searched. As one expert puts it, with the amount of sensitive information stored on smartphones today, the tools provide a "window into the soul."[3]

Mobile device forensics is typically a two-step process: data extraction, then analysis. MDFTs help law enforcement accomplish both. An MDFT is a computer program and its supplemental equipment (*e.g.*, cables and external storage) that can copy and analyze data from a cellphone or other mobile device. The software can run on a regular desktop computer, or on a dedicated device like a tablet or a "kiosk" computer. These tools are sold by a range of companies, including Cellebrite, Grayshift, MSAB, Magnet Forensics, OpenText (formerly Guidance Software), Oxygen Forensics, and AccessData.

[3] C.M. "Mike" Adams, "Digital Forensics: Window Into the Soul," Forensic, June 10, 2019, *available at* https://www.forensicmag.com/518341-Digital-Forensics-Window-Into-the-Soul/.

According to records obtained from Seattle's Police Department, SPD has spent *at least* $240,000 on MDFTs from vendors including Cellebrite, MSAB, Magnet Forensics, and Grayshift.[4]

Modern cellphones are a convenient combination of many tools: they're phones, cameras, notebooks, diaries, navigation devices, web browsers, and more. Smartphones centralize patterns of life on a single device with seemingly endless storage. There has never been an easier, more centralized way to access troves of personal data about individuals. MDFTs allow law enforcement to access all of this data and more, often without individuals understanding how much information they are handing over.

Our technical analysis of how MDFTs work and their capabilities surfaces three key points:

1. **MDFTs are designed to copy all of the data commonly found on a cellphone.** Mobile device forensic tools are designed to extract the maximum amount of information possible. This includes data like contacts, photos, videos, saved passwords, GPS records, phone usage records, and even "deleted" data. A "logical extraction" of the phone extracts data as it is presented on the phone to the user, while a "physical extraction" of the phone allows for law enforcement to download data bit by bit from the phone, offering more information to be later reconstructed and analyzed.

2. **MDFTs make it easy for law enforcement to analyze and search data copied from phones.** A range of features help law enforcement quickly sift through gigabytes of data — a task that would otherwise require significantly more labor. MDFTs can chronologically sort all information on the phone, use location data to show every single place a person has been on a map, and use face recognition to search every image on the phone for a specific person. The tools allow for keyword searches of all data, sorting by file type regardless of its location on the phone (*e.g.*, all of the images on a phone, regardless where they came from) and even create networked graphs to show social relationships.

3. **MDFTs can circumvent most security features in order to copy data.** MDFTs exploit the security vulnerabilities or design flaws present in a wide range of

[4] This number comes from public records requests and is listed in the Appendix of *Mass Extraction*. https://www.upturn.org/work/mass-extraction/#. This total is an undercount, given that our public records project concluded in 2020 and SPD has likely renewed MDFT licenses and purchased new MDFTs in 2020, 2021, and 2022.

phones. Even in instances where full forensic access is difficult due to security features like strong password protection, mobile device forensic tools can often still extract meaningful data from phones. MDFTs take advantage of the fact that, in order to balance convenience and security, phones don't actually encrypt all data on a device. When all else fails, vendors offer "advanced services" in which the phone is sent to a vendor's lab for intensive unlocking attempts.

In 2018, the Seattle PD purchased 20 such "actions" for $33,000,[5] and email records show them using Cellebrite to unlock various iPhones within days or weeks.[6] For example, SPD sent Cellebrite an iPhone X with an unknown 6-digit passcode in August 2018: Cellebrite received it on August 24, began processing on August 28, finished processing on September 12, and shipped it back the same day. Cellebrite Premium allows law enforcement to bring these advanced unlocking capabilities in-house for $75,000 to $150,000, based on the frequency of use.[7]

Ultimately, MDFTs offer law enforcement a powerful window into almost all data stored on — or accessible from — a cellphone, including substantial amounts of data that regular users cannot see. Data extracted by an MDFT can be stored indefinitely and repeatedly searched. This would be like allowing law enforcement to repeatedly and indefinitely search a person's home, without that person knowing. MDFTs provide sweeping access to personal information on a phone, enabling "an extent of surveillance that in earlier times would have been prohibitively expensive."[8] In many circumstances, this access can be disproportionately invasive compared to the scope of evidence being sought and poses an alarming challenge to existing Fourth Amendment protections.

2. MDFTs are used as a general purpose investigative tool, even when the offense has no digital component.

The emergence of MDFTs represents a dangerous expansion in law enforcement's investigatory powers. In 2011, only 35% of Americans owned a smartphone.[9] Today, it's at

[5] *See* Seattle Police Department Purchase & Supply Request, https://beta.documentcloud.org/documents/20394507-installment_101.
[6] *See* Seattle Police Department, Cellebrite Advanced Services emails, https://beta.documentcloud.org/documents/20394508-installment_51.
[7] Cellebrite, "Premium access to all iOS and high-end Android devices," *available at* https://cf-media.cellebrite.com/wp-content/uploads/2020/07/ProductOverview_CellebritePremium.pdf.
[8] *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007).
[9] Pew Research Center, "Mobile Fact Sheet," June 12, 2019, *available at* https://www.pewresearch.org/internet/fact-sheet/ mobile/.

least 81% of Americans.[10] Moreover, many Americans — especially people of color and people with lower incomes — rely solely on their cellphones to connect to the internet.[11] For law enforcement, "[m]obile phones remain the most frequently used and most important digital source for investigation."[12] Seattle PD remarked in their own impact assessment that roughly 63% of investigations include digital evidence as part of the investigation.[13] While that percentage may seem high, if anything, it is a significant undercount of how often law enforcement agencies use MDFTs.

The records we've obtained demonstrate that law enforcement agencies use MDFTs as an all-purpose investigative tool for a broad and growing array of offenses. Law enforcement use MDFTs to investigate not only cases involving major harm, but also for graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses. Through our public records request, we received documentation from SPD that they conduct phone searches for offenses spanning from murder to robbery, violation of pretrial conditions of release, gun possession, and drug charges. This contradicts SPD's own claim that these tools are used for "collecting evidence related to serious and/or violent criminal activity."[14] Given how routine these searches are today, together with racist policing policies and practices, it's likely that these technologies disparately affect and are used against communities of color.

3. There are virtually no policies in place governing the use of these powerful tools.

In response to our records request, SPD did not provide us with any specific policies governing the use of MDFTs. Instead, SPD only provided general policies on searches, search warrants, and an irrelevant policy on locating a cellphone during an emergency. SPD's impact assessment only states that officers rely on warrants or consent for searches,

---

[10] *Id.* (Noting 96% own a cellphone of some kind.)
[11] Camille Ryan, U.S. Department of Commerce, Economics and Statistics Administration, U.S. Census Bureau, "Computer and Internet Use in the United States: 2016," American Community Survey Reports, August 2018; Jamie M. Lewis, *Handheld Device Ownership: Reducing the Digital Divide?*, March 2017, https://www.census.gov/library/working-papers/2017/ demo/SEHSD-WP2017-04.html.
[12] Cellebrite Annual Industry Trend Survey 2019: Law Enforcement, at 3.
[13] 2022 Surveillance Impact Report — Computer, Cellphone, and Mobile Device Extraction Tools, Seattle Police Department, at 4, *available at* https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Computer%2C%20Cellphone%2C%20%26%20Mobile%20Device%20Extraction%20Tools.pdf
[14] *Id.*, 5.

and does not describe any other policies to safeguard people's rights.[15] Indeed, SPD says that "[a]s it relates to extraction tools themselves, use is authorized, and constrained, only by consent or search warrant."[16] Section 4 of this testimony will describe in greater detail the profound limitations of consent and search warrants as measures to "safeguard people's rights."

As described in these comments already, MDFTs are some of the most powerful tools at law enforcement's disposal; and based on the available evidence, SPD has no policy to monitor, track, control, oversee, or even attempt to account for their use of these tools. This surveillance technology oversight process is an opportunity for the council to remedy this. Council must act to curb SPD's use of these tools and to protect the rights of Seattle residents.

Policies governing MDFTs should have specific requirements for how law enforcement write warrants and search phones, in order to guard against overbroad searches that violate peoples' rights. The Fourth Amendment requires warrants to describe with particularity the places to be searched and the things to be seized. This "particularity requirement" was designed to protect against "general warrants," such that law enforcement could not indiscriminately rummage through a person's property. While police departments' policies obtained by Upturn acknowledge the need to have a sound legal basis to search a phone (via consent or search warrant), few provide more clarity or direction beyond this general acknowledgement. When law enforcement downloads an entire copy of a person's phone, they violate the particularity requirement and leave individuals vulnerable to overbroad searches of their private activities, communications, and thoughts.[17]

In order for a cellphone search warrant to abide by the requirements of the Fourth Amendment, it must, at a minimum:

- Specify the particular items of evidence to be searched and seized from the phone;
- Ensure that the nexus between each category of information on a cellphone — such as texts, photographs, or emails — and the alleged criminal activity is specific and clear (cellphone search warrants must be based on more than the fact that a defendant possesses a phone);

[15] *Id.*
[16] *Id.*, 15.
[17] See an extended discussion of this in Section 4.

- Strictly limit search authorization to the narrowest time period for which probable cause has been properly established;
- Strictly prohibit a search of "any and all data," or of a laundry list of data on a phone; and
- Forswear reliance upon the plain view exception and general statements that say because digital data might possibly be disguised or manipulated, law enforcement must be able to search the entirety of a cellphone.

A specific cellphone search warrant policy should ideally describe these minimum features.

Further, SPD's current policies have no clear limits on data retention, or how that data may be used beyond the scope of an immediate investigation. Unlike a physical search of someone's home, once a copy of a person's phone has been downloaded, law enforcement can hold onto and repeatedly search that copy forever. Absent specific policies or laws that require notifying someone that their phone has been searched, it would be impossible for those under investigation to know of — let alone challenge — situations where law enforcement continues to rifle through previously extracted data for new or unrelated investigations.

Additionally, without specific prohibitions, law enforcement could copy data from someone's phone — say, their contact list — and add that information into a far-reaching police surveillance database that may harm an individual and their contacts for years to come. SPD might share information with other law enforcement agencies in the King County area, the state of Washington, or with other states and the federal government.[18] Law enforcement should also not be able to indiscriminately use cloud data extraction tools, which can access information that is not locally stored on the phone (SPD also has no policies for these tools).

There are a handful of state laws that do prescribe evidence retention periods specifically for digital evidence obtained from cellphones. For example, New Mexico's recently enacted Electronic Communications Privacy Act requires that "any information obtained through the execution of the warrant that is unrelated to the objective of the warrant be destroyed within thirty days after the information is seized and be not subject to further review, use

[18] The Wisconsin Supreme Court recently held that cellphone evidence obtained from a consent search in one jurisdiction can be shared with other law enforcement agencies pursuing unrelated investigations, without needing new legal authorization. *See State v. Burch*, 2021 WI 68, 961 N.W.2d 314 (Wis. 2021).

or disclosure."[19] The City of Seattle, too, should adopt meaningful limitations on retention of digital evidence.

4. Law enforcement regularly use MDFTs without a warrant — but even with warrants, little is done to minimize the harm of invasive searches.

In 2014, the Supreme Court held in *Riley v. California* that in order to search a cellphone, police must get a warrant.[20] However, courts have long held that "consent searches" are an exception to the Fourth Amendment's warrant requirement. Records Upturn obtained show that, for some agencies, law enforcement regularly rely on a person's consent as the legal basis to search cellphones. For the cellphone searches SPD documented and conducted between 2017 and 2019, one-third were consent searches.

However, "consent searches" are inherently coercive. Due to power and knowledge imbalances between residents and law enforcement, there is enormous disincentive to refuse to give consent, and it is much worse for people of color who are under threat of police violence. In fact, many states ban consent searches at traffic stops, and California[21] and New Jersey[22] have banned consent searches for minors, in order to address this racialized power imbalance. A recent study designed "specifically to examine the psychology of consent searches" highlights the problems in relying on a so-called "reasonable person" to adjudicate the lawfulness of consent searches.[23] Participants were brought into a laboratory and presented with a "highly invasive request: to allow an experimenter unsupervised access to their unlocked smartphone."[24] More than 97% of participants handed their phone over to be searched when requested — even though only

---

[19] *See* https://nmlegis.gov/Sessions/19%20Regular/final/SB0199.pdf. Similarly, California's Electronic Communications Privacy Act allows judges to, at their discretion, "require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings." *See* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.
[20] *Riley v. California*, 573 U.S. 373 (2014).
[21] *See* John M. Broder, "California Ending Use of Minor Traffic Stops as Search Pretext," New York Times, Feb. 28, 2003, *available at* https://www.nytimes.com/2003/02/28/us/california-ending-use-of-minor-traffic-stops-as-search-pretext.html *and* California Senate Bill 203. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB203
[22] *See* Routine Automobile Consent Searches are Illegal in New Jersey. https://www.lsnjlaw.org/Criminal-Charges-and-Convictions/Motor-Vehicle-Laws/Pages/Ban-Routine-Automobile-Consent-Searches.aspx
[23] Roseanna Sommers, Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L. J. 1962 (2019).
[24] *Id.*, 1980.

14.1% of a separate group of observers said that a "reasonable person" would hand over their phone in such a situation.[25] This study reveals that there is a profound, "systematic bias whereby neutral third parties view consent as more voluntary, and refusal easier, than actors experience it to be."[26]

Additionally, MDFTs are not well understood by the public, and they are able to extract much more data than most people would assume. Many people may give consent to police to see their text messages or another specific category of data with the assumption that police will simply look at the phone manually, while police actually perform full extractions using MDFTs and retain data indefinitely. Consent searches of cellphones are especially egregious as people do not know the extent of the information they are giving away, and how that information will be searched and retained.

Warrants are not much better. As part of Upturn's public records research, we obtained and studied hundreds of search warrants that authorized law enforcement to search cellphones using MDFTs. Many of these warrants authorized a search of "any and all data" on a cellphone. Others authorized a search of a laundry list of effectively every type of data one could plausibly find on a cellphone. Others authorized a "full extensive download and/or search of the [phone] to include all compartments, and items within the electronic devices that may contain contraband or evidence of the crime, and the data stored within said devices." Still others authorized a search of a cellphone for "evidence related to this [narcotics offense] and other criminal offenses." And for many, regardless of the precise words used, the nexus between a phone's data and the alleged offense was tenuous. Repeatedly, across the country, we saw search warrants that authorized an unlimited, unrestricted search of a cellphone.

Relatedly, few policies provide guidance on what examiners should do if they encounter potential evidence of another crime that is not detailed in the initial search warrant. Using a search warrant to look for digital evidence of one potential crime, only to then search for digital evidence of a different crime is unconstitutional. Without clear and enforced guidance, law enforcement could go on a "fishing expedition" in search of evidence of any crime, far beyond the original justification for a search. We observed only two policies that provided any guidance on this point.[27]

---

[25] *Id.*, at 1980.
[26] *Id.,* at 2019.
[27] For example, the Santa Clara District Attorney's Office advises that if an "[e]xaminer discovers evidence of another crime(s) that is outside the scope of the submitted search warrant, the Examiner may continue the examination for items named in the warrant. The Examiner should contact the submitting agency and/or the prosecutor handling the case for guidance before conducting any searches for evidence not

The risk of overbroad searches is especially worrying given the fact that it's nearly impossible for those outside of law enforcement — such as defense lawyers — to repeat the steps that a forensic examiner took and to audit the scope of a search. A handful of agency policies do require examiners to document how a search was conducted, but the level of documentation required is still unlikely to allow a defense lawyer to meaningfully audit a search.

Legal scholars and courts have wrestled with the problems of overbroad digital searches for decades.[28] It's especially striking, given the prominence of these legal debates, that law enforcement agencies including Seattle Police Department have largely allowed officers and forensic examiners to search cellphones without detailed policies and with few constraints. SPD asserts that their cellphone searches are restricted to consent searches and warrants[29] — in practice, this means that residents of Seattle have no protections against overbroad violations of their rights.

---

named in the original warrant." *See* Santa Clara District Attorney's Office, Santa Clara County Crime Laboratory Computer Forensic Standard Operating Procedures, https://beta.documentcloud.org/documents/20394644-2019-08-19-pra-resp-email-att-standard-operating-procedures-rev-26-112820181. As another example, the San Diego Police Department says that if "an examiner discovers evidence of another crime(s) that is outside the scope of the submitted legal authority, the examiner will notify the assigned prosecutor and/or submitting investigator of the discovery and nature of any evidence of other crime(s) outside the scope of the original search warrant." *See* San Diego Police Department, Forensic Technology Unit Manual, https://beta.documentcloud.org/documents/20392583-forensic-technology-unit-manual-082218-current.

[28] *See, e.g.,* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1 (2011); James Saylor, *Computers As Castles: Preventing the Plain View Doctrine From Becoming a Vehicle for Overbroad Digital Searches*, 79. Ford. L. Rev. 2809 (2011); Eric Yeager, *Looking for Trouble: An Exploration of How to Regulate Digital Searches*, 66 Vand. L. Rev. 685 (2013); Andrew D. Huynh, *What Comes after Get a Warrant: Balancing Particularity and Practicality in Mobile Search Warrants Post-Riley*, 101 Cornell L. Rev. 187 (2015); Adam Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in cellphone Searches*, 69 Vand. L. Rev. 585 (2016); Michael Mestitz, *Unpacking Digital Containers: Extending Riley's Reasoning to Digital Files and Subfolders*, 69 Stan. L. Rev. 321 (2017); Sara J. Dennis, *Regulating Search Warrant Execution Procedure for Stored Electronic Communications*, 86 Ford. L. Rev. 2993 (2018); Laura Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L. J. Forum 961 (2019); Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643 (2020); Cameron Cantrell, *A Dignitary Fourth Amendment Framework and Its Usefulness for Mobile Phone Searches*, 25 Va. J.L. & Tech 242 (2022).

[29] 2022 Surveillance Impact Report — Computer, Cellphone, and Mobile Device Extraction Tools, Seattle Police, *available at* https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Computer%2C%20Cellphone%2C%20%26%20Mobile%20Device%20Extraction%20Tools.pdf

5. MDFTs are too powerful in the hands of law enforcement. Recognizing that they are already in widespread use across the country, several policies must be enacted to limit how MDFTs expand law enforcement's investigatory power.

We believe that MDFTs are simply too powerful in the hands of law enforcement and should not be used. But recognizing that MDFTs are already in widespread use across the country, we offer a set of preliminary recommendations that we believe can, in the short-term, reduce the use and harm of MDFTs in Seattle:

- **Ban the use of consent searches of mobile devices.** Police consent searches in any context are troubling, but the power and information asymmetries of cellphone consent searches are egregious and unfixable. Accordingly, policymakers should ban the use of consent searches of cellphones.[30]

  As explained in Section 4, the doctrine underlying "consent searches" is a legal fiction.[31] When courts pretend that "consent searches" are voluntary, they fail to account for the important racial differences in how individuals interact with law enforcement.[32] As one scholar noted, "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."[33] Given the extreme power asymmetries, it's a "simple truism that many people, if not most, will always feel coerced by police 'requests' to search."[34] Further, most of the

[30] California's Racial and Identity *Profiling* Advisory Board recently suggested that policymakers should "should consider prohibiting consent searches of cell phones." *See* Racial & Identity *Profiling* Advisory Board, Racial & Identity *Profiling* Advisory Board Annual Report 2022, 112 (January 2022).
[31] Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773, 775 (2005) ("Over 90% of warrantless police searches are accomplished through the use of the consent exception to the Fourth Amendment.")
[32] Tracey Maclin, *"Black and Blue Encounters" Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?*, 26 Val. U. L. Rev. 243, 248 (1991). ("Instead of acknowledging the reality that exists on the street, the Court hides behind a legal fiction. The Court constructs Fourth Amendment principles assuming that there is an average, hypothetical person who interacts with the police officers. This notion . . . ignores the real world that police officers and black men live in.")
[33] Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 242-243 (2001). ("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.") Indeed, as another scholar argued, the "consent search doctrine is the handmaiden of racial profiling." See George C. Thomas III, *Terrorism, Race and a New Approach to Consent Searches*, 73 Miss. L. J. 525, 542 (2003).
[34] Marcy Strauss, *Reconstructing Consent*, 92 J.Crim. L. & Criminology 211, 221.(2001.)

"consent to search" forms Upturn obtained from law enforcement agencies don't clearly specify how they will search the phone, the tools they'll use, or the extent of the search.[35]

Some believe that officers should provide warnings to ensure consent searches are voluntary. Such warnings would inform the subject of the search that they are being asked to voluntarily, knowingly, and intelligently consent to a search. But warnings are not enough. One study found that participants who received a warning about their right to refuse a consent search were just as likely to comply with the search.[36] This is also consistent with an earlier analysis of data collected from the Ohio Highway Patrol on motor vehicle stops, which found no decrease in consent rates after a law requiring warnings was introduced.[37]

Banning consent searches is not a new suggestion.[38] Nor is it a perfect solution, as it's easy for law enforcement to obtain a search warrant. But banning consent searches of cellphones can help limit police discretion, limit the coercive power of police, and minimize the amount of information that can be collected from people

[35] The Denver Police Department's consent form mentions that devices may be submitted "to the computer forensic laboratory for copying and examination." *See* https://beta.documentcloud.org/documents/20390003-consent-for-search-of-cell-phone-tablet. The Tampa Police Department's mentions that "this search may require the temporary utilization of software and/or hardware." *See* https://beta.documentcloud.org/documents/20393153-tpd-form-142-e-consent-to-search-electronic-media-devices-english. The Colorado State Patrol's consent form mentions that they can "submit the electronic device described below to a computer/electronic forensic examiner . . . who has specialized training necessary to conduct such an examination." *See* https://beta.documentcloud.org/documents/20391059-csp-343-consent-to-search-electronic-device. The Illinois State Police's consent to search form mentions that their search "may include the duplication/imaging and complete forensic analysis of any data contained within the internal, external, andlor removable storage media of this device." *See* https://beta.documentcloud.org/documents/20391550-img_0001.

[36] Roseanna Sommers, Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L. J. 1962, 2000 (2019).

[37] Illya Lichtenberg, *Miranda in Ohio: The Effects of Robinette on the "Voluntary" Waiver of Fourth Amendment Rights*, 44 HOW. L.J. 349 (2001) (Examined highway stops in Ohio between 1987 and 1997. During that time period, the state introduced a law requiring police to inform motorists that they were free to leave before requesting consent. Lichtenberg found no decrease in consent rates among motorists before versus after the reform was adopted.)

[38] For example, the New Jersey Supreme Court outlawed consent searches during traffic stops where no reasonable suspicion exists. The California Highway Patrol banned its use of consent searches as part of a broader class action lawsuit brought because of racial profiling. And in Rhode Island, by law, "[n]o operator or owner-passenger of a motor vehicle shall be requested to consent to a search by a law enforcement officer of his or her motor vehicle, that is stopped solely for a traffic violation, unless there exists reasonable suspicion or probable cause of criminal activity."

under investigation. Seattle City Council should ban consent searches of cellphones.

- **Require easy-to-understand audit logs.** Seattle City Council should require that mobile device forensic tools used by law enforcement have clear recordkeeping functions, specifically, detailed audit logs and automatic screen recording. With such logs, judges and others could understand the precise steps that law enforcement took when extracting and examining a phone, and public defenders would be better equipped to challenge those steps. Audit logs and screen recordings would document a chronological record of all interactions that law enforcement had with the software, such as how they browsed through the data, what search queries they used, and what data they could have seen. This information would be stored in the MDFT itself as a log that is easily shareable with auditors, judges, and defenders.

  There is an extreme power and resource imbalance between public defenders and law enforcement in general,[39] and especially when it comes to digital evidence. Few public defenders have access to MDFTs. Instead, defenders are forced to examine forensic reports that are thousands of pages long and "easily navigable only if you have a forensic company's proprietary software"— which they can rarely afford.[40] Further, defenders and judges often have no way of knowing whether law enforcement actually stayed within the bounds of a search warrant for a phone. For courts, simply taking law enforcement's word for it should be insufficient — lying

[39] Research has demonstrated that fewer than 30 percent of county-based and 21 percent of state-based public defender offices have enough attorneys to adequately handle their caseloads. *See* Bureau of Justice Statistics, Lynn Langton and Donald Farole Jr., County Based and Local Public Defender Offices, 2007 (2010), 8, https://www.bjs.gov/content/pub/pdf/clpdo07.pdf; Bureau of Justice Statistics, Lynn Langton and Donald Farole Jr., State Public Defender Programs, 2007 (2010), 12, https://bjs.ojp.gov/content/pub/pdf/spdp07.pdf. *Also see* Justice Policy Institute, System Overload: The costs of Under-Resourcing Public Defense, 2011, *available at* http://www.justicepolicy.org/uploads/justicepolicy/documents/system_overload_final.pdf; American Bar Association, Gideon's Broken Promise: America's Continuing Quest for Equal Justice (2004); Bryan Furst, A Fair Fight: Achieving Indigent Defense Resource Parity, Brennan Center, September 9, 2019, *available at* https://www.brennancenter.org/sites/default/files/2019-09/Report_A%20Fair%20Fight.pdf.

[40] Kashmir Hill, "Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone." New York Times, November 22, 2019, *available at* https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html.

under oath is endemic to the institution of American policing.[41] Thus, audit logs would be especially helpful for defenders trying to suppress evidence that was obtained illegally.

This recommendation even comports with principles articulated by law enforcement associations, like the Association of Chief Police Officers, which has said that "[a]n audit trail . . . of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."[42] Seattle Police Department even wrote that "all device utilization is documented and **subject to audit** by the Office of Inspector General and the federal monitor at any time."[43] Having these logs ensure that actual, detailed audits are possible.

The critical caveat is that audit logging is unlikely to be an effective tool for broad transparency and police accountability. This tool will not necessarily improve police behavior, but on a case-by-case basis, this tool could give public defenders

---

[41] *See, e.g.*, Irving Younger, "The Perjury Routine," The Nation, May 8, 1967; Myron R. Orfield, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 Chi. L. Rev. 1016 (1987); Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, City of New York, Commission Report (1994) at 38; Stanley Fisher, *"Just the Facts, Ma'am": Lying and the Omission of Exculpatory Evidence in Police Reports*, 28 N. Eng. L. Rev. (1993); Joseph Goldstein, "'Testilying' by Police: A Stubborn Problem," The New York Times, March 18, 2018, *available at* https://www.nytimes.com/2018/03/18/nyregion/testilying-police-perjury-new-york.html; Peter Keane, "Why cops lie," San Francisco Chronicle, March 15, 2011; Michael Oliver Foley, Police Perjury: A Factorial Survey, (2000); Samuel Gross, et al., *Government Misconduct and Convicting the Innocent: The Role of Prosecutors, Police and Other Law Enforcement*, National Registry of Exoneration, September 1, 2020, *available at* https://www.law.umich.edu/special/exoneration/Documents/Government_Misconduct_and_Convicting_the_Innocent.pdf.

[42] Association of Chief Police Officers, *APCO Good Practice Guide for Computer based Electronic Evidence*, March 2012, *available at* https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. *Also see*: Rick Ayers, Sam Brothers, Wayne Jansen, *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101, Revision 1, National Institute of Standards and Technology, May 2014, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. (noting that "[p]roper documentation is essential in providing individuals the ability to re-create the process from beginning to end."); Scientific Working Group on Digital Evidence, SWGDE Best Practices for Mobile Phone Forensics, Feb. 11, 2013, *available at* https://drive.google.com/open?id=18dwENQNztbEa0G9GLSUeDxZxeDEeUc-3 (noting that documentation should include "sufficient detail to enable another examiner, competent in the same area of expertise, to repeat the findings independently.").

[43] Computer, Cellphone, and Mobile Device Extraction Tools. Seattle Police Department. https://www.seattle.gov/documents/Departments/Tech/Privacy/Computer%2C%20Cellphone%2C%20%26%20Mobile%20Data%20Extraction%20One%20Pager.pdf

and judges a significantly clearer window into the nature and extent of cellphone searches.

- **Enact robust data deletion and sealing requirements.** Seattle City Council should require law enforcement to delete any extracted cellphone data that is not related to the objective of the warrant within thirty days of the date the information is obtained.[44] In addition, for cases that result in a conviction, data that was deemed relevant should be sealed at the conclusion of the case. For other cases, where charges are dismissed or do not result in conviction, all data should be deleted, relevant or not. Data deemed relevant in one case should never be used for general intelligence purposes or used in unrelated cases.

  In the absence of clear law or policy, law enforcement could use personal information like contact lists, photos, and location data to fuel harmful police surveillance systems. This is true not only for the person whose phone was searched, but also for anyone they have used their phone to contact — friends, family, colleagues, or even new acquaintances. Cellphone searches are unlike traditional seizures because law enforcement extracts all of the data on the device and only after this seizure do they search for case-relevant information. Maintaining information outside the scope of the warrant is akin to law enforcement maintaining the ability to indefinitely and limitlessly search a home.

- **Require public logging of SPD use of MDFTs.** The City of Seattle should require public reporting and logging of how law enforcement use mobile device forensic tools. These records should be released at least monthly, as this would allow more immediate access to information by advocates, policymakers, and the public seeking to understand the capabilities and practices of their police agency. Agencies should additionally release annual reports on overall department usage.

  These records should include aggregate information such as:

  - How many phones were searched in a given time period.
  - Whether those searches were by consent (though consent searches should be banned), or through a warrant.
  - Warrant numbers associated with searches, when applicable.
  - The types of offenses being investigated.

[44] The only exception should be for exculpatory information.

- How often MDFTs led to successful data extractions.
- Explanations for any failed extractions.
- Which tools were used for extraction and analysis, and their version numbers.

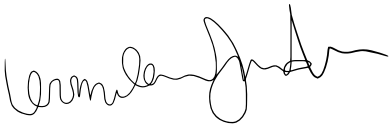
Conclusion

Mobile device forensic tools are far too powerful to be in the hands of law enforcement. Phones centralize more information about a person than previously possible and MDFTs are designed to extract the maximum amount of information from them. The racial disparities in who police target for searches and surveillance mean that Black and brown people living in Seattle are far more likely to be harmed by cellphone searches. That these tools have no real limits or policies governing their use is untenable.

Short of an outright ban of MDFTs, there are many ways to immediately reduce the harm these tools currently create: Audit logs, clear public logging, data deletion, and sealing can reduce the scale at which MDFTs create and exacerbate harm. Banning consent searches in general, and especially for cellphones, would protect individuals from coercive searches by police and from unwittingly turning over essentially all of their personal information.

I hope that this information is useful to the Council and Surveillance Working Group. Thank you for the opportunity to comment on these technologies.

Sincerely,



Urmila Janardan
Policy Analyst, Upturn
urmila@upturn.org