



VIA EMAIL

October 27 2020

Mayor Bob Sampayan
Vice Mayor Hermie Sunga
Councilmember Hakeem Brown
Councilmember Pippin Dew
Councilmember Robert McConnell
Councilmember Katy Miessner
Councilmember Rosanna Verder-Aliga

Dear Mayor Sampayan and Honorable Members of the Vallejo City Council,

Thank you for scheduling a hearing on the Vallejo cell site simulator policy. We write regarding the proposed policy (the "Policy") before the Vallejo City Council for consideration on October 27, 2020 as item 8b on the regular meeting agenda. As written, the policy does not adequately protect the civil rights and civil liberties of Vallejo residents from the harms of cell site simulator surveillance.

We strongly encourage you to use this occasion as a first step towards implementing a municipal ordinance providing for community control over police surveillance that would provide additional transparency pertaining to the use of surveillance devices by the police and help to avoid another future situation where a Vallejo agency initially fails to comply with a California state law regulating surveillance technology. Such an ordinance would accomplish this by ensuring a public discussion, a vote by elected leaders, and robust policies for any surveillance technology before they are acquired and put into use. At this time, seven Northern California jurisdictions – including Oakland, Davis, Berkeley, and San Francisco – have adopted ordinances of this kind.

Cell site simulators are powerful surveillance devices that mimic a cell phone tower and thereby trick wireless devices into communicating with them. These devices raise significant constitutional, privacy, and civil liberties concerns. This privacy-invasive surveillance tool conducts general searches, invades privacy, and disparately impacts people of color. To protect the rights of the people of Vallejo, we urge the council to require the police to get rid of this tool. Should you allow the police to retain this concerning technology, elected officials and members of the public must know how and when the devices will be used and what safeguards exist to protect rights and prevent abusive surveillance. We have several suggestions to strengthen the city's policy and enable stronger accountability.

THE POLICY SHOULD EXPLICITLY PROHIBIT CELL SITE SIMULATOR USE IN CONNECTION WITH OR IN THE VICINITY OF FIRST AMENDMENT ACTIVITIES

Cell site simulators can collect information about many phones in an area, which can reveal who is present at a particular place or event where First Amendment activity is occurring. As written, the Policy only makes a general statement of respect for the First Amendment. That statement does not contain explicit guidance about the use of a cell site simulator where there may be First Amendment activity at issue. To ensure that people's First Amendment rights are not intentionally or unintentionally infringed upon through use of this technology, Vallejo should commit in this Policy to never use a cell site simulator in the vicinity or in connection with First Amendment activities, including but not limited to protests, places of worship, or near political gatherings. The Policy should make explicit that the use of a cell site simulator in the vicinity or in connection with such events is prohibited.

THE POLICY SHOULD EXPLICITLY PROHIBIT CELL SITE SIMULATOR USE ON BEHALF OF, OR THE SHARING OF INFORMATION DERIVED FROM CELL SITE SIMULATOR USE, WITH FEDERAL IMMIGRATION AUTHORITIES

The City should ensure that federal immigration agencies cannot exploit city surveillance technology. In other contexts, we have seen federal immigration entities seek to use surveillance technologies to assist¹ The current Policy lacks appropriate protections to prevent this from occurring. The Policy should be amended to explicitly prohibit the use of the cell site simulator on behalf of immigration agencies and the sharing of information derived from the use of a cell site simulator with the same.

THE POLICY SHOULD PROHIBIT MONITORING OR INTERCEPTING COMMUNICATIONS AS WELL AS COLLECTING THEM.

The KeyW CONDOR cell site simulator purchased by the Vallejo Police Department may have the capability to eavesdrop or monitor on phone calls and text messages. The policy suggests that any such capabilities of a cell site simulator will not be used to “collect” sensitive information including but not limited to emails, texts, and images. The Policy should also separately make explicit that the cell site simulator will also not be used to *intercept or monitor* this information.²

¹ See, e.g., Vasudha Talla, Records Reveal ICE Using Mass Surveillance Database to Track People With Aid of Local Law Enforcement, ACLU of Northern California, Mar. 13, 2019,

²Example of suggested modification (suggestions in **bold**): “Cellular site simulators used by the Vallejo Police Department shall not be used to collect, **eavesdrop on or intercept** the contents of any communication, in accordance with 18 U.S.C. § 3121 (c). Cellular site simulators employed by the Vallejo Police Department shall not capture, **eavesdrop on**, or intercept emails, texts, contact lists, images or any other data contained on the phone.”

DATA OBTAINED UNDER EXIGENCY USE SHOULD BE IMMEDIATELY DELETED IF THE WARRANT REQUEST IS DENIED

If the cellular site simulator is used for an identified exigency and the warrant applied for to support the use is denied by a court, any information collected during the alleged exigency should be immediately purged and deleted. This is consistent with the Police Chief's statement to the Council on March 24th that a warrant or court order is required to use the cell site simulator and necessary to avoid possible misuse of the exigency clause. A procedure for purging or deleting such data should be explicitly stated in the policy.

THE POLICY'S EXIGENCY LANGUAGE IS NOT CONSISTENT WITH CALIFORNIA ELECTRONIC PRIVACY LAW

The California Electronic Communications Privacy Act (CalECPA, Cal. Penal Code § 1546 et. Seq.) imposes a high standard that must be met in order to justify the exigent access to electronic device information. The current Policy does not mirror this standard in its language. Under the law, a government entity without a warrant may access electronic device information by means of electronic communications with the device where there is an "emergency involving danger of death or serious physical injury" requiring such access. Cal. Penal Code § 1546.1(c)(6). The current Policy omits "serious" in "serious physical injury." The Policy should be amended to reflect the legally required standard by adding "serious" to the exigency language so it does not merely say "bodily injury."

NOTIFICATION REQUIREMENTS CONTAINED IN PENAL CODE 1546.2 SHOULD BE STATED IN THE POLICY

People should not be left in the dark about the use of cell site simulators against them. Vallejo residents who are subject to the use of cell site simulator surveillance have a right to be told meaningful information about such surveillance when it occurs. As a general rule, current law (CalECPA) requires that the government notify the subject of a warrant or an exigent action to obtain information from an electronic device. Ca. Penal Code § 1546.2.³ The Policy should explicitly specify the process for providing notice to people impacted by surveillance, including criminal defendants, in compliance with the law.

³ "[A]ny government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency request, a notice that informs the recipient that information about the recipient has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three days after obtaining the electronic information."

It is also important that Vallejo Police make courts aware that the use of these devices may also interfere with normal cell phone service. The disruption of cell network can harm public safety if people who need to access emergency services are unable to establish a cell phone connection. To ensure courts are aware of this, the Policy should require that any warrant application include information describing to the court the possibility that such disruption may occur, where it is a possibility.⁴

THE USE POLICY SHOULD EXPLICITLY MANDATE THAT THE ANNUAL LOG AND REPORT WILL BE PUBLICLY RELEASED

Vallejo residents and the City Council should not be kept in the dark about how the cell site simulator is used. At the March 24, 2020 meeting of the Vallejo City Council, Police Chief Shawny Williams said that the usage log and annual report “will be publicly available on our website.” However, the Policy only states, “The annual report will be made available to the public with redaction of information related to any ongoing investigations or other exempt material.” We strongly recommend that the policy include a written requirement for posting this information on the City of Vallejo website so that the public is provided meaningful information about how their government uses this surveillance technology .

We look forward to working with you to develop frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Thank you for your time and consideration.

Tracy Rosenberg for Oakland Privacy
Raquel Ortega for the ACLU of Northern California
Nathan Sheard for the Electronic Frontier Foundation

cc:

Police Chief Shawny Williams
City Manager Greg Nyhoff
Interim City Attorney Randy J. Risner

⁴ For example, in a warrant application dated July 13, 2012, the US government acknowledged that a cell site simulator may at times disrupt cell phone service: “Because of the way the Mobile Equipment sometimes operates, its use has the potential to intermittently disrupt cellular service to a small fraction of ...wireless customers within its immediate vicinity.” *In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of Pen Register and Trap and Trace Devices for the Cellular Telephone Facility Assigned to the Telephone Number 908-448-3855*, at *8, D.N.J., Mag. No. 12-3092, <https://www.wired.com/wp-content/uploads/2015/02/Stingray-pen-register-order-and-application.pdf>