November 19, 2015

For Immediate Release

Contact: Brian Hofer Email: brian.hofer@gmail.com Tel: (510) 303-2871

Alameda County Board Of Supervisors Passes Most Comprehensive Cell Phone Interceptor Privacy Policy In the Country

Oakland-In an example of collaboration with privacy advocates, on November 17th the Alameda County Board of Supervisors passed a comprehensive privacy policy regulating the county's use of cell phone interceptor equipment (often referred to in the press by "*Stingray*" or "*Hailstorm*") before approving the purchase of an equipment upgrade. The policy requires a warrant before any deployment of the device.

Governor Jerry Brown signed SB 741 (Hill, S-13-D) into law earlier this year requiring cell phone interceptor technology be subject to public hearings prior to purchase and annual use audits. Alameda's purchase was first presented in October 2015 and was intended to go forward before the new law took effect on January 1, 2016.

Privacy activists from Oakland Privacy Working Group, an ad-hoc citizens group that came together in the City of Oakland in 2013 to engage with municipal government on issues of privacy and surveillance equipment, delayed the vote of approval and, in conjunction with the ACLU of Northern California and Bay Area Council on American-Islamic Relations (CAIR-SFBA), met with every member of the Board of Supervisors to insist the upgrade purchase not go forward until a comprehensive privacy policy was drafted, approved by the Board and was in compliance with the new state law.

The Board of Supervisor's vote was unanimous. It was accompanied by a statement from Supervisor Richard Valle that the County would soon take up a global privacy ordinance for all surveillance equipment used by the County Sheriff and District Attorney, similar to ordinances now under consideration in the City of Oakland and Santa Clara County.

"Stingrays" are fake cell phone towers which divert cell phone signals away from commercial towers and into the equipment. The system collects metadata, and with accompanying software can also monitor the contents of cell phone traffic within the vicinity of a targeted phone number or location. Their use, which is widespread in US law enforcement agencies, has been largely cloaked with non-disclosure agreements required by manufacturer Harris Corporation. Prosecutors have numerous times gone so far as to drop criminal prosecutions rather than disclose the use of Stingrays in public courtrooms. Public records requests by the ACLU and individual privacy advocates have uncovered the extent of the device's use across the country which, until recently, has been entirely unregulated.

In response to growing unease over the dragnet surveillance performed by these interceptor devices, the Department of Justice announced a new policy for their use by federal agents in September of 2015 to "enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard and increase privacy protections in relation to law enforcement's use of this critical technology." Earlier this year, Washington state adopted a statute governing cell phone interceptor use, requiring law enforcement to get a warrant prior to deploying the device and that law enforcement explain in detail to the judge how the equipment works.

The use of any surveillance equipment is a danger to the people's rights under the 4th Amendment. The use of equipment without the public's knowledge and without constraints, as has been the history of "Stingray" usage to date, is beyond the pale. The Oakland Privacy Working Group applauds Alameda County in taking this historic step to conform to strictly regulate cell phone simulator technology, and looks forward to working with the County to develop an overarching policy for all current and future surveillance capabilities.

"We thank the Board for calling for a public comment period on the use policy, and for the District Attorney being receptive to the feedback her office received. The end result is a strong policy with significant safeguards built in and transparency as to use." Brian Hofer, Oakland Privacy Working Group.

###