TESTIMONY OF NATHAN FREED WESSLER, Esq.

LD 894 – Ought to Pass

An Act To Increase Government Accountability by Removing the Restriction on the Dissemination of Information Regarding Investigations

Committee on Criminal Justice and Public Safety

April 12, 2021

Senator Deschambault, Representative Warren, and members of the Committee, thank you for the opportunity to offer testimony in support of LD 894. My name is Nate Freed Wessler, and I am a deputy director of the American Civil Liberties Union's Speech, Privacy, and Technology Project, where I focus on ensuring that law enforcement agencies' use of surveillance technologies comply with the Fourth Amendment's protections for privacy. In my work, I frequently make use of state and federal freedom of information laws, which are a critical tool for members of the public to hold government agencies accountable. I have also published one of the few law review articles about the precise issue before the Committee this morning—government agencies refusing to confirm or deny the existence or nonexistence of records, which is commonly known as a "Glomar response."[1]

I grew up in Litchfield and Hallowell, where my mother still lives and is a constituent of Representative Warren. I remember my social studies teacher at Hall-Dale

[1] *See* Nathan Freed Wessler, Note, *"We Can Neither Confirm Nor Deny The Existence or Nonexistence of Records Responsive To Your Request": Reforming the Glomar Response Under FOIA*, 85 N.Y.U. L. Rev. 1381 (2010).

Middle School teaching me the meaning of Maine's motto, Dirigo: I lead. I am proud of all the ways this state leads the nation on issues of privacy policy and good government, including passing one of the earliest and strongest protections against warrantless access to cell phone location information back in 2013,[2] and passing the strongest internet privacy law in the country two years ago.[3] But unfortunately, on the issue before the Committee this morning, Maine is dead last in the country. On behalf of the ACLU and ACLU of Maine, I urge the committee to vote "ought to pass" on LD 894, which would bring Maine back into synch with the laws of 48 other states and the federal Freedom of Information Act. Passing this law will take Maine out of the running for the unfortunate distinction as least transparent and accountable state in the nation.

The current text of title 16, section 807 dangerously undermines the basic transparency that we expect of government agencies in a democratic society. Instead of allowing agencies to respond to requests submitted under the Freedom of Access Act, it requires that Maine law enforcement agencies refuse to confirm or deny the existence or nonexistence of records any time one of the underlying records is exempt from disclosure. This makes it virtually impossible for members of the public, reporters, and lawmakers to know how our taxpayer dollars are being spent, and whether police are engaged in controversial or privacy-invasive practices. Without basic transparency, there cannot be adequate accountability.

There are two irredeemable problems with Section 807, which are best addressed by repeal. **First**, Section 807 gives agencies no discretion: it *requires* them to refuse to

[2] LD 415 (126th Leg., 2013), codified at 16 M.R.S. §§ 647–650.

[3] LD 946 (129th Leg., 2019), codified at 35-A M.R.S. § 9301.

confirm or deny whether they have records on a particular subject. No other state has a law like this, and for good reason. The law is counterproductive, because it hobbles agencies' ability to engage in public debate about matters of public concern, such as whether police are appropriately using invasive surveillance technologies that can sweep in information about innocent bystanders. And it can lead to absurd results, forcing law enforcement agencies to choose between their responsibility to provide accurate information to the communities they serve and their fear of violating the law.

Second, Section 807 requires Glomar responses when they are not justified, without any showing that responding to a request for records would cause harm. No other state or federal statute or court decision permits this. In narrow circumstances, courts have allowed Glomar responses when information about whether records exist is itself exempt from disclosure. Section 807, in contrast, requires agencies to clam up before they even search for records, and without any showing that confidential information would be revealed by confirming or denying that records exist.

As a result, Maine's practice is way out of step with the practices of federal, state, and local law enforcement agencies across the country. For example, in 2016,[4] and again in 2020,[5] the Maine State Police refused to confirm or deny whether the agency had records about purchase and use of a controversial and invasive cell phone surveillance

[4] Curtis Waltman, *Maine State Police "Can Neither Confirm Nor Deny" Use of Cellphone Surveillance*, Muckrock (Nov. 9, 2016), https://www.muckrock.com/news/archives/2016/nov/09/msp-glomar/.

[5] Randy Billings, *Bill Aimed at Lifting Shroud of Secrecy Covering Police Surveillance Advances*, Portland Press Herald (Mar. 3, 2020), https://www.pressherald.com/2020/03/03/bill-aimed-at-lifting-shroud-of-secrecy-covering-police-surveillance-advances/.

technology known as a "cell site simulator" or "Stingray."[6] Issuing a Glomar response about this topic is not the norm. Largely as a result of public records requests about cell site simulator technology submitted by the ACLU, journalists, and privacy activists across the country, we now know that at least 75 state and local law enforcement agencies in 27 states have the technology, as do at least 14 federal agencies.[7] When presented with a request for records about purchase or use of cell site simulators, the vast majority of law enforcement agencies across the country have acknowledged whether they have responsive records, and have released at least some of their underlying documents. This is true of major federal law enforcement agencies such as the Federal Bureau of Investigation and the Drug Enforcement Administration and smaller federal agencies such as the Criminal Division of the Internal Revenue Service; of state police agencies from states large and small, from the Florida Department of Law Enforcement to the Delaware State Police; and of police departments in cities ranging in size from New York City, Los Angeles, and Chicago, to Lakeland, Florida, and Rochester, New York. Here in northern New England, I am aware of proper responses from the New Hampshire State Police, Vermont State Police, and the Boston Police Department addressing whether they have records about cell site simulators. Maine's Glomar

[6] Cell site simulators are powerful tools that track, locate, and identify people's cell phones. They work by mimicking legitimate cell phone towers and tricking phones in the area into communicating with the police device instead of the actual tower network. This technology raises privacy concerns because it can precisely locate people, including inside of their homes and other constitutionally protected spaces, and because even when police are looking for a particular suspect, the technology sweeps in information about bystanders who just happen to be nearby, and can even interfere with those bystanders' phone calls.

[7] *See* ACLU, *Stingray Tracking Devices: Who's Got Them*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them.

response stands virtually alone. Indeed, last year, at virtually the same time that the Maine State Police issued its Glomar response about this technology, I received 1,094 pages of documents from U.S. Immigration and Customs Enforcement about its purchase and use of cell site simulator devices. If ICE can engage in basic transparency about this technology, so can MSP.

This isn't the only concerning surveillance technology about which the Maine State Police have issued a Glomar response. As the Portland Press Herald has reported, MSP refused to confirm or deny the existence or nonexistence of records about face recognition technology to the paper in 2019.[8] And in 2016, MSP refused to confirm or deny the existence or nonexistence of records about its use of powerful technology that monitors people's constitutionally protected conversations on social media platforms.[9] This, too, is not normal. Numerous law enforcement agencies across the country have released records about their use of both of these privacy-invading and error-prone technologies.[10]

---

[8] Randy Billings, *Maine State Police May Be Spying On You*, Portland Press Herald (Feb. 9, 2020), https://www.pressherald.com/2020/02/09/maine-state-police-may-be-spying-on-you/.

[9] https://www.muckrock.com/foi/maine-13/geofeedia-inc-contracts-invoice-social-media-surveillance-policies-maine-state-police-30851/.

[10] *See, e.g.*, Clare Garvie, et al., Center on Privacy & Technology, Georgetown Law, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* 15 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf ("[W]e submitted detailed public records requests [about face recognition technology] to over 100 law enforcement agencies across the country. In total, our requests yielded more than 15,000 pages of responsive documents. Ninety agencies provided responsive documents—or substantive responses—of some kind."); *ACLU v. U.S. Dep't of Justice*, __ F. Supp. 3d __, No. 19-cv-290, 2019 WL 6117421

Basic transparency matters in a democracy. Transparency provides the information that citizens and lawmakers need to debate and enact protections against government abuses. For example, after police departments in Washington State and Illinois confirmed that they use cell site simulators, lawmakers in those states enacted strong laws that require police to obtain a judge's permission and take other steps to protect people's privacy before using the devices.[11] Information revealing the Baltimore Police Department's use of social media monitoring technology to surveil protesters led to pressure on Facebook, Twitter, and other social media companies, which eventually decided to cut off access to their users' data for the surveillance company being used—and abused—in Baltimore and elsewhere.[12] And in at least than 20 cities across the country, information about automated face recognition systems has led lawmakers to enact bans or moratoriums on police use of that troubling technology.

Repealing Section 807 is necessary to restoring Mainers' ability to obtain basic information about government practices. But it is important to understand that passage of LD 894 will leave plenty of options for police in Maine to protect legitimately confidential information. If a document properly falls under an exemption to disclosure, such as because its release would interfere with an active criminal investigation or

---

(N.D. Cal. Nov. 18, 2019) (listing information about social media surveillance released by various federal agencies in response to ACLU FOIA request).

[11] *See* 725 Ill. Comp. Stat. 137/5–137/15; Wash. Rev. Code § 9.73.260.

[12] *See* Kevin Rector & Alison Knezevich, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, Baltimore Sun (Oct. 11, 2016), https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

constitute an invasion of personal privacy, then police can still redact it or withhold it completely.[13]

And, in narrow circumstances where it is truly necessary, police may still be able to issue a Glomar response. That is how things work under the federal Freedom of Information Act (FOIA).[14] FOIA does not have any explicit provision about agencies issuing a Glomar response. But starting in the 1970s, federal courts recognized that if an agency can show that confirming or denying the existence or nonexistence of records on a specific subject would itself reveal a fact that is exempt from disclosure under FOIA, the agency can maintain a Glomar response.[15] There are narrow circumstances where that makes sense. If someone sends a freedom of access request to Maine police asking for records about whether a particular individual is a confidential law enforcement source, courts may deem it appropriate to issue a Glomar response in order to avoid jeopardizing the privacy or safety of that person.[16] But what is not appropriate is an agency using a Glomar response anytime a member of the public seeks basic information about surveillance technologies and police practices that have the potential to violate core

[13] *See* 16 M.R.S.A. § 804(1), (3).

[14] 5 U.S.C. § 552.

[15] *See Phillippi v. CIA*, 546 F.2d 1009 (D.C. Cir. 1976).

[16] *See, e.g.*, *Carpenter v. U.S. Dep't of Justice*, 470 F.3d 434 (1st Cir. 2006) (permitting a Glomar response to protect information about whether a particular person is a government informant); *see also N. Jersey Media Grp. Inc. v. Bergen Cty. Prosecutor's Office*, 146 A.3d 656 (N.J. Super. Ct. App. Div. 2016) (permitting a Glomar response to protect information about whether a particular individual is under criminal investigation in order to prevent "the irreparable harm suffered by a person who has been the subject of unproven allegations of criminal wrongdoing" and has not been arrested or charged).

constitutional rights. Courts have rightly rejected overbroad Glomar responses under the federal FOIA,[17] and they should have the latitude to do the same in Maine.

A vote for this bill is a vote for transparency. It is a vote to protect our democratic institutions. It would ensure a better informed public, and help guarantee that our tax dollars are spent on sensible policy. I urge you to vote ought to pass.

Thank you for your time and attention. I am happy to try to answer questions, and would welcome any member of the Committee to reach out to discuss this important legislation via my colleagues Meagan Sway and Michael Kebede at the ACLU of Maine.

[17] *See, e.g.*, *ACLU v. U.S. Dep't of Justice*, __ F. Supp. 3d __, No. 19-cv-290, 2019 WL 6117421 (N.D. Cal. Nov. 18, 2019) (rejecting FBI Glomar response as to certain uses of social media monitoring because "disclosure of social media surveillance—a well known general technique—would not reveal the *specific means* of surveillance" in ways that would jeopardize particular investigations); *see also ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2013) (rejecting CIA Glomar response because the agency's justification for it was "neither logical nor plausible").