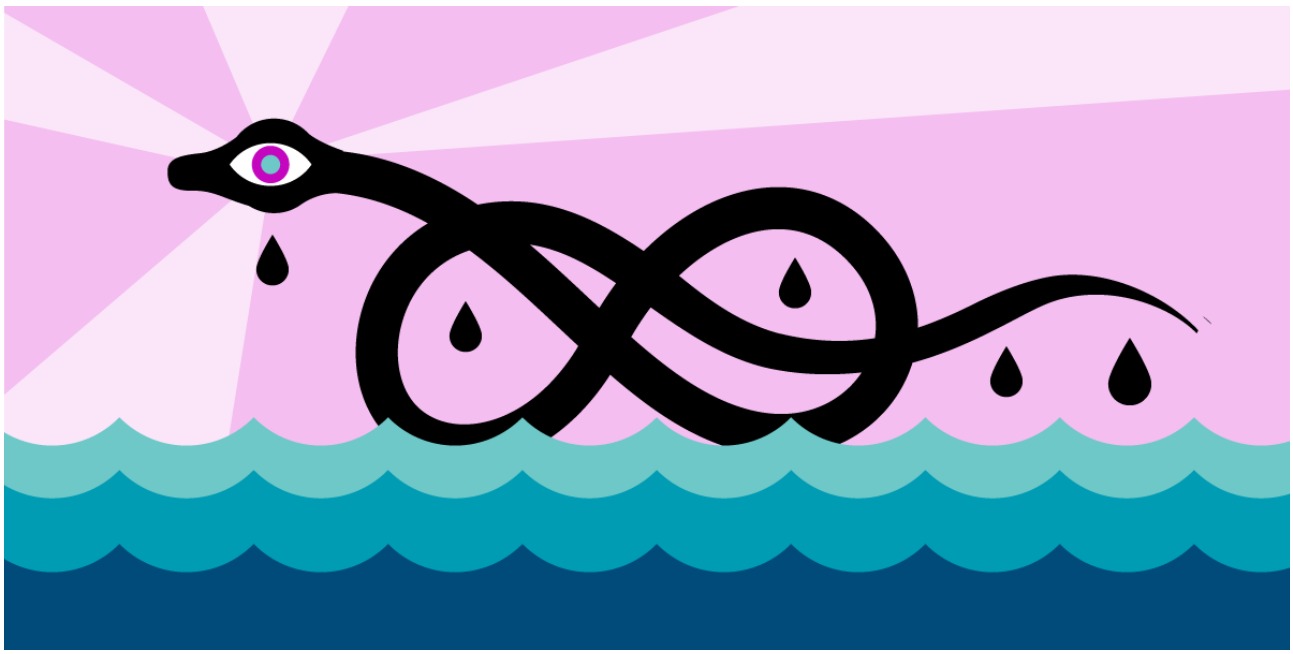
DECEMBER 15, 2016

eff.org

Investigating Law Enforcement's Possible Use of Surveillance Technology at Standing Rock



One of the biggest protests of 2016 is still underway at the Standing Rock Sioux Reservation in North Dakota, where Water Protectors and their allies are fighting Energy Transfer Partners' plans to drill beneath contested Treaty land to finish the Dakota Access Pipeline. While the world has been watching law enforcement's growing use of force to disrupt the protests, EFF has been tracking the effects of its surveillance technologies on water protectors' communications and movement.

Following several reports of potentially unlawful surveillance, EFF sent

technologists and lawyers to North Dakota to investigate. We collected anecdotal evidence from water protectors about suspicious cell phone behavior, including uncharacteristically fast battery drainage, applications freezing, and phones crashing completely. Some water protectors also saw suspicious login attempts to their Google accounts from IP addresses originating from North Dakota's Information & Technology Department. On social media, many reported Facebook posts and messenger threads disappearing, as well as Facebook Live uploads failing to upload or, once uploaded, disappearing completely.

While some have attributed these issues to secret surveillance technologies like cell-site simulators ("CSSs," also known colloquially as Stingrays) and malware, it's been very difficult to pinpoint the true cause or causes.

To try to figure this out, EFF also sent more than 20 public records requests to federal, state and local law enforcement agencies that have been sighted at Standing Rock or are suspected of providing surveillance equipment to agencies on the ground. So far, only one federal agency – the US Marshals' Service – has denied use of cell-site simulators, while the remaining federal agencies have yet to respond or have claimed their responsive documents are so numerous as to make production untenable and costly. Of the fifteen local and state agencies that have responded, thirteen deny having any record at all of cell site simulator use, and two agencies—Morton County and the North Dakota State Highway Patrol (the two agencies most visible on the ground)—claim that they can't release records in the interest of "public safety,"—even though they fail to specify what public safety interest they seek to protect or how long they expect such an interest to outweigh the public's right to know what they are doing at Standing Rock. Hennepin County, Minnesota—noted to both have access to CSSs and to have withdrawn officers and equipment from Standing Rock—has dodged our public records request by passing the buck to the Minnesota Department of Homeland Security and Emergency Management,

which has yet to respond to our inquiry.

Law enforcement agencies should not be allowed to sidestep public inquiry into the surveillance technologies they're using, especially when citizens' constitutional rights are at stake. This across-the-board lack of transparency is a real barrier to the kind of independent assessment and testing necessary to understand what technologies are being deployed on the ground, and by whom. For example, a benign variable like overloaded rural cell networks may be to blame for some of the connectivity problems water protectors have experienced. However, we can't discount the possibility of interference caused by law enforcement's use of surveillance technology against domestic activists without knowing what technologies are being used, where, when, how, why, and by whom. We need greater law enforcement transparency, deeper levels of investigation and public oversight, and continued independent testing on the ground.

We're continuing to collect incident reports from water protectors on the ground, and we're keeping an eye out for any signs of cell-site simulator use. If you're at Standing Rock, here's a list of potential signs to look out for:

1. Apparent connectivity, but unable to transmit/receive or unusual delay in calls/texts (bars, but service not normal)

2. Unexpected loss of mobile signal (no bars)

3. Sudden mobile phone battery draining

4. Unexpected downgrading in cellular network (4G to 3G, 3G to 2G, etc.)

5. IMSI catcher evidence as detected by software (e.g. AIMSICD, Snoopsnitch)

If you directly witness digital communication interference while at Standing Rock that you'd like to report, please let us know here.

It is past time for the Department of Justice to investigate the scope of law enforcement's digital surveillance at Standing Rock and its consequences for civil liberties and freedoms in the digital world. The government has a choice: if it will not be transparent enough to allow the public to police it, then it must police itself. However, if the agencies charged with serving and protecting Americans are in fact persecuting and threatening our civil rights, then they must be held accountable and stopped from violating the very rights they were created to defend.

- US Marshals' Service response
- FBI response
- Bismarck PD response
- Burleigh County response
- City of Minot response
- Gov of ND response
- Grand Forks Police response
- Grand Forks Sheriffs' response
- Hennepin Co. response
- Mercer Co. response
- Morton Co response
- ND DCR response
- ND SLC response
- NDHP response
- Stark Co. response
- Stutsman Co Sheriff response
- Williams Co. response

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

SUBMIT