A Taste of Its Own Medicine:
Michigan Holds First Public Hearing on
Secretive Hailstorm and Stingray Surveillance Devices

On Tuesday, May 13, Michigan became the first state to hold a public hearing on Hailstorm and Stingray surveillance devices.

The Oakland County Sheriff’s Office recently became the first in Michigan to purchase a Hailstorm surveillance device for ordinary domestic use and has refused to answer fundamental questions about the powerful War on Terror surveillance technology.

Organized by House Oversight Committee Chair Tom McMillin (R) in response to the Oakland County Sheriff’s Office refusal to answer questions or appear before the committee, the hearing was a public accounting of what is known about Hailstorm and Stingray devices.

Oakland County’s intransigence has led to exactly what it was hoping to avoid – public knowledge and debate about the existence and propriety of the invasive Hailstorm technology in the hands of law enforcement.

On hand to testify were two people with unique knowledge of the devices and their use by law enforcement.

Chris Soghoian, Principal Technologist and Senior Policy Analyst for the National ACLU, testified about what we know about this technology and why it’s not actually as secretive as the Harris Corporation would have us believe.

Brian Owsley, a former U.S. Magistrate Judge for the Southern District of Texas and the first post-9/11 judge to issue an order denying the government’s request to use a Stingray device, explained how law enforcement seek judicial approval by misleading judges about the invasiveness of this technology.

The hearing was live-streamed for the public, and here’s a summary of Chris Soghoian and Judge Owsley’s testimony educating the Michigan legislature and citizens about the Hailstorm/Stingray devices that may be coming to a municipality near you.
What We Know About Hailstorm and Stingray Surveillance Devices

The Hailstorm surveillance device is an updated version of Stingray, a family of technology that has been used in the military and intelligence community for the last 15-20 years.

This technology extracts cellular data and intercepts calls and texts by masquerading as cell towers for Verizon, AT&T, and other phone companies.

This means that all of the calls made by these companies’ customers are processed through Hailstorm/Stingray instead. To ensure people’s wireless devices (including iPads, tablets and laptops) connect to them, Hailstorm/Stingray devices provide the strongest signal of the available cell towers.

These devices disguise themselves as commercial towers, allowing cell users to connect with a cell tower without knowing it’s actually a direct line to the police.

As Chris Soghoian explained, this is the equivalent of police officers pretending to be phone company employees so that they can enter and inspect every home under the guise of providing service repairs – a sinister deception.

Unlike other technology, signals from Hailstorm/Stingray devices are powerful enough to penetrate through the exteriors and walls of buildings, cars and the most private and traditionally protected places to reach your phone and wireless devices. This forces your devices to respond with a signal without ever indicating to you that they are communicating with the police.

Hailstorm/Stingray devices have the capability to collect call logs, contact lists, text messages, and all other types of cellular data to learn who you communicate with most frequently. Hailstorm/Stingray technology also allows the government to learn the unique identifier associated with every device by the manufacturers. Once the police have your identifier, they can track the location of that device at all times.

By its very nature, this technology is overly broad.

These devices don’t just collect one target’s information. They pull a dragnet of information from hundreds or thousands of wireless devices in its vicinity.

While law enforcement sometimes claim that they are only saving the data of their targets, thousands of individuals are having their information collected without ever knowing how that data might or might not be used or who will see it.
In addition to wiretapping and intercepting calls, these powerful devices can be enhanced to allow authorities to eavesdrop on conversations and text messages, redirect calls to the police, and deliver malicious software and viruses to targeted devices.

Even more troubling, Hailstorm/Stingray devices are capable of preventing all calls or texts from going through (or choosing to allow a select few calls to go through) by jamming 4G and 3G networks, forcing all devices onto the older and less advanced 2G network.

This jamming ability disrupts the vital and sometimes lifesaving role that phones play in our daily lives. After all, the police don’t know whether or why you’re calling your doctor, your spouse, or your children’s school in an emergency.

These devices range in size, scope and capabilities. They can be used in cars with directional antennas pointed at a specific location or an antenna that is all-encompassing. They can be placed in briefcases, on drones, or attached to the body of a police officer as he walks through a protest and identifies all of the devices present (the Florida police requested the use of Hailstorm/Stingray devices precisely for this purpose during the WTO protests).

Police employ Hailstorm/Stingray devices in at least two major scenarios.

In the first, the police know the general vicinity but not the exact location of the targeted device and the phone company cannot provide high accuracy location information (for example, the wireless device may be indoors where only the Hailstorm device is strong enough to reach). In this scenario, the police drive through neighborhoods playing Marco Polo with hundreds or thousands of wireless devices until they detect a match.

In the second scenario, the police want to target a known individual but cannot identify their device, so they sit outside the individual’s frequented places, collecting a list of all of the devices at each location so that they can deduct which device belongs to the individual. In the process, the police create a powerful social and behavioral analysis map, similar to the NSA. This information reveals the intimate details of innocent people whose lives also revolve around those locations and who may have no connection with the individual targeted by police.

Not only are the stated uses of these devices constitutionally suspect, their incredible power and flexibility makes them extremely tempting for abuse, overreach or misuse by police.

Read Chris Soghoian’s report on Stingray surveillance devices and their impact on national security and individual privacy at http://goo.gl/ZeuNcz
Deceiving the Courts and Legislatures

Judges and legislative bodies are being hoodwinked into granting the police permission to use these devices. Across the country, decision-makers are misled about their capabilities – and that’s if they’re even told that the device in question is Hailstorm or Stingray.

Former U.S. Magistrate Judge Brian Owsley testified to explain how law enforcement seeks judicial approval by misleading judges about how indiscriminate and invasive this technology really is.

Hailstorm/Stingray surveillance devices are being purchased by local law enforcement through Department of Homeland Security grants. These grants are intended for the purpose of fighting serious rather than ordinary crimes, and so no public hearing is required for their purchase. This ensures law enforcement avoid public knowledge and debate, as well as any otherwise required approval and oversight process by municipal and state bodies.

Judge Owsley testified that prosecutors seeking judicial orders often use inappropriate pen register applications without disclosing or explaining that they are actually seeking approval for a Hailstorm or Stingray device. Pen register applications are intended for surveillance on a specific phone number and are granted under a lower legal standard because they only collect the outgoing numbers dialed.

Because Hailstorm and Stingray devices sweep up the information of innocent bystanders and third parties, violating their reasonable expectations of privacy, they require the stronger Fourth Amendment standard of a warrant based on probable cause.

Judges who see these pen register applications may not even realize that what they are actually authorizing is a blanket intercept of all cellular data on potentially thousands of cell phones, iPads and tablets rather than a traditional, targeted form of surveillance.

Troublingly, this deception may lead judges to issue orders that then create new legal precedent establishing the acceptance and legality of Hailstorm and Stingray devices without ever evaluating their constitutionality.

Judge Owsley was one of the first judges to refuse the DEA’s request for a rubber stamp order to use a Stingray device, in part because prosecutors consistently failed to meet his request that they provide him with the legal basis granting the government authority to use this technology. His was only the second order to address a cell tower simulator, and the first after the passage of the Patriot Act. Read it at http://goo.gl/4mMFX9

His order also required that law enforcement provide notice to innocent people that their data had been acquired by police and assurance that it had been destroyed.
Requiring police to give the public notice of how these devices are used is an important check on how frequently police use such tools.

If police are using Hailstorm/Stingray too liberally, the magnitude and frequency of such letters allows for electorate feedback and forces law enforcement to be more judicious about its use.

Judge Owsley also fought to have orders granting use of these devices unsealed in order to educate judges about how law enforcement were asking for permission, if they were providing truthful disclosure or misleading judges, and the scope and nature of the orders granted, but his requests were denied.

Read Judge Brian Owsley’s testimony in full at http://goo.gl/2szxPp
Violating Privacy Under Cover of Secrecy: What We Don’t Know

Because there is still so much secrecy, we still don’t know a lot of crucial information on how these devices are impacting Michiganders’ privacy.

The Oakland County Sheriff’s Office has refused to answer fundamental questions about the Hailstorm device, citing a nondisclosure agreement it had signed with the manufacturer, the Harris Corporation, which purportedly prohibits law enforcement from telling anyone – even judges and legislatures – what the device actually does and what its capabilities are.

We don’t know the specific Hailstorm device purchased by the Oakland County Sheriff’s Office or what its features or upgrades are. And, as Chris pointed out, it’s possible that even law enforcement officials are unaware of the full capabilities and invasiveness of the devices they use for mundane purposes.

We don’t know when or how the Oakland County police have already tested or used their Hailstorm device. We don’t know whether they have internal guidelines or limits on the types of crimes in which they can be used. The Oakland County Sheriff’s Office has refused to disclose any details or cooperate with the Detroit News’ FOIA request, while claiming that they follow the traditional oversight procedures of obtaining a judicial warrant. Read the Detroit News report at http://goo.gl/vDefz0

We don’t know if warrants are actually being obtained and under what justifications and which types of cases or if law enforcement are providing judges with accurate disclosures of the inherent risks and capabilities.

We don’t know what type of data is being stored or how it is being stored or for how long, nor do we know if or how any data is destroyed. Outside of a few orders like Judge Owsley’s, there is no requirement that law enforcement provide notice that data has been collected, saved or destroyed to the potentially hundreds of people affected every time they use Hailstorm/Stingray.

Without knowing how Hailstorm/Stingray devices are being used, how can lawyers, legislators and the public decide if they should ever be used?
Preventing Public Debate for Private Gain

While their manufacturer insists these surveillance devices cannot be publically discussed due to a nondisclosure agreement, these protests ring false on trade grounds.

The Harris Corporation, a defense contractor, primarily had sold these devices to federal agencies like the FBI, DHS, CIA, and NSA, but their sales have now trickled down to local law enforcement. In other words, the powerful and highly invasive surveillance technologies used for national security purposes and on wartime battlefields are now being used for routine and mundane law enforcement purposes on Main Street.

In fact, as Chris Soghoian explained, this technology is at least 20 years old. Far from being tools so secret that they should be kept hidden from the public, these tools are manufactured by numerous companies who make their manuals and patents public online and at trade shows. Their results are easily recreated by graduate students for the price of a used car (and frequently assigned as homework). These devices are already in the hands of almost every oppressive despot in the world.

In fact, the real reason they want to keep this information secret is to keep judges and legislatures in the dark and keep themselves in business.

By actively preventing public debate under the guise of trade secrets, the Harris Corporation brazenly ignores democratic accountability and judicial oversight in favor of the company’s own public relations and profit-making desires.
Shining a Light: Why It Matters and What Can Be Done

It would be highly illegal for any of us ordinary citizens to do the equivalent of what the Oakland County Sheriff’s Office claims is no big deal – yet is big enough for them to simultaneously maintain total secrecy.

While there are many things that law enforcement is solely authorized to do, the Founding Fathers were absolute in their prohibition that no judge can grant nor can any law enforcement act on a general warrant.

Yet that is exactly what Hailstorm and Stingray surveillance devices do: they search the walls of every home and building in the vicinity, indiscriminately sweeping up any and all information from countless wireless devices with no telling how the information will be used against us.

We should be able to trust that our phone conversations are private and feel reassured that when we try to dial our families, friends, employers, doctors and sensitive parties, our calls will go through to the people we intended to reach.

We should know if our cellular data is being intercepted or prevented.

We should know if our information is being saved or sold and why.

Most importantly, we should be allowed to exercise our democratic rights in response to what we find out.

While we hope Michigan joins Utah and Indiana in passing legislation requiring police to obtain a warrant based on probable cause in accordance with the Fourth Amendment before collecting cellular data, those states did so without a hearing bringing all the facts into the light.

Tuesday’s hearing should serve as an example for more states to take the lead and bring these invasive and powerful surveillance devices out of the shadows and before the public, where our Constitution requires they belong.