OFF NOW
How Your State Can Help Support the 4th Amendment
CONTENTS

Introduction .................................. 1
The Plan ..................................... 2
Is It Legal? .................................... 3
The Legislation ............................... 4
Our Progress ................................. 6
Additional Focus: Local ..................... 8
Conclusion .................................... 9
Appendix: Model Legislation ............. 10
INTRODUCTION

Information from documents obtained by whistleblower Edward Snowden in the summer of 2013 proved what many long suspected: the National Security Agency spy net spans much wider and sinks much deeper than bureaucrats and politicians would have us believe.

It only flirts with hyperbole to say the NSA spies on virtually everybody in the world.

Recent revelations also shattered the illusion that internal controls safeguard the rights of Americans, despite comforting assurances mouthed by government panels and congressional committees. Consider this: according to a report from Glenn Greenwald, “In its (the FISA Court) 35-year history, the court has approved 35,434 government requests for surveillance, while rejecting only 12.”

Forty years ago, before the advent of the Internet, Sen. Frank Church warned America about the federal spy program, saying that if a dictator took over the NSA it “could enable [him] to impose total tyranny.”

Decades later, Congress has done nothing about it. In fact, it made things worse. Courts have consistently rubber-stamped spying and presidents have offered nothing but glib promises of reform. Politicians in D.C. have failed to address the issue, even in the wake of leaked documents and damning revelations.

Simply put, we cannot count on the federal government to rein in and limit an out of control federal agency operating behind a shroud of secrecy.

So what can we do?
THE PLAN

Instead of relying on the federal government to reform its own spy program, the OffNow plan involves working at the state level. The goal - direct state governments and their political subdivisions to refuse cooperation or participation with any federal agency engaged in illegal surveillance. That includes denying them vital state-provided resources like electricity or water in order to make it so difficult for them to operate, they will have no choice but to stop violating your rights.

We can turn it off!

For instance, the data facility in Utah will reportedly use as much as 1.7 million gallons of water per day when operating at full capacity. The city of Bluffdale entered into a contract with the NSA to supply that water. Utah does not have to help a federal agency violate your rights. It can refuse to provide material support to the agency and potentially force it to reform or shut down.

With this knowledge, a strategy was born.

The OffNow plan approaches things very differently than traditional strategies, and that gives it a great chance to succeed. Our plan doesn’t depend on the political elite in D.C., but works through regular people at the grassroots level. Rather than counting on the federal government to stop federal spying programs, the OffNow plan works with states and local communities to make things increasingly difficult and eventually untenable for federal spy programs by simply saying NO!

Utah does not have to help a federal agency violate your rights. It can refuse to provide material support...

The short version: we intend to pull out the rug, box them in and shut them down.

In the summer of 2014, an article sparked an idea. In August, 2006, the Baltimore Sun reported that the NSA had maxed out its power grid in Ft. Meade, Md.

“The NSA is already unable to install some costly and sophisticated new equipment. At minimum, the problem could produce disruptions leading to outages and power surges. At worst, it could force a virtual shutdown of the agency.”

That was possibly the first public report highlighting a major problem that had been brewing within the NSA for years. Simply put, resources in Maryland could not sustain the desired expansion of the agency, and without building facilities in new locations, the NSA faced a major logistical problem.

At that time, the agency was already aggressively searching for new locations, and it was soon expanding its operation, including building its data storage facility in Bluffdale, Utah.

The Baltimore Sun article revealed the NSA’s Achilles Heel. It needs resources like water and electricity to run and cool its massive spy computers. Research reveals that state governments or their political subdivisions (local governments) often provide those resources. Legally they don’t have to. These realities led to a startling revelation.

The OffNow plan targets the surveillance state through six main avenues.

1. Denying federal agencies engaged in warrantless surveillance the resources they need to operate.

2. Prohibiting the introduction of warrantless information collected by the feds and shared with state and local law enforcement in state criminal proceedings.

3. Ending warrantless location tracking of cell-phones, and physical surveillance by drones.

4. Ending cooperative partnerships between universities and the NSA.

5. Penalizing corporations that cooperate with mass, warrantless surveillance.

6. Addressing state and local actions that feed into the larger surveillance-state, such as fusion centers, suspicious activity reporting, surveillance cameras and license plate readers.
IS IT LEGAL?

The idea of a state refusing to cooperate with a federal agency certainly causes a lot of raised eyebrows. Doesn’t the supremacy clause of the Constitution require state acquiescence?

No.

Can a state or local government legitimately and legally refuse to provide support to the NSA or other federal agencies?

Absolutely!

While state governments are limited practically in what actions they can take to block a federal agency, the federal government cannot require a state to implement or enforce its programs or policies. That the federal government cannot commandeer state resources or personnel rests on a well established legal doctrine.

Under the anti-commandeering doctrine, the Supreme Court has consistently held that the federal government cannot force states to help implement or enforce federal acts or programs. This rests primarily on four Supreme Court cases: Prigg v. Pennsylvania (1842), New York v. US (1992), Printz v. US (1997) and National Federation of Businesses v. Sebelius (2012).

The Printz case serves as the cornerstone.

“We held in New York that Congress cannot compel the States to enact or enforce a federal regulatory program. Today we hold that Congress cannot circumvent that prohibition by conscripting the States’ officers directly. The Federal Government may neither issue directives requiring the States to address particular problems, nor command the States’ officers, or those of their political subdivisions, to administer or enforce a federal regulatory program. It matters not whether policymaking is involved, and no case-by-case weighing of the burdens or benefits is necessary; such commands are fundamentally incompatible with our constitutional system of dual sovereignty.”

The anti-commandeering doctrine puts state refusal to cooperate with the NSA on solid legal footing.
OffNow has developed a suite of legislation ranging from a broad and multi-faceted bill, to more narrow and specifically targeted language. This allows lawmakers to pick a strategy that works within their state’s political climate. In states open to taking aggressive action against warrantless, mass-surveillance, legislators can pursue a one-step strategy. But in other states, an incremental, multi-step approach will prove more effective.

We’ve designed the legislation with a stack of Legos in mind. Lawmakers can take it apart and put it together in a variety of ways, tailoring their approach to the specific political environment of each state.

The Fourth Amendment Protection Act

This bill serves as the cornerstone of OffNow’s legislative strategy. It stands alone as a comprehensive bill addressing illegal spying from the state level in three ways.

First, the legislation would prohibit state and local agencies from providing any material support to the NSA within their jurisdiction. That includes cutting off water, electricity and other state supplied resources.

While nine states host official NSA facilities (that we know of), this legislation is intended for introduction in all 50 states. Success will only come with passage in multiple states - both those with and without facilities. The public generally remains unaware of the NSA’s intention to build and support a facility until after the contracts are signed, and this often happens in secret. States need to take proactive steps to prevent further NSA expansion.

And should a state home to an NSA facility pass the bill, it becomes essential that neighboring states support their effort by following suit. This makes action in the facility state more effective because the federal agency can’t easily pick up and move across the border. And while monetary reality makes this difficult already (NSA internal documents reveal that their expansion has often been limited by budgetary considerations in recent years), removing the welcome mat in states where the agency does not yet have a presence creates bigger roadblocks. Our goal: to box the NSA in and make it difficult, or nearly impossible in practice, for it to expand.

Second, the legislation prohibits the receipt of warrantless information funnelled from NSA to state and local law enforcement via the DEA Special Operations Division (SOD) and fusion centers, blocking a narrow, but intrusive practical effect of federal spying. While it doesn’t stop the unwarranted collection of data by the NSA, it does dictate what the state can do with it once collected. The Fourth Amendment Protection Act makes data gathered by the feds without a warrant and shared with state agents inadmissible in state court.

Third, the NSA partners with 171 universities around the country. These schools conduct government funded research, helping the NSA expand its capabilities. They also serve as recruiting grounds for future spies. State universities would be banned from these cooperative agreements with the NSA under the Fourth Amendment Protection Act.

Electronic Data Privacy Act

Recognizing that passage of the Fourth Amendment Protection Act will prove difficult in many states, and likely involves a multi-year process, the Electronic Data Privacy Act serves as a powerful first step. By banning the use of warrantless data in court, this state legislation can thwart some of the practical effects of federal spying programs.

From documents obtained by Reuters, we know the NSA expressly shares warrantless data with state and local law enforcement through a formerly-secret unit known as the Special Operations Division (SOD). That information is being used for day-to-day criminal prosecutions, not international terrorism cases, according to the documents obtained by Reuters in late 2013.

The Electronic Data Privacy Act makes illegally collected data inadmissible in state court, and that includes warrantless data shared with state and local law enforcement by federal agencies.

States can also implement the measure through a constitutional amendment, often approved as a ballot measure.

Freedom from Drone Surveillance Act
The expanding use of drones for domestic policing at the state and local level poses significant threats to privacy. In most states, law enforcement can utilize drones with virtually no restrictions.

Drone use by state and local law enforcement also has national implications. In fact, the federal government serves as the primary engine behind the expansion of drone surveillance carried out by states and local communities. The Department of Homeland Security issues large grants to local governments so that those agencies can purchase drones. The likely goal? Fund a network of drones around the country and put the operational burden on the states. Once they create a web over the whole country, DHS steps in with requests for “information sharing,” under the PATRIOT Act or other federal acts.

The Freedom from Drone Surveillance Act not only provides immediate privacy protection to people within that state, it also puts a dent in a long-term program for seemingly endless surveillance on a federal level.

**Freedom from Location Surveillance Act**

Another narrow, but important first step against the growing surveillance state, the Freedom From Location Surveillance Act, bans state and local law enforcement from obtaining the location information of a person’s electronic device without a warrant.

We know the NSA and FBI track the physical location of people through their cellphones. In late 2013, the Washington Post reported that NSA is “gathering nearly 5 billion records a day on the whereabouts of cellphones around the world.” This includes location data on “tens of millions” of Americans each year – without a warrant.

Similar to the Electronic Data Privacy Act above, this legislation would prohibit state and local law enforcement from engaging in this practice. It would also have a direct effect on how federal agencies use this information in practice by banning the use of it in state courts.

**C.H.O.I.C.E. ACT: CORPORATE RESPONSIBILITY**

Corporations proved the most aggressive opponents of the Fourth Amendment Protection Act during the 2014 legislative session.

While many NSA locations rely heavily on state and local governments to operate, corporations also fill the gap. Defense contractors, utility companies, tech firms, construction contractors and many others willingly accept taxpayer dollars to do the NSA’s dirty work. This is, in essence, an ultra-insidious form of corporate welfare - a massive surveillance industry, funded by your tax dollars.

Follow up legislation to the fourth Amendment Protection Act would allow states to end business relationships with compliant corporations happy to profit from NSA abuses.

The C.H.O.I.C.E. Act (Creating Helpful Options for Institutions, Corporations, and Enterprise) would make corporations voluntarily enabling federal agencies engaged in illegal spying ineligible to bid for state contracts. Essentially, it would force corporations to make a choice: work with federal agencies spying on Americans, or do business with the state. When passed into law, the state would no longer officially
OUR PROGRESS

In the OffNow campaign’s first year, legislators in more than a dozen states introduced the Fourth Amendment Protection Act, including Utah and the NSA’s home state of Maryland. The campaign quickly took on a bipartisan tone, with lawmakers from both sides of the aisle sponsoring and voicing support for the legislation. In today’s hyper-partisan political sphere, this represents no small feat.

A transpartisan coalition, including many national and state organizations spearheaded by the Bill of Rights Defense Committee and the Tenth Amendment Center, helped knit together unified support from a vast array of organizations ranging from Occupy to Tea Party groups.

Because of the aggressive nature of the approach, including provisions to turn off water to the NSA data center in Bluffdale, Utah, the effort quickly garnered national and international media attention. OffNow received repeated coverage in mainstream media, including US News and World Report, the Associated Press, ABC News, CBS News, The Guardian, VICE Magazine, Mother Jones and several other national and local publications.

Politicians took notice as well. An elected member of Congress denounced the effort to turn off resources to the NSA in Maryland as “dangerous.”

A blogger at a prominent think-tank deemed the effort dangerous as well. Why? Because it can work. We consider that a green light to push forward!

The OffNow campaign jumpstarted several important media inquiries. As a direct result of our efforts in Utah, a reporter with the Salt Lake Tribune did an investigative piece on the water contract between the City of Bluffdale and the NSA, revealing the NSA got a sweetheart deal. The Tribune also forced the city to disclose actual water use at the facility. Inspired by the work of OffNow, a reporter for VICE Magazine dug into the corporate and tech industry opposition to state efforts to limit NSA spying.

The first year of the OffNow campaign was successful simply in the fact that it sparked inquiry and elevated awareness. But there was also legislative success.

In Utah, the move to turn off water to the NSA Data Center got off to a good start. Rep. Marc Roberts introduced the Fourth Amendment Protection Act, and a state House committee gave it a fair hearing. The committee voted to send the bill to “interim study” for further consideration. The legislation will receive public hearings between now and Dec. 2014 in preparation for reintroduction for the 2015 legislative session in Utah.

In California, powerful state senators Ted Lieu (D-Torrance) and Joel Anderson (R-San Diego) introduced a strategically-modified version of the Fourth Amendment Protection Act during the 2014 session.

Instead of creating a law to immediately turn off resources to the NSA, it created a mechanism and a two-step process, but also expanded the ban on material...
support or resources to any and all federal agencies engaged in these types of surveillance programs.

While, at the time of this writing, the bill won’t likely get to Gov. Brown’s desk unscathed, it did pass the State Senate in this form by a landslide. The vote was 29-1!

In Arizona and Oklahoma, this legislation was voted out of committee in full effect. In both states, Republican leadership worked behind the scenes to prevent the legislation from getting full vote on the chamber floor. Bill sponsors have indicated that they plan to introduce the legislation again in 2015.

In Maryland, home of the NSA headquarters, surveillance lobbyists, including law enforcement organizations, came out in full force to oppose the bill. Bruce Fein, a leading Constitutional-attorney and top Justice Department official during the Reagan administration, came to testify in favor of the bill.

“I think that this bill is in the finest traditions of a state government opposing federal encroachment,” Fein said. “The spirit of the Fourth Amendment bill is about restoring the Fourth Amendment in the state of Maryland and sending a signal to the federal government that the state of Maryland does not want to be complicit in the daily violation of the Fourth Amendment.”

Preliminary outreach to lawmakers in all of the states who introduced legislation last year indicates all plan to continue the fight in 2015. And with grassroots pressure, bills could also be introduced in NSA facility states like Texas, Hawaii, and Georgia and others.

Several states also considered Electronic Data Privacy acts last year. This legislation was passed in Utah and signed into law by Gov. Herbert in 2014, making it the second state in the country to pass such a measure. In early 2013, Maine got a head start, taking the first step towards enacting a similar law.

On Aug. 5, Missouri voters overwhelmingly approved a state constitutional amendment by a 75 percent margin, giving “electronic data and communications” the same state constitutional protections as “persons, homes, papers and effects.” The amendment also addresses a small practical effect of NSA spying. By prohibiting state agents from “accessing” warrantless electronic data, it makes such data gathered by federal agencies such as the NSA and shared with state and local law enforcement inadmissible in state criminal proceedings.

In 2014, bills to ban cellphone location data collection without a warrant were signed into law in a number of states, including Colorado, Maine, Montana and Utah.
ADDiTIONAL FOCUS: LOCAL

The OffNow campaign primarily focuses on action against federal surveillance programs. But with the line between federal, state and local law enforcement becoming increasingly blurred, Americans also need to pay attention to local actions to see and understand the big picture.

The expanding use of drones for domestic policing at the state and local level poses significant privacy threats. In most states, law enforcement can utilize drones with virtually no restrictions. Ten states have passed law limiting drone use, including warrant requirements and some with prohibitions on weaponization. Other states need to follow suit, and states with laws on the books can take further action to close loopholes and strengthen their provisions.

Drone use by state and local law enforcement also has national implications. In fact, the Federal government serves as the primary engine behind the expansion of drone surveillance carried out by states and local communities. The Department of Homeland Security issues large grants to local governments so that those agencies can purchase drones. The likely goal? Fund a network of drones around the country and put the operational burden on the states. Once they create a web over the whole country, DHS steps in with requests for “information sharing,” under the PATRIOT Act or other federal acts.

Fusion centers make up part of the Information Sharing Environment (ISE) a consortium that includes the NSA, FBI, Department of Defense and many others. The ISE facilitates information sharing, officially for “national defense.” But we know through leaked documents that federal agencies share large amounts of illegally gathered information with state and local law enforcement, and it has no connection with national defense at all. State and local law enforcement also share information “upstream” to these federal agencies.

With the rapid evolution of information sharing between local, state and federal law enforcement agencies, locally-gathered information won’t remain “local” for very long.

Simply put, when local governments seize the power to watch you, that information will ultimately end up in the hands of federal agencies most certainly trying to monitor the actions, communications and movement of virtually every person on earth.

Add to this an FBI facial recognition program coming online this year and you have an Orwellian nightmare scenario. As the technology improves and facial recognition “learns” to identify more people, federal agencies will gain the capability to track your every movement, in real time, through networks of cameras owned by local government and private entities, but funded by the DHS.

With the rapid evolution of information sharing between local, state and federal law enforcement agencies, locally-gathered information won’t remain “local” for very long.
CONCLUSION

Some 40 years ago, author Philip K. Dick gave a stark warning - “There will come a time when it isn’t, ‘They’re spying on me through my phone,’ anymore. Eventually, it will be, ‘My phone is spying on me.’”

After nearly four decades, we can no longer call these kinds of warnings about the surveillance state alarmist. In fact, former high level NSA technical chief William Binney said that the goal of the NSA is “total population control.”

It’s easy to think that we cannot possibly do battle with an agency so powerful, intrusive and ubiquitous. But as we’ve seen, the NSA has its Achilles Heel. Even the mighty fall. Just ask Goliath. Or Ceasar. Or the Soviet Politburo.

But we cannot shrink back in fear. We cannot become overwhelmed with pessimism. We cannot remain on the defensive. We must think creatively, act swiftly and take the offensive.

OffNow does just that. It attacks the soft underbelly of the spy-state and seeks change from the bottom up, not the top down. It bypasses the political class in D.C. and relies on state power animated by grassroots activists. Our goal is to hinder the operation of the NSA through legitimate state and local action, and force substantive changes.

We are not obligated to help the NSA, or any agency violate our rights.

In fact, it should be resisted through all legitimate means. By saying “No!” and denying the spy-state the material support and compliance it needs, we can preserve our basic civil liberties and privacy rights.

And if Rosa Parks taught us anything - it’s that saying NO can change the world.
APPENDIX: MODEL LEGISLATION

NOTE: All legislation is available for download at http://offnow.org/legislation

We understand that passing legislation depends on a variety of factors, including the political makeup of the legislature, party politics, the mood of constituents and many other variables. With this in mind, we have developed a suite of privacy-related legislation for consideration.

Bills range from the broad Fourth Amendment Protection Act prohibiting all material support or resources to the NSA to narrower bills dealing only with data sharing and location tracking that provide lower hanging fruit where a specific victory can plow the field for further action.

The legislative package was designed with a stack of Legos in mind, allowing you to put them together in a way that best fits your state’s political environment. They can be introduced singularly or in combination.

Please don’t hesitate to contact us to discuss strategy and figure out the best way to address privacy issue.

<table>
<thead>
<tr>
<th>THE LEGISLATIVE PACKAGE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 4TH AMENDMENT PROTECTION ACT</td>
<td>11</td>
</tr>
<tr>
<td>2. ELECTRONIC DATA PRIVACY ACT</td>
<td>12</td>
</tr>
<tr>
<td>3. FREEDOM FROM DRONE SURVEILLANCE ACT</td>
<td>15</td>
</tr>
<tr>
<td>4. FREEDOM FROM LOCATION SURVEILLANCE ACT</td>
<td>16</td>
</tr>
<tr>
<td>5. C.H.O.I.C.E. ACT</td>
<td>17</td>
</tr>
</tbody>
</table>
1. 4TH AMENDMENT PROTECTION ACT

Our signature model legislation, the 4th Amendment Protection Act, would ban a state from taking actions which provide “material support or resources” to warrantless federal spying programs. This includes provisioning of resources, and banning the state from using data obtained without warrant in state court.

States should pass this legislation whether they have a physical NSA facility or not. Banning the warrantless data in court will have an immediate effect. And, since the NSA rarely publicizes its plans in advance, it's essential to ensure that their ability to expand with more data center facilities around the country is restricted before they get off the ground.

NOTE: This bill can be modified for strategic considerations for your state. If you’re a legislator interested in this bill, please contact us for more information.

******

DRAFTING NOTE - change all text in (CAPS AND PARENTHESES) to be specific to your state.

Be It Enacted by the Legislature of the State of (STATE):

SECTION 1. SHORT TITLE.

This act shall be known and may be cited as the “(STATE) 4th Amendment Protection Act.”

SECTION 2. PROHIBITION ON ASSISTANCE TO FEDERAL AGENCIES ENGAGED IN ILLEGAL COLLECTION OF ELECTRONIC DATA OR METADATA

This state and its political subdivisions shall not assist, participate with, or provide material support or resources to enable or facilitate, a federal agency in the collection or use of a person's electronic data or metadata, without that person's informed consent, or a warrant, based upon probable cause, that particularly describes the person, place, or thing to be searched or seized, or in accordance with a legally-recognized exception to the warrant requirements.

SECTION 3. SEVERABILITY

The provisions of this act are hereby declared to be severable and if any provision of this act or the application of such provision to any person or circumstance is declared invalid for any reason, such declaration shall not affect the validity of the remaining portions of this act.

SECTION 4. EFFECTIVE DATE

This act takes effect upon approval by the Governor.
2. ELECTRONIC DATA PRIVACY ACT

For those states where legislators are not yet willing or able to get the full 4th Amendment Protection Act passed, the Electronic Data Privacy Act is a powerful first step. By banning the use of warrantless data in court, this state legislation can thwart some of the practical effects of federal spying programs.

******

Be it enacted by the Legislature of the state of (STATE):

Section 1. Section (NUMBER) is enacted to read:

(NUMBER) Definitions.

As used in this chapter:

(1) “Electronic communication service” means a service that provides to users of the service the ability to send or receive wire or electronic communications.

(2) “Electronic device” means a device that enables access to or use of an electronic communication service or remote computing service.

(3) “Government entity” means the state, a county, a municipality, a higher education institution, a local district, a special service district, or any other political subdivision of the state or an administrative subunit of any political subdivision, including a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, commission, or an individual acting or purporting to act for or on behalf of a state or local agency.

(4) “Remote computing service” means the provision of computer storage or processing services by means of an electronic communications system.

(5) “Stored data” means – means data or records that are in stored on an electronic device that contains:

(a) information revealing the identity of users of the applicable service, device, or program; or
(b) information about a user’s use of the applicable service, device, or program; or
(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user; or
(d) the content of a wire communication or electronic communication sent to or by the user; or
(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user’s electronic device.

(6) “Transmitted data” means data or records that are in the possession, care, custody, or control of a provider of an electronic communications service, or a remote computing service, that contains:
(a) information revealing the identity of users of the applicable service, device, or program; or

(b) information about a user’s use of the applicable service, device, or program; or

(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user; or

(d) the content of a wire communication or electronic communication sent to or by the user; or

(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user’s electronic device.

Section 2. Section (NUMBER) is enacted to read:

(NUMBER) Electronic data and metadata privacy -- Warrant required for disclosure.

(1) (a) Except as provided in Subsection (2), a government entity may not obtain the stored data, or transmitted data of an electronic device without a search warrant issued by a court upon probable cause.

(b) A government entity may not use, copy, or disclose, for any purpose, the stored data, or transmitted data of an electronic device that is not the subject of the warrant that is collected as part of an effort to obtain the stored data, or transmitted data of the electronic device that is the subject of the warrant in Subsection (1)(a).

(c) The data described in Subsection (1)(b) shall be destroyed in an unrecoverable manner by the government entity no later than 24 hours after the data is collected.

(2) A government entity may obtain the stored data, or transmitted data of an electronic device without a search warrant:

(a) with the informed, affirmative consent of the owner or user of the electronic device; or

(b) in accordance with judicially recognized exceptions to warrant requirements; or

(c) if the owner has voluntarily and publicly disclosed stored data or transmitted data.

Section 3. Section (NUMBER) is enacted to read:

(NUMBER) Notification required – Delayed notification.

(1) Notice must be given to the user whose stored data, transmitted data, or electronic device was searched or obtained by a government entity.

(2) Unless delayed notice is ordered pursuant to subsection (3), the government entity shall provide notice to the user whose electronic device was searched or whose stored data or transmitted data was obtained by a government entity within three days of obtaining the stored data or transmitted data or conducting the search. The notice must be made by service or delivered by registered or first-class mail, email, or any other means reasonably calculated to be effective as specified by the
court issuing the warrant. The notice must contain the following information:

(a) the nature of the law enforcement inquiry, with reasonable specificity;

(b) the stored data or transmitted data of the user that was supplied to or requested by the governmental entity and the date on which it was provided or requested;

(c) if stored data or transmitted data was obtained from a provider of electronic communication service or other third party, the identity of the provider of electronic communication service or the third party from whom the information was obtained; and

(d) whether the notification was delayed pursuant to subsection (3) and, if so, the court that granted the delay and the reasons for granting the delay.

(3) A government entity acting pursuant to Section (NUMBER) may include in the application for a warrant a request for an order to delay the notification required pursuant to this section for a period not to exceed ninety days. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result. Upon expiration of the period of delay granted pursuant to this subsection and any extension granted pursuant to subsection (4), the government entity shall provide the user a copy of the warrant together with a notice pursuant to subsections (1) and (2).

(4) A government entity acting pursuant to Section (NUMBER) may include in its application for a warrant a request for an order directing a provider of electronic communication service to which a warrant is directed not to notify any other person of the existence of the warrant for a period of not more than ninety days. The court shall issue the order if the court determines that there is reason to believe that notification of the existence of the warrant may have an adverse result. Absent an order to delay notification or upon expiration of the period of delay, a provider of electronic communication service to which a warrant is directed may provide notice to any other person.
3. FREEDOM FROM DRONE SURVEILLANCE ACT

Passing legislation to limit drone use at the state level not only provides immediate privacy protection to people within that state, it also puts a dent in a long-term program for seemingly endless surveillance at the federal level. This bill bans the use of drones by state and local law enforcement to gather information without a warrant in most cases. It also prohibits weaponized drones, and establishes rigid requirements for transparency, and documentation of state drone use. With the federal government working hard behind the scenes to create a network of drones across the United States and aggressively seeking to share information with state agencies, this legislation also serves to thwart one pillar of the federal spy-state.

*******

For the latest version of this legislation, please visit [http://offnow.org/legislation](http://offnow.org/legislation)
4. FREEDOM FROM LOCATION SURVEILLANCE ACT

A narrow, but important first step against the growing surveillance state, the Freedom From Location Surveillance Act bans state and local law enforcement from obtaining the location information of a person's electronic device without a warrant. The NSA is tracking the physical location of people through their cellphones. In late 2013, the Washington Post reported that NSA is “gathering nearly 5 billion records a day on the whereabouts of cellphones around the world.” This includes location data on “tens of millions” of Americans each year – without a warrant.

******

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF (STATE):

Section 1. Location information privacy -- civil penalty.

(1) Except as provided in subsection (2), a government entity may not obtain the location information of an electronic device without a search warrant issued by a duly authorized court.

(2) A government entity may obtain location information of an electronic device under any of the following circumstances:

(a) the device is reported stolen by the owner;
(b) in order to respond to the user’s call for emergency services;
(c) with the informed, affirmative consent of the owner or user of the electronic device; or
(d) there exists a possible life-threatening situation.

(3) Any evidence obtained in violation of this section is not admissible in a civil, criminal, or administrative proceeding and may not be used in an affidavit of probable cause in an effort to obtain a search warrant.

(4) A violation of this section will result in a civil fine not to exceed $50.

Section 2. Definitions.

As used in [section 1] and this section, the following definitions apply:

(1) “Electronic communication service” means a service that provides to users of the service the ability to send or receive wire or electronic communications.

(2) “Electronic device” means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.

(3) “Government entity” means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for or on behalf of a state or local agency.

(4) “Location information” means information concerning the location of an electronic device that, in whole or in part, is generated or derived from or obtained by the operation of an electronic device.

(5) “Location information service” means the provision of a global positioning service or other mapping, locational, or directional information service.

(6) “Remote computing service” means the provision of computer storage or processing services by means of an electronic communications system.
5. C.H.O.I.C.E. ACT

While government agencies primarily drive the surveillance state, in many cases, private corporations enable NSA spying as well. Corporations willingly providing the NSA with essential services enable the agency to carry out the largest privacy violations in the history of the world. While a state cannot stop a private entity from helping the federal government violate your rights, it can choose not to do business with such an organization. The C.H.O.I.C.E. Act (Creating Helpful Options for Institutions, Corporations, and Enterprise) does just that. The bill bars corporations enabling federal spying from winning state contracts. This legislation gives corporations a choice, either do business with spies, or do business with us.

DRAFTING NOTE - change all text in (CAPS AND PARENTHESES) to be specific to your state.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF (STATE):

Section 1. Short Title. This Act may be cited as the ‘Creating Helpful Options for Institutions, Corporations, and Enterprise (C.H.O.I.C.E. Act) Act of (YEAR)’.

Section 2. The legislature finds and declares all of the following:

(A) The bulk collection of electronic data or metadata of the people of the State of (STATE), without, informed, affirmative consent, or a warrant based upon probable cause, and particularly describing the person, place or thing to be searched or seized, or acting in accordance with a legally-recognized exception to the warrant requirements, constitutes an unreasonable search and seizure and violates the right to privacy of the People of this state.

(B) It is this State's prerogative to freely choose to award contracts to those corporations and other business entities that do not actively and voluntarily assist in the violation of the right to privacy of the People of this state as described in Section 2(a).

(C) It is the policy of this state to refuse to award contracts to those corporations and other business entities that are found to be actively, knowingly, and voluntarily assisting, or providing material support or resources to, the bulk collection of electronic data and metadata of the people of the State of (STATE), without:

   (1) Informed, affirmative consent of the person or persons whose electronic data or metadata is being collected, or;

   (2) A warrant based upon probable cause, and particularly describing the person, place or thing to be searched or seized, or;

   (3) Acting in accordance with a legally-recognized exception to the warrant requirements.

Section 3. Procurement, service, and other contracts prohibited to entities facilitating privacy violations.

(A) Upon an official determination by a court of this state that a corporation or other business entity is actively, knowingly, and voluntarily assisting, or providing material support or resources to, the bulk collection of electronic data and metadata of the people of the State of (STATE) without, informed, affirmative consent, or a warrant based upon probable cause, and particularly describing the person, place or thing to be searched or seized, or acting in accordance with a legally-recognized exception to the warrant requirements, this state and its political subdivisions shall not:

   (1) Contract for any new business with the corporation or other business entity found to be in viola-
tion of Section 3(a).

(2) Renew or extend any existing contract with the corporation or other business entity found to be in violation of Section 3(a).

(B) Nothing in this section shall be construed to:

(1) Prohibit any corporation or other business entity from cooperating with federal authorities when required under federal law, or

(2) Create any power, duty or obligation in conflict with any federal law.

Section 4. Corporate Certification

(A) A corporation or other business, prior to entering into a contract with the State of (STATE), or with a political subdivision of the State of (STATE), must execute a certification, under oath, subject to the penalty of perjury, and file it with the Secretary of State, on a form provided by the secretary of state, affirming that it is not actively, knowingly, and voluntarily assisting or providing material support or resources to the bulk collection of electronic data and metadata of the people of the State of (STATE), without:

(1) Informed, affirmative consent of the person or persons whose electronic data or metadata is being collected, or;

(2) A warrant based upon probable cause, and particularly describing the person, place or thing to be searched or seized, or;

(3) Acting in accordance with a legally-recognized exception to the warrant requirements.

(B) Said certification is and shall be considered an ongoing affirmation until rescinded or until the expiration of the corporation's or other business entity's contractual relationship with the State of (STATE) or a political subdivision of the state of (STATE).

(C) A corporation or other business may at any time rescind said certification by serving the Secretary of State with notice, and the Secretary of State shall immediately forward a copy thereof to the Attorney General.

Section 5. Enforcement.

(A) An agency of this state or a political subdivision of this state may not receive state grant funds if the agency or political subdivision is found to have, by consistent actions, actively, knowingly and voluntarily violated Section 3 of this Act.

(1) State grant funds for the agency or political subdivision shall be denied for the fiscal year following the year in which a final judicial determination in an action brought under this section is made that the agency or political subdivision has by consistent actions, actively, knowingly and voluntarily violated Section 3 of this Act.

(B) Any citizen residing in the jurisdiction of this state or a political subdivision of this state may file a complaint with the attorney general if, at the time of the complaint, the citizen offers evidence to support an allegation that the state or political subdivision has adopted a rule, order, ordinance, or policy under which the state or political subdivision violates Section 3 of this Act.
(C) If the attorney general determines that a complaint filed under Section 4(B) of this act against this state or a political subdivision of this state is valid, the attorney general may file a petition for a writ of mandamus or apply for other appropriate equitable relief in a district court in which the principal office of the state or political subdivision of this state is located to compel the state or political subdivision to comply with Section 3 of this Act.

(1) The attorney general may recover reasonable expenses incurred in obtaining relief under this Section, including court costs, reasonable attorney’s fees, investigative costs, witness fees, and deposition costs.

(D) The attorney general may defend any agency or political subdivision of this state that the federal government attempts to sue or prosecute for an action or omission consistent with the requirements of this section.

Section 6. Severability

The provisions of this act are hereby declared to be severable and if any provision of this act or the application of such provision to any person or circumstance is declared invalid for any reason, such declaration shall not affect the validity of the remaining portions of this act.

Section 7. Effective Date

This act takes effect upon approval by the Governor.