Background

In the wake of 9/11, Congress rushed to pass a wave of national security legislation that has since been used to conduct mass surveillance of American citizens’ phone and internet data. Since then, Congress and the public have learned how the authorities granted in those laws have been used in ways that Congress never intended or foresaw, and that represent a massive expansion of the government’s surveillance of U.S. persons. Unfortunately, the conversation about reforming those important pieces of legislation has typically pitted privacy against national security concerns.

Mass surveillance of U.S. persons is permitted and conducted under a three-part surveillance architecture: the USA PATRIOT Act of 2001, the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, and Executive Order 12333. Unless these measures are radically changed, mass surveillance of citizens, including programs that target the Arab American and American Muslim communities as well as activists in other movements like Black Lives Matter, will continue. Many of these surveillance programs violate the Fourth Amendment by allowing the government to affect Fourth Amendment searches without a warrant or showing of probable cause. It has also been proven that the knowledge of government surveillance has a deeply troubling chilling effect on citizens’ private and public behaviors.

The most significant piece of legislation passed was the USA PATRIOT Act, which enormously expanded the government’s surveillance powers over U.S. citizens and non-citizens alike. With the proliferation of internet-based communications since the passage of the PATRIOT Act, its scope has grown in unanticipated ways and has forcefully challenged the long-held legal principal of a “reasonable expectation of privacy” which is a test used to determine when the government is required to obtain a search warrant for private communications. Programs permitted under the PATRIOT Act have had grave consequences for individual freedoms, including for Arab Americans and American Muslims who have been targeted by FBI informant programs, and watch listed without the ability to contest that designation.

Following several high profile intelligence leaks regarding U.S. surveillance programs, there has been growing support for reform - both from the public at large who is uncomfortable with the willful complicity of internet and phone companies with the government’s bulk data collection programs, and from communities like Arab Americans and American Muslims who have been targeted under these programs. Last year, a debate over surveillance reform ensued in the days leading up to the expiration of Section 215, a key provision of the PATRIOT Act. This provision provided the legal basis for domestic surveillance programs that affect ordinary Americans living in the U.S. While a Senate floor fight lead to the expiration of the problematic Section 215, soon after its expiration, the Senate passed a compromise bill called the USA FREEDOM Act to restore in modified form several PATRIOT Act provisions. The expiration of Section 215 and passage of the USA FREEDOM Act were important first steps in rolling back the illegal and ineffective bulk collection of data. However, the USA FREEDOM Act, or “PATRIOT Act 2.0” still permits mass surveillance.

The Problem

The post-9/11 understanding of surveillance has pitted privacy against national security concerns. Reform efforts have correctly set out to reframe the discussion around surveillance programs so that there is a greater balance between credible surveillance programs and the constitutional right to privacy for all U.S. citizens. Once again, however, we are seeing how events in the Middle East have tremendous implications on the protection of civil rights and civil liberties domestically. Now, surveillance powers are being emphasized as important tools for the fight
In order to protect Arab Americans, American Muslims, and all Americans from intrusive and unconstitutional surveillance, the legality of mass surveillance must be challenged and we must demand greater transparency from intelligence agencies. Some of the key loopholes and trends that permit mass and targeted surveillance include:

- The USA FREEDOM Act - although hailed as a “reform” to the PATRIOT Act - did not go far enough to protect the warrantless, indiscriminate surveillance of American persons by the National Security Administration (NSA). The modest reforms made by the 2015 USA FREEDOM Act change the procedure by which the government searches metadata troves, but it does not address the massive intelligence dragnet that is created by the NSA’s foreign surveillance programs. And while USA FREEDOM makes a small gesture towards greater transparency, it does not significantly improve the public’s understanding of how the government is spying domestically.

- Section 702 of the FISA Amendment Act of 2008 permits the NSA to collect the contents of communications, called metadata. Even though it’s ostensibly used for foreign targets, Section 702 surveillance sweeps up the communications of Americans, and the NSA has acknowledged that it searches this information without a warrant for the communications of Americans. The Section will expire in December 2017 and will certainly be proceeded by a policy debate about whether to reauthorize, reform, or sunset the authority it provides. This is an opportunity for Members of Congress and surveillance reform activists to find a better balance between lawful surveillance of foreign threats and protection of Americans’ right to privacy and warrantless search and seizure.

- Executive Order 12333 essentially explains how the President can order his/her Administration - including the 17 intelligence agencies - to spy on foreigners and any U.S. person without Congressional or Judicial approval and oversight. Through leaked information, the public has learned that EO 12333 is being used as the legal basis for surveillance programs which sweep up metadata on U.S. citizens in their expansive dragnets without a probable cause warrant. The lack of Congressional or Judicial oversight of Executive Order 12333 programs means that no one except the President knows the true scope of surveillance programs that the U.S. government is using domestically and internationally.

- Specific Arab American community surveillance concerns:
  - The Obama Administration’s introduction of “Countering Violent Extremism” – as a concept for domestic counterterrorism and as a $10 million undertaking of the Department of Homeland Security – have thus far amounted to discriminatory surveillance of Arab Americans and American Muslims. CVE’s two main programs threads, community engagement and social media campaigns, are surveillance initiatives by a different name. Demonstratively, the FBI recently announced
they are rolling out “Shared Responsibility Committees” (SRCs) as part of CVE efforts. SRCs are a version of the FBI’s confidential informant program that seeks to empower community members to conduct surveillance and report their own community members who they conclude are at risk for becoming violent extremists to the FBI. This intrusive surveillance initiative further marginalizes and unravels American Muslims and the communities they live in. See the CVE issue brief for further information.

Leaked reports about information sharing practices between the National Security Agency (NSA) and the Israeli SIGINT National Unit (ISNU) are concerning. A report of a “Memorandum of Understanding” between NSA and ISNU revealed that ISNU receives unfiltered data on various communications, emails, and phone calls made by American citizens. Some of these communications include those made by Arab and Palestinian Americans domestically. These information-sharing practices violate the civil liberties of our community. Necessary safeguards must be implemented to protect Americans, regardless of background, against bulk data collection that can be utilized by foreign governments, including Israel.

**Moving Forward**

In order to achieve a better balance between necessary national security surveillance programs and constitutionally guaranteed rights, we are encouraging Congress and the Obama Administration to:

- Support legislation that builds on the reforms of the USA FREEDOM Act requiring greater transparency and accountability around surveillance activities which implicate American citizens. Congress should take up greater oversight of surveillance activities, and the White House should proactively seek ways to better educate the public about its privacy protections in regard to surveillance objectives.

- Allow Section 702 of the FISA Amendments Act to expire in 2017.

- When Section 702 of the FISA Amendments Act is up for reauthorization in 2017, support aggressive reform efforts that promote greater transparency and more vigorous privacy protections so that innocent American citizens are not caught in the foreign surveillance dragnet.

- Oppose the Senate’s “Compliance with Court Orders Act.”

- Support the FOIA Improvement Act.

- Urge the DHS and ODNI Offices of Civil Rights and Civil Liberties to implement Privacy and Civil Liberties Oversight recommendations on data collection, retention, and sharing.

- Pressure the Department of Justice to uphold the rights and equal protection of Arab Americans and American Muslims. This includes ending the discriminatory surveillance initiatives the Department of Homeland Security runs through “Countering Violent Extremism” and minimizing metadata shared with foreign governments.