

KEN MONTENEGRO AND STEVEN RENDEROS SECURITY 08.08.17 10:00 AM

# WARRANTLESS US SPYING IS SET TO EXPIRE SOON. LET IT DIE



GETTY IMAGES

**SURVEILLANCE TECHNOLOGIES HAVE** historically restricted the freedoms of communities of color and immigrants in this country. This history continues today through a resurgent national security apparatus with emboldened nationalist tendencies. Members of Congress have the power to rein these surveillance mechanisms. At this moment, Section 702 of the Foreign Intelligence Surveillance Act (FISA) is pending reauthorization from Congress. This piece of legislation must be reformed in order to prevent dragnet surveillance, backdoor searches of phone and email records, and unlawful targeting of communities of color and immigrant communities. Unless these revisions are made, Congress should let the provision expire.

## WIRED OPINION

### ABOUT

Ken Montenegro (@kmontenegro) is national vice president of the National Lawyers Guild in New York. Steven Renderos (@stevenrenderos) is organizing director at the Center for Media Justice in Oakland, California.

---

Section 702 allows for warrantless surveillance of conversations between people in the US and in foreign countries. The law passed in 2008 during the George W. Bush's presidency, was extended by the Obama administration, and is now set to expire at the end of 2017, unless Congress reauthorizes the provision—a move the Trump administration supports.

Rebuttals to questions of surveillance often go something like this: 'If you've got nothing to hide, then you shouldn't be worried.' But a review of American history points to the same groups being routinely spied on by the government: black and native bodies, immigrants, poor communities, and anybody deemed as an "other" or a threat to national security. High-profile cases of surveilled prominent figures include civil rights leaders [Martin Luther King Jr.](#) and [Cesar Chavez](#), who were both monitored by the FBI.

More recently, [cities like Baltimore](#) experienced dragnet surveillance after protesting against the police murder of Freddie Gray. [Black Lives Matter](#) activists in Ferguson, Missouri became [targets of surveillance](#). Muslim communities have long [withstood surveillance of their neighborhoods, mosques, and community leaders](#). If history is any indicator, the net cast on those suspected of being threats to our nation's safety is vast—and in a time where much of the nation is intent on resisting and dissenting, this puts much of the country at risk of being surveilled. Furthermore, surveillance, particularly enabled under 702, is [nefariously opaque](#).

---

## RELATED STORIES

---

LILY HAY NEWMAN

The Attack on Global Privacy Leaves Few Places To Turn

---

JENNIFER STISA GRANICK

Mass Spying Isn't Just Intrusive---It's Ineffective

---

BRIAN BARRETTDon't Buy the Latest Trump Surveillance Hype

---

Proponents of Section 702, such as the [Heritage Foundation](#), and Trump's homeland security and counterterrorism advisor Thomas Bossert, argue that oversight protocols and existing language in the provision will prevent significant overreach. In an op-ed in the *New York Times* published earlier this year, Bossert [claimed](#) that Section 702 doesn't allow for targeting of US citizens, emphasizing that the provision "expressly forbids intentional targeting" and that an individual court order supported by probable cause is needed to surveil citizens and foreigners inside the US.

But newly declassified memos [reviewed by The Hill](#) revealed a slew of violations by the NSA and FBI during the Obama administration, proving that although intentional targeting of US citizens may not be allowed, citizens' data is nonetheless being intercepted—and searched. Among the various violations cited in the memo are "numerous overcollection incidents," and "the misuse of overly broad queries or specific US person terms to search through NSA data."

Immigrants are also largely at risk of being surveilled through Section 702's so-called [upstream monitoring](#), which allows communication to a friend or family member outside of the country (or browser history, chat logs), to be searched for potential "selectors" or keywords of interest. This means that more than a quarter of the US population—more than 84 million people—are at risk of having their data intercepted.

We recently visited our nation's capitol with a delegation of community leaders and policy advocates from across the country to meet with Senators Al Franken (D-MN), Kamala Harris (D-CA), and Ron Wyden (D-OR), along with Representatives Justin Amash (R-MI) and Keith Ellison (D-MN), to discuss the impacts of new surveillance technologies on immigrant communities and religious minorities. Among the solutions proposed was to reform Section 702 to close the backdoor search loophole, and prevent overly broad law enforcement from being used to target immigrants and citizens of color, religious minorities, and activists.

liberties groups including the ACLU and Color of Change to send [a letter](#) to the House Judiciary Committee recommending reforms to the provision. History shows that intelligence programs without adequate oversight, demonstrated by [COINTELPRO](#) and the contents of the [Edward Snowden](#) revelations, inevitably overstep their mandates.

Congress should recall the origins of the fourth amendment in this moment: Let's stop putting mass surveillance technologies in the hands of intelligence agencies, especially with nothing but the misplaced hope they will do the right thing.

*Ken Montenegro ([@kmontenegro](#)) is national vice president of the National Lawyers Guild in New York. Steven Renderos ([@stevenrenderos](#)) is organizing director at the Center for Media Justice in Oakland, California. WIRED Opinion publishes pieces written by outside contributors and represents a wide range of viewpoints. [Read more opinions here.](#)*

---

## RELATED VIDEO

---



---

SECURITY

## incognito windows

Thanks to an assist from Congress, your cable company has the legal right to sell your web-browsing data without your consent. This is how to protect your data from preying eyes.

#SURVEILLANCE #CONGRESS #FISA

[VIEW COMMENTS](#)

## SPONSORED STORIES

POWERED BY OUTBRAIN



AMERICANPATRIOTLIFE

Green Drink Turning Seniors Into "Young Bucks"



BUSINESS INSIDER

Absolutely the Best Sheets You'll Ever Sleep in



BABEL

How this app made by 100 linguists gets you speaking a new language in 3 weeks



HONEY

You should never shop on Amazon without using this trick - here's why



HUBBLE CONTACTS

These Two Guys Are Disrupting The Contact Lense Industry



FIRSTLEAF

Your \$20 Bottle of Wine is Worth \$3

---

# MORE SECURITY

---

CYBERSECURITY

## **All the Ways US Government Cybersecurity Falls Flat**

LILY HAY NEWMAN

---

DON'T PANIC

## Your Handy Guide to the Many Tech Anxieties of Our Time

---

BUSINESS

## Sorry, Banning 'Killer Robots' Just Isn't Practical

TOM SIMONITE

---

SECURITY

---

HACKS

## Watch Hackers Hijack Three Robots for Spying and Sabotage

ANDY GREENBERG

---



FICTION

## What if All Your Secrets Went Public?



---

## GET OUR NEWSLETTER

---

WIRED's biggest stories delivered to your inbox.

Enter your email

---

SUBMIT

---

## FOLLOW US ON YOUTUBE

---

Don't miss out on WIRED's latest videos.

---

FOLLOW

ADVERTISE	SITE MAP
PRESS CENTER	FAQ
ACCESSIBILITY HELP	CUSTOMER CARE
CONTACT US	SECUREDROP
T-SHIRT COLLECTION	NEWSLETTER
WIRED STAFF	JOBS
RSS	

#### CNMN Collection

Use of this site constitutes acceptance of our user agreement (effective 3/21/12) and privacy policy (effective 3/21/12).

Affiliate link policy. Your California privacy rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.

































