



IRS Chief Acknowledges Use of ‘Stingray’ E-Surveillance Program

Kimberly Morin

December 4, 2015

In testimony before the U.S. Senate Finance Committee, Internal Revenue Service Commissioner John Koskinen revealed the tax collection agency’s use of “Stingrays” and other spy hardware designed to facilitate easy electronic surveillance and monitoring of citizens’ private data.

Stingrays mimic cell phone towers by broadcasting signals to cell phones in the area. After a phone connects to the Stingray, government agents can intercept text messages, stop phone service, and record voice conversations.

Secrets and Spy Gadgets

Andrew Crocker, an attorney with the Electronic Frontier Foundation, says government agencies have historically been unwilling to explain how or why they use Stingrays.

“There has been intense secrecy around Stingrays in general,” Crocker said. “It has led judges to get very fed up. I think the IRS’ secrecy is simply part of the larger unwillingness of the government to provide transparency about Stingray use.”

Calls for More Information

Crocker says lawmakers need more information about the IRS spy program.

“I would say we’d need to see some oversight and reporting on how broadly the IRS interprets this type of investigation and numbers for how often Stingrays are actually used,” Crocker said. “That might give us a better basis to judge the IRS’ claims.”

Eyes on You

Adam Bates, a policy analyst with the Cato Institute's Project on Criminal Justice, says government agencies' rationales for prying into law-abiding citizens' lives are often flimsy.

"It's not just the IRS," Bates said. "The Stingray device has been shrouded in government secrecy for its entire operational history. The typical arguments for the secrecy are that terrorists or drug kingpins will be able to evade surveillance if they know how the devices function, but that's never been a very persuasive argument.

"Terrorists and drug kingpins figured out long ago that their cell phones were liabilities, and the data we have on how these devices are employed by law enforcement on a daily basis suggests that they're entirely used for routine law enforcement matters that do not require this extreme lack of transparency," Bates said.

Constitutional Issues

Bates says lawmakers should press IRS officials for more answers about their in-house spy program.

"Again, it's hard to prove because so little is known about how the IRS is using them, but the devices are capable of sweeping up troves of personal data, from the surveillance target and innocent bystanders alike," Bates said. "When used without a warrant for routine police work, there is a serious constitutional issue here."