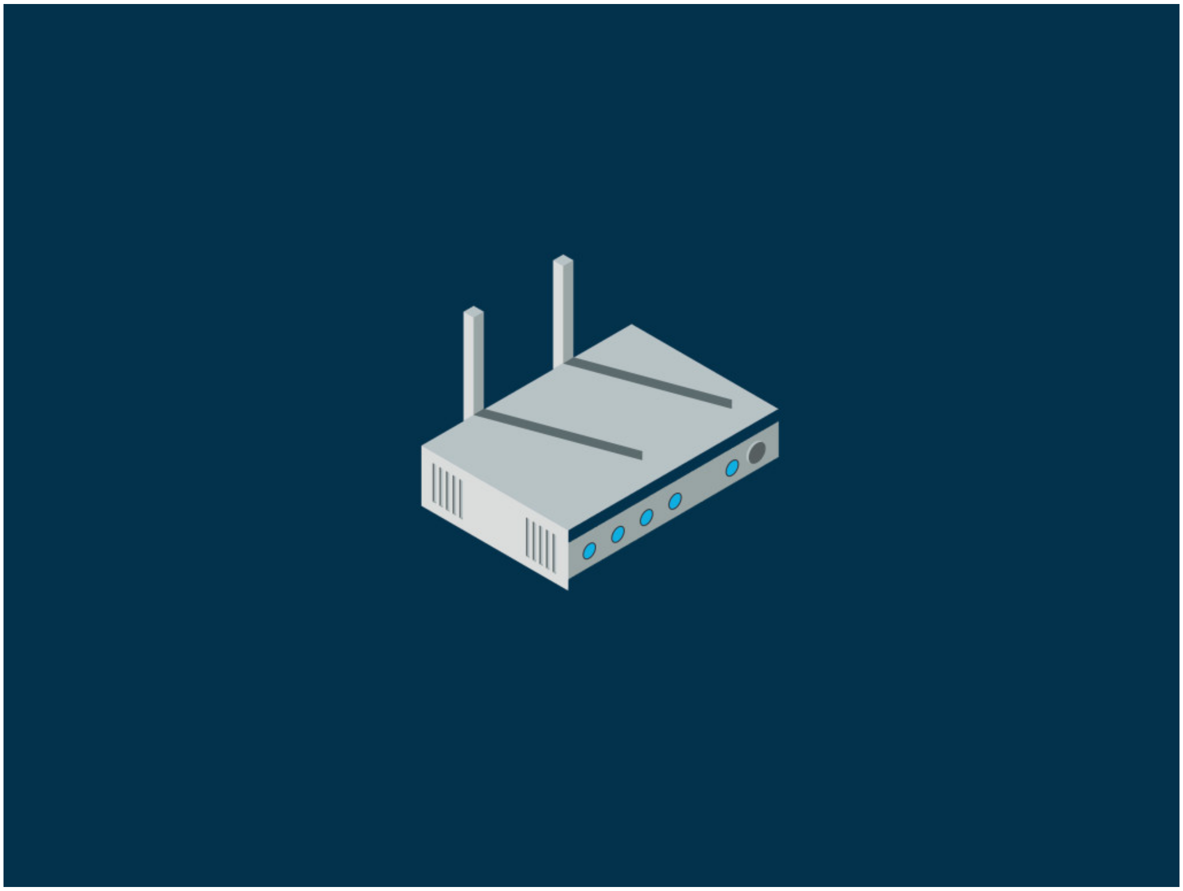
KYLE WIENS SECURITY 03.23.16 7:00 AM

WAY TO GO, FCC. NOW MANUFACTURERS ARE LOCKING DOWN ROUTERS



GETTY IMAGES

SHARE

473

1

91

because custom router firmware is actually a really good thing? Sure, it's fun to improve your router by extending the range or making your network friendlier for guests. But open firmware is important for other reasons: it enables critical infrastructure, from emergency communications for disaster relief and building free community access points to beefing up personal security.

Well, there goes that. Because even though the FCC said its new requirements were not intended to lock down router software or block the installation of open source firmware, at least one large manufacturer has reacted by doing just that. And more could follow.

Way to go, FCC.

Last month, Libre Planet—a free software community—raised the alarm that TP-Link, one of the largest router manufacturers, had begun locking down firmware in newly released routers. As proof, Libre Planet pointed to a transcript of a support conversation. In the chat, a TP-Link rep says that the lockdown—which blocks the installation of open source firmware—was a reaction to new FCC requirements.

That's a problem, because alternative router software packages like DD-WRT are hugely popular. These tools provide more sophisticated features and faster security patches than confirm whether their support chat rep was correct. The company directed us to a new FAQ page confirming the lockdown. The FAQ reads,

Why is TP-LINK limiting the functionality of its routers?
TP-LINK is complying with new FCC regulations that require manufacturers to prevent certain firmware customizations on wireless routers.”

SHARE

473

1

91

WIRED OPINION

ABOUT
Kyle Wiens is the co-founder and CEO of iFixit, an online repair community and parts retailer internationally renowned for their open source repair manuals and product teardowns.

Foreseeable Consequences

What exactly are these regulations? The FCC recently updated its requirements for “U-NII devices operating on the 5 Ghz bandwidth”—a designation that covers a wide range of Wi-Fi devices and routers—to stop users from modifying RF (radio frequency) devices outside of their intended parameters. Last year, the FCC proposed an expansion on the RF modding prohibition to anything with a software-defined radio.

The wording of the rules was met with concern that the FCC was functionally mandating

SHARE

473

1

91

guidance asking manufacturers to "describe in detail how the device is protected from 'flashing' and the installation of third-party firmware such as DD-WRT." DD-WRT is a popular open source firmware available for many consumer routers.

Thousands of people lodged complaints with the FCC, urging the organization to take steps to protect open source software. The outcry prompted an official response from the FCC soon after.

"Were we mandating wholesale blocking of Open Source firmware modifications? We were not," Julius Knapp—Chief of the FCC's Office of Engineering & Technology—explained in a blog post. He went on, "I'm pleased that this issue attracted considerable attention and thoughtful submissions into the record and would like to make it clear that the proposal is not intended to encourage manufacturers to prevent all modifications or updates to device software."

The FCC even changed the troublesome wording in their compliance documents—omitting any reference to 'third-party software' and 'DD-WRT.'

Goodbye to Third-Party Software

Despite the reassurances, experts were quick to point out that it would be easier, quicker, and

"Routers are built around a System on Chip, with the CPU and radio in a single package," Hackaday's Brian Benchoff explains. "The easiest way to prevent modification of the radio module would be to prevent modification to the entire router. Some would call it fear mongering, but there was an expectation these proposed FCC rules would inevitably lead to wireless routers being completely locked down."

It looks like those fears were warranted. Locking that firmware down seems to be what TP-Link just did. TP-Link also issued this statement:

> The FCC requires all manufacturers to prevent [the] user from having any direct ability to change RF parameters (frequency limits, output power, country codes, etc.) In order to keep our products compliant with these implemented regulations, TP-LINK is distributing devices that feature country-specific firmware. Devices sold in the United States will have firmware and wireless settings that ensure compliance with local laws and regulations related to transmission power.
>
> As a result of these necessary changes, users are not able to flash the current generation of open-source, third-party firmware. We are excited to see the creative ways members of the open-source community update the new firmware to meet their needs. However,

SHARE

473

1

91

The company appears to be using this as an excuse to wash its hands of third-party software. Even though the FCC's rules only require the manufacturer to prevent modifications to the RF parameters—not to prevent the installation of third-party firmware.

"TP-Link appears to be citing its own interpretation of a proposed FCC policy change—an interpretation the FCC has expressly rejected—as an excuse to lock down its devices," says John Bergmayer, Senior Staff Attorney specializing in telecommunications at Public Knowledge. "It's bad enough when companies go out of their way to put unnecessary restrictions on their customers. But it's just galling when they pretend they are somehow 'required' to do so. But even when complying with actual legal requirements, companies should do it in a way that does not put unnecessary restrictions on consumers."

And while it's reasonable to ask home hackers and hobbyists not to modify RF parameters in ways that would throw it out of compliance—instituting a wholesale router lockdown is tantamount to throwing the baby out with the bathwater. Sure, you could write custom code to hop onto an unauthorized band. With a little hardware modding to stop users from turning routers into a physical weapons. “There’s only so much a company can or should do to prevent theoretical bad behavior,” Bergmayer added.

A Domino Effect

In the meantime, going over and above the FCC’s rules means TP-Link is pushing the door closed on a lot of the beneficial applications of third-party firmware—including personal security. Open source firmware tends to be more rigorously scrutinized, updated, and secured. Worse, this precedent makes it likely that other manufacturers will take the easy route and lock down their routers as well.

“It’s a sad state of affairs, but custom firmware will eventually be loaded onto these routers; it’s just a little harder now and slightly more absurd,” Hackaday’s Benchoff goes on to say.

Requiring owners to jump through hoops to install better software on their routers is absurd. But jumping those particular hoops may also be illegal: breaking digital locks over firmware goes against anti-circumvention measures in the Digital Millennium Copyright Act. Which could make hacking these new routers a punishable offense. It’s unlikely that a manufacturer would go after a single hobbyist who hacks her router open source router software.

SHARE

473

1

91

TP-Link directs customers who have concerns about the changes to contact the FCC, which is pretty much a way to say “Don’t blame us, blame them.” And Libre Planet, for one, is planning to fight the FCC on its new rules, calling them “a major security and privacy threat which will lead to even buggier and more insecure wireless hardware.”

Fixing the Bigger Problem

Of course, there’s still that pesky issue of copyright law to deal with. Specifically—why in the world is putting different firmware on your own router potentially a violation of US copyright law in the first place? Because the DMCA is an even more horrible rule than the FCC’s new router guidelines. Fortunately, some forward-thinking lawmakers are trying to fix copyright law—including Zoe Lofgren (D, CA), who has been working to move the Unlocking Technology Act through Congress for the last few years. And Blake Farenthold (R, TX) has introduced YODA, a bill that reaffirms your property rights for firmware.

Still, unless the FCC, Congress, or manufacturers make some serious changes quickly, new routers could come with a brand new feature that you

SHARE

473

1

91

#DIGITAL MILLENNIUM COPYRIGHT ACT #FCC

#HACKS AND CRACKS #ROUTERS #TP-LINK

#WIRED OPINION

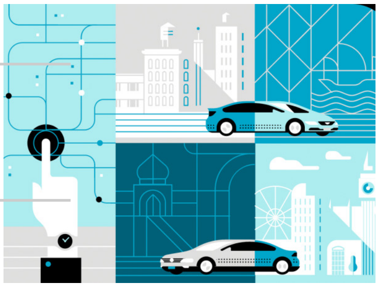
VIEW COMMENTS

SHARE

473

1

91

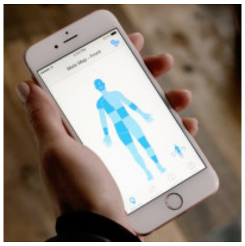


SECURITY

Uber Will Pay $10,0… 'Bug Boun…

1 DAY

...



ANALYSIS

Apple's CareKit Is the Best Argument Yet for Strong Encryption

2 DAYS

CYBERCRIME

Hacker Lexicon: A Guide to Ransomware,

09.17.15

WE RECOMMEND

JULIA GREENBERG

You Just Won the Lottery. Now Here's What You Do: Nothing

MARGARET RHODES

Playboy Trades Nipples for Good Design, and It Works

KLINT FINLEY

In Europe, You'll Need a VPN to See Real Google Search Results

SARAH ZHANG

The Hunt for Secret Nuclear Tests Digs Up Scientific Gold

SHARE

473

1

91