

The New York Times

Facebook Says It's Policing Fake Accounts. But They're Still Easy to Spot.



I saw that many of the accounts were covering the U.S. elections on all of the social networks.



How do bots and trolls work to infiltrate social media platforms and influence U.S. elections? We take a closer look at these insidious online pests to explain how they work.
Oct. 31, 2017 | Image by Aaron Byrd/The New York Times

By Scott Shane (<http://www.nytimes.com/by/scott-shane>) and Mike Isaac (<http://www.nytimes.com/by/mike-isaac>)
Nov. 3, 2017

WASHINGTON — Executives of Facebook, Twitter and Google pledged to Congress this week to do more to prevent the fakery that has polluted their sites. “We understand that the people you represent expect authentic experiences when they come to our platform,” Colin Stretch, the general counsel of Facebook, told the Senate Intelligence Committee. He said the company was doubling its review staff to 20,000 and using artificial intelligence to find more “bad actors.”

Mr. Stretch, meet Keven S. Eversley (<https://www.facebook.com/aleksandar.teovski.7>). Mr. Eversley’s Facebook profile informs us that he is from Minneapolis. But a glance at the web address for his profile reveals a different name: Aleksandar Teovski. And nearly all of his Facebook friends, his family photographs, his alma mater and even his employer are in Macedonia, a center for internet fakery.

Despite months of talk about the problem of fraud facing Facebook and other tech companies, and vows to root it out, their sites remain infected by obvious counterfeits. The Russian influence operation during the 2016 election, which occasioned the three congressional hearings this week, is only one especially consequential sample of a far larger problem, in which the platforms are gamed for profit or political influence.



Colin Stretch, the general counsel of Facebook, testified this week before multiple congressional committees. Eric Thayer for The New York Times

Most experts say financial motives for the chicanery, in fact, are far more common than political goals. “Keven Eversley” is probably a case in point. Every few days, the Eversley profile posts on Facebook links to sensational, if fact-challenged, articles, all from the same obscure website, conswriters.com (<http://conswriters.com/>): President Trump has ended welfare for immigrants; the F.B.I. was ordered to halt its investigation into the mass shooting in Las Vegas; Hillary Clinton was “hit with terrible news” about Benghazi, Libya.

Conswriters.com, like hundreds of “clickbait” sites, pastes enticing headlines on articles that read like the work of time-pressed high school students. But it is packed with Google ads that generate revenue for every click, highlighting Google’s foundational role in the ecosystem of online deception.

Jonathan L. Zittrain, who studies the internet and society at Harvard, said the companies are reluctant to aggressively purge bogus users and deceptive content because of their business model, which is built on signing up more and more people.

“These platforms are oriented to maximize user growth and retention,” Mr. Zittrain said. “That means not throwing up even tiny hurdles along the sign-up runway, and not closing accounts without significant cause. I suspect they figure there are enough accounts that are the subject of complaints to review without looking for more to assess.”

It takes no great technical expertise to spot the dubious accounts, and amateur sleuths around the country have taken up the task. Zachary Elwood, a technical writer and an author of poker books in Portland, Ore., who started tracking evidence of fake Facebook profiles

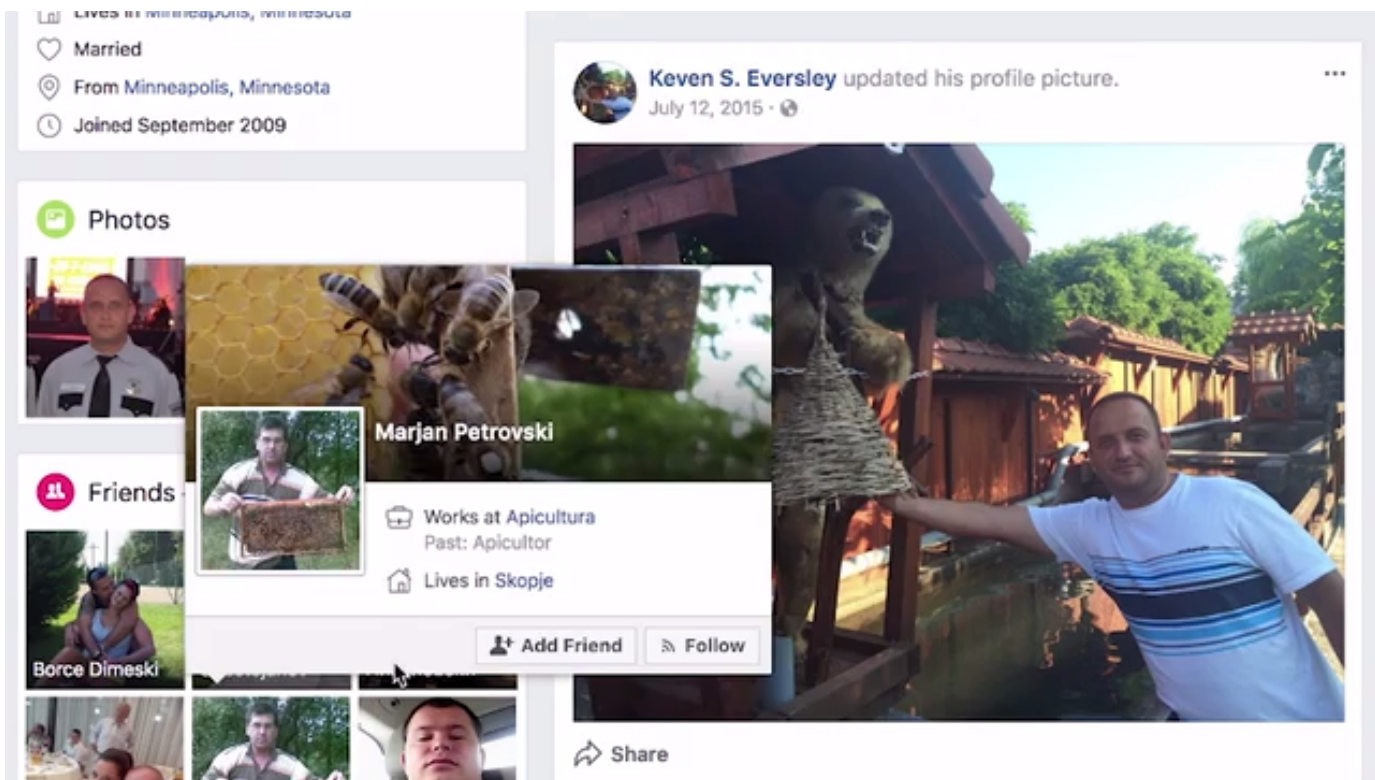
(<https://medium.com/@apokerplayer/examining-fake-rightwing-and-pro-trump-facebook-accounts-ff9b71894f57>) this year, found dozens of impostors, including Keven Eversley.

He noticed that a dozen profiles (https://www.facebook.com/search/people/?q=harry%20taylor&filters_city=%7B%22name%22%3A%22users_location%22%2C%22args%22%3) several clearly with Macedonian content, using the same photographs and other details of a single real person, a Virginia real estate agent named Harry Taylor. Mr. Elwood found a network of what appeared to be attractive pro-Trump American women, but older posts and other details revealed that the accounts originated in the Middle East.

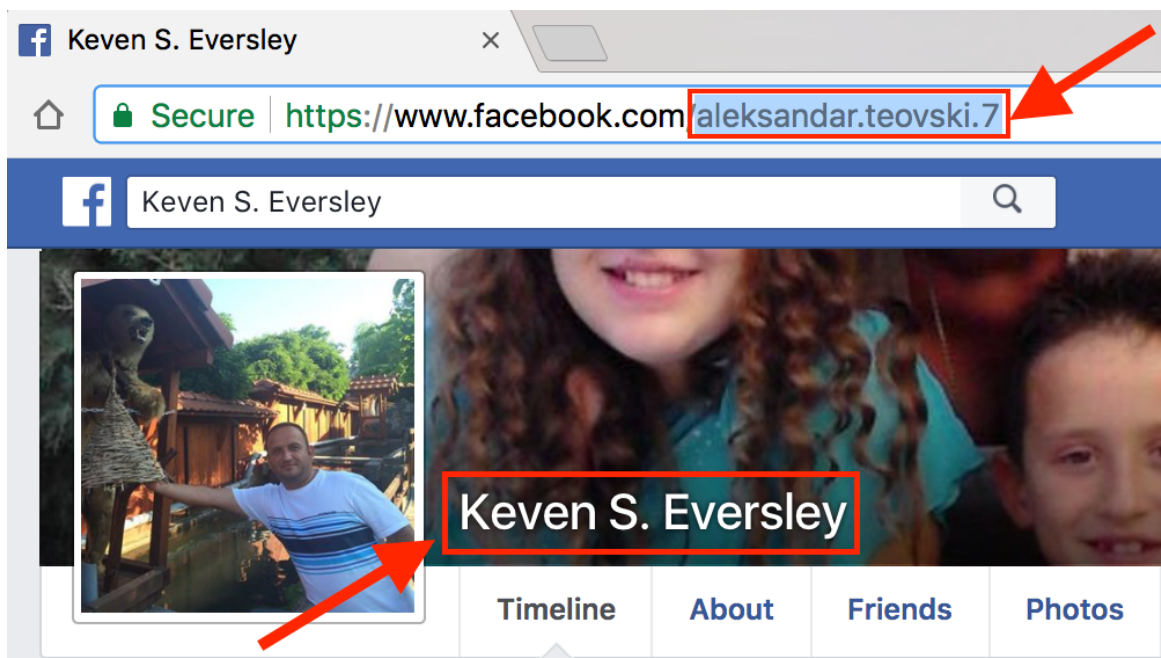
“It’s amazing how sloppy some of these accounts are,” Mr. Elwood said. “I hate liars and I’m drawn to understand stuff like this.”

Red Flags: How to Spoke Fake Content

Check out who a profile is “friends” with. Is the hometown listed on a profile similar to its friend base? For example, “Keven Eversley” claims to be from Minneapolis, but the majority of his friends are from Skopje, Macedonia.



Compare the profile's public name to its web address. For the Eversley profile, it has a different name in the address: Aleksandar Teovski.



If a profile seems suspicious, search for similar pages that draw on the same personal details or images.



The screenshot displays a list of five Facebook profiles, all named "Harry Taylor". Each profile includes a profile picture, a name, a location or bio, and interaction buttons. The profiles are as follows:

- Profile 1:** Photo of an older couple. Name: Harry Taylor. Location: Marlton, New Jersey. Button: Follow.
- Profile 2:** Photo of an older man. Name: Harry Taylor. Bio: REALTOR RETIRED. Button: Add Friend.
- Profile 3:** Photo of an older man. Name: Harry Taylor. Bio: Keller Williams Realty, Inc.. Button: Add Friend.
- Profile 4:** Photo of an older couple. Name: Harry Taylor. Bio: Retired. Button: Add Friend.
- Profile 5:** Photo of an older man. Name: Harry Taylor. Button: Add Friend.

With 2.3 billion users worldwide, Facebook relies on complaints to police its content. So, Mr. Elwood used Facebook's internal complaint tool to report the Keven Eversley profile and 27 others showing evidence of deception. In all but a couple of cases, Facebook responded with a standard message of thanks for the feedback but said the profiles did not violate its community standards (<https://www.facebook.com/communitystandards>) — even though those standards require users to give their “authentic identities.”

“The reporting process is frustrating,” Mr. Elwood said. “Facebook seems to be lagging way behind the problem.”

Facebook estimates that about 200 million of its more than 2.07 billion users may be fakes. Sean Edgett, Twitter’s general counsel, testified before Congress that about 5 percent of its 330 million users are “false accounts or spam,” which would add up to more than 16 million fakes.

“Spammers and bad actors are getting better at making themselves look more real,” Mr. Edgett said.

Independent experts say the real numbers are far higher.

On Twitter, little more than an email address is needed to start tweeting. Facebook’s requirement that users be their authentic selves means the company asks for a smattering of information to sign up — name, birthday, gender and email address. But few checks exist to verify that information.

“Part of the problem is that Facebook is a black box,” said Michael Serazio, a professor of communications at Boston College. “They do what they do, and we don’t know to what degree their operations can even handle these issues — not to mention how handling them maps with their economic model.”

In fact, fighting too hard against deception may clash with the business models that have allowed the companies to thrive. Facebook, Google and Twitter all offer self-serve advertising systems allowing anyone in the world to buy, target and deliver ads for as much — or as little — money as they wish to spend. More scrutiny could hamper growth.

Facebook, for instance, reported record profits this week (<https://www.nytimes.com/2017/11/01/technology/facebook-earnings-russia-zuckerberg.html>) in its quarterly earnings even as executives testified about Russian exploitation of their services. Shares of the social network soared to an all-time high on Wednesday afternoon after the news. Mark Zuckerberg, Facebook’s chief executive, insisted in the earnings call that the company is prepared to sacrifice profits to crack down on illicit activity.

“Protecting our community is more important than maximizing our profits,” he said.

Whether public concern about the manipulation of the platforms might at some point threaten the business remains to be seen. But many customers who run up against the fakery problem end up unhappy.

Kristofer Goldsmith, an assistant director for policy and government relations at Vietnam Veterans of America, noticed last summer a look-alike Facebook page calling itself Vietnam Vets of America that initially borrowed the real group's logo. Linked to a website hosted in Bulgaria, the upstart page pushed viral content, weighing in on N.F.L. players' protests of police shootings. It posted looping videos that were months or years old but presented them as breaking news, he said.

"Sometimes their grammar was off," Mr. Goldsmith said, but there was no way to know who was behind the page.

Soon, the look-alike page had 200,000 followers — more than the 120,000 than the page of the real group, which has a long history of service, a congressional charter and chapters around the country. Mr. Goldsmith said the linked website had few ads, so he suspected a political motive, probably in line with the Russian campaign to divide Americans.

In August, Mr. Goldsmith began complaining to Facebook. But officials there hesitated; hosting pages for millions of groups, they were hardly equipped to assess in detail whether a particular veterans group was worthy and another was not.

Finally, in late October, Facebook shut the newer page, deciding it had illicitly stolen the intellectual property of the older page. But Mr. Goldsmith said the experience was disturbing.

"I don't think they're taking a very proactive approach," he said of Facebook. "There was a foreign entity targeting American vets and inserting itself into divisive debates. Someone could do this to us every month."

(https://www.facebook.com/dialog/feed?app_id=9869919170&link=https%3A%2F%2Fwww.nytimes.com%2F2017%2F11%2F03%2Ftechnology%2Ffacebook-fake-accounts.html&smid=fb-share&name=Facebook%20Says%20It%E2%80%99s%20Policing%20Fake%20Accounts.9)
(<https://twitter.com/intent/tweet?url=https%3A%2F%2Fwww.nytimes.com%2F2017%2F11%2F03%2Ftechnology%2Ffacebook-fake-accounts.html&text=Facebook%20Says%20It%E2%80%99s%20Policing%20Fake%20Accounts.9>)
(mailto:?)

Lilia Chang contributed to this article.

A version of this article appears in print on November 6, 2017, on Page B3 of the New York edition with the headline: Facebook Says It's Policing Fake Accounts. So Why Are They Still Easy to Spot?. Order Reprints (<http://www.nytreprints.com/>) | Today's Paper (<http://www.nytimes.com/pages/todayspaper/index.html>) | Subscribe (<https://www.nytimes.com/subscriptions/Multiproduct/lp8HYKU.html?campaignId=48JQY>)

Related Coverage

How Russia Got Americans to Turn Against One Another

(<https://www.nytimes.com/2017/11/01/us/politics/facebook-google-twitter-russian-interference-hearings.html?action=click&module=RelatedCoverage&pgtype=Article®ion=Footer&contentCollection=Related>)

Why Tech Giants Suddenly Shun the 'Social Media' Label

(<https://www.nytimes.com/2017/11/02/technology/russia-investigation-tech-companies.html?action=click&module=RelatedCoverage&pgtype=Article®ion=Footer&contentCollection=Related>)

Follow our latest updates on the Senate testimony of social media executives.

(<https://www.nytimes.com/2017/11/01/us/politics/russia-technology-facebook.html?action=click&module=RelatedCoverage&pgtype=Article®ion=Footer&contentCollection=Related>)

Interested in All Things Tech?

The Bits newsletter will keep you updated on the latest from Silicon Valley and the technology industry.

SEE SAMPLE ([HTTPS://WWW.NYTIMES.COM/NEWSLETTERS/SAMPLE/BITS](https://www.nytimes.com/newsletters/sample/bits))

Enter your email address

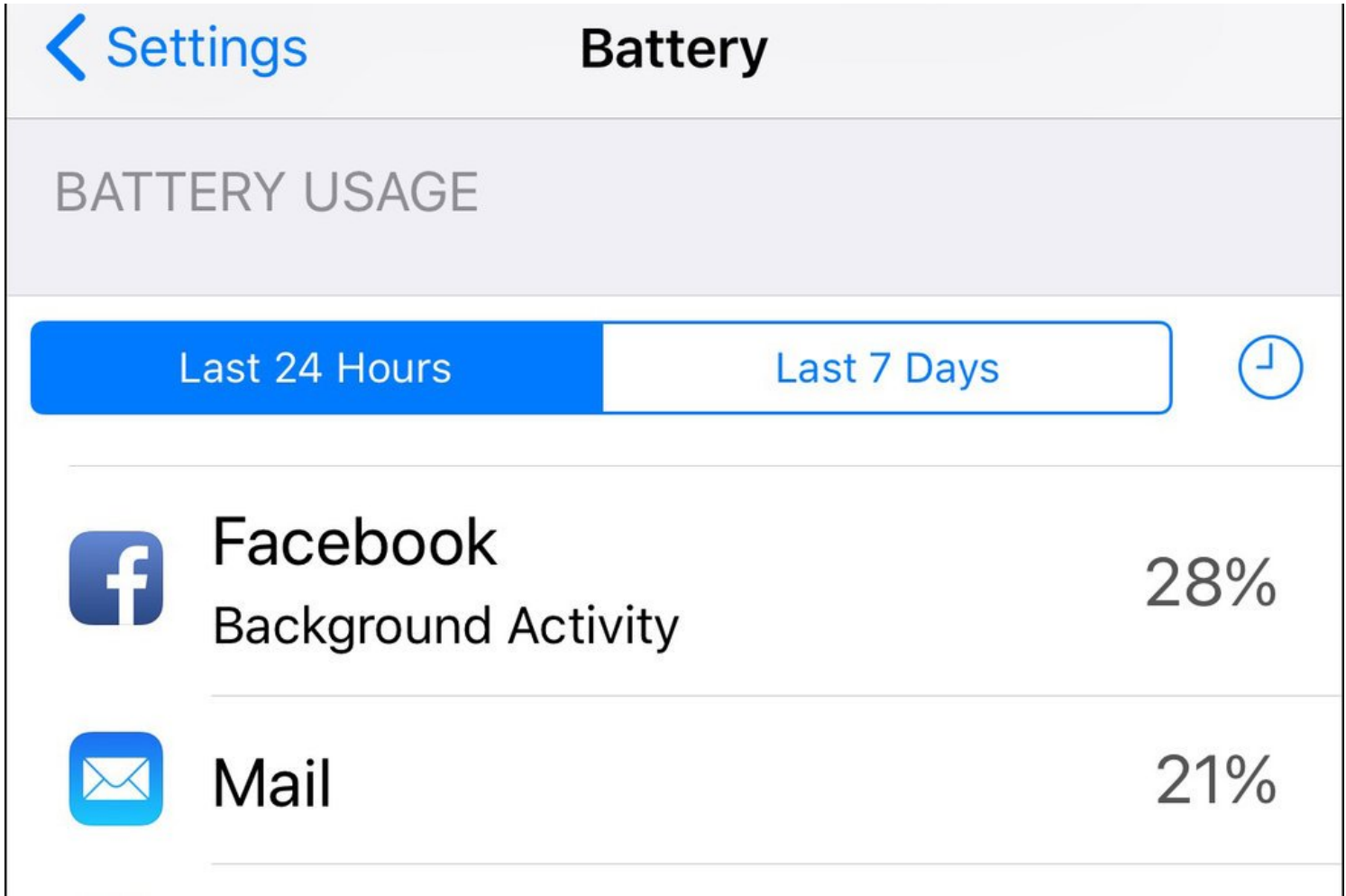
☐ You agree to receive occasional updates and special offers for The New York Times products and services.

I'm not a robot

reCAPTCHA
Privacy - Terms

Sign Up

More in Technology (<https://www.nytimes.com/section/technology?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)



The New York Times

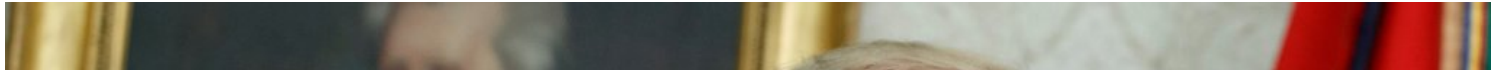
(<https://www.nytimes.com/2017/11/06/technology/personaltech/iphone-battery-drain.html?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)

Slowing iPhone Battery Drain

Older iPhone models often take a performance and power hit when a new version of iOS arrives, but software updates may help.

(<https://www.nytimes.com/2017/11/06/technology/personaltech/iphone-battery-drain.html?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)

1h ago





Evan Vucci/Associated Press

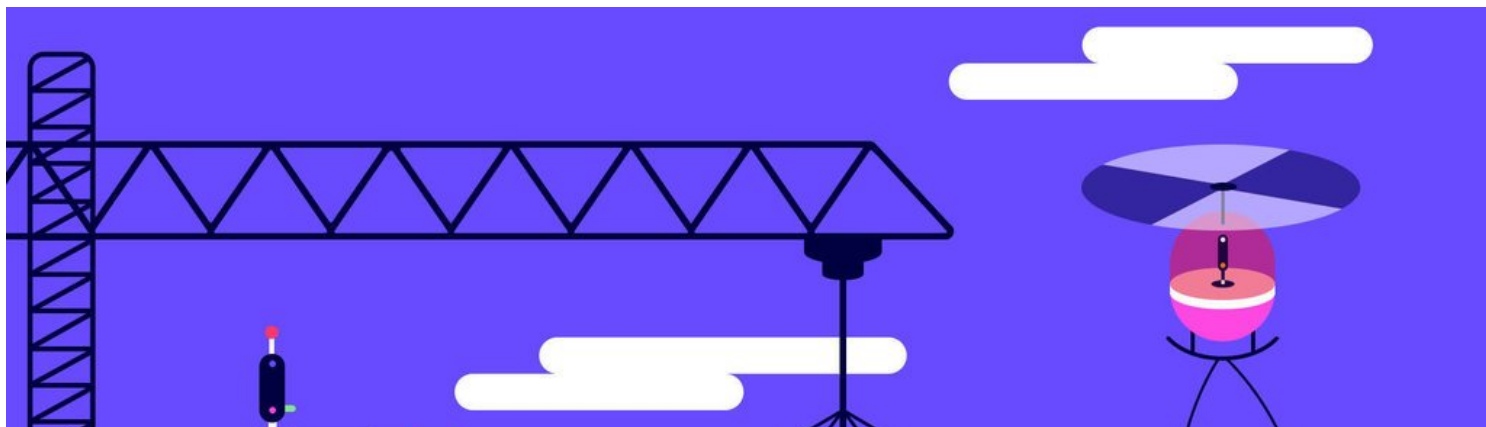
(<https://www.nytimes.com/2017/11/06/business/dealbook/broadcom-qualcomm-merger.html?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)

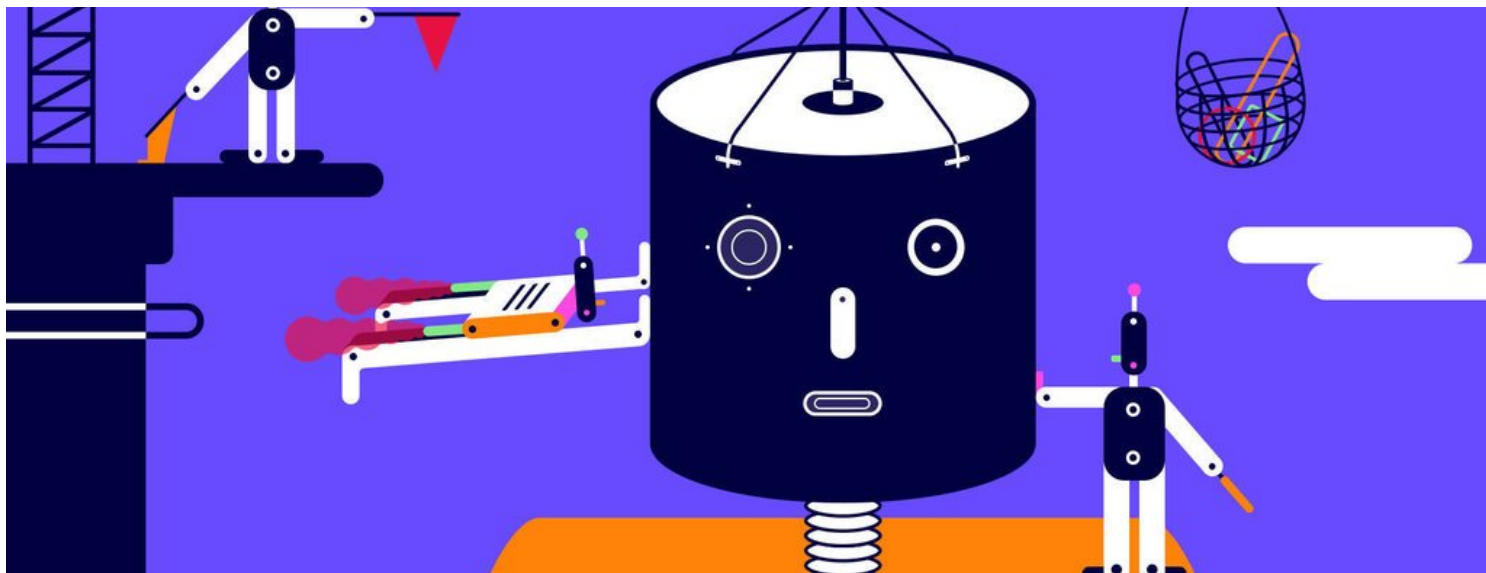
Broadcom offered \$105 billion to buy the rival chip maker Qualcomm.

The takeover bid sets up a battle between two of the biggest chip makers, whose products touch nearly every smartphone in the world.

(<https://www.nytimes.com/2017/11/06/business/dealbook/broadcom-qualcomm-merger.html?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)

48m ago





Mengxin Li

(<https://www.nytimes.com/2017/11/05/technology/machine-learning-artificial-intelligence-ai.html?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)

Building A.I. That Can Build A.I.

Google and others, fighting for a small pool of researchers, are looking for automated ways to deal with a shortage of artificial intelligence experts.

(<https://www.nytimes.com/2017/11/05/technology/machine-learning-artificial-intelligence-ai.html?action=click&module=MoreInSection&pgtype=Article®ion=Footer&contentCollection=Technology>)

Nov. 5

