



Inside Track

New FBI Director Hints at Backdoors for Encryption

Newly minted FBI Director Christopher Wray seems to be picking up right where his predecessor, James Comey, left off in the war against encryption, telling the attendees at the International Conference on Cyber Security on January 9 that strong encryption is “an urgent public safety issue.”

While speaking at the conference in New York, Wray said that in the fiscal year ending September 30, the FBI was unable to access more than half of the devices it attempted to access, owing to them being encrypted. He said that the number of inaccessible devices was nearly 7,800, adding that the inability to break the encryption on those devices — despite having warrants to access the data stored on them — hinders the agency’s work.

While giving lip service to the importance of strong encryption and security, Wray said the current situation that allows individuals to protect the data on their devices with unbreakable encryption cannot be allowed to continue, adding, “We face an enormous and increasing number of cases that rely heavily, if not exclusively, on electronic evidence.” What Wray appears to be working his way up to is the creation of a “backdoor” to encryption. A backdoor is an idea that has been proposed by surveillance hawks — and rejected by privacy advocates — for years.

While encryption has been the standard in business for more than 20 years, it has not been largely adopted by the average citizen for much of anything, including e-mail. Until recently. The upswing in the use of powerful encryption to protect data is the direct result of people reacting to what Edward Snowden revealed to the world in May 2013: U.S. government agencies routinely spy on everyone, including American citizens.

Privacy advocates should brace themselves for another round of demands for an end to powerful encryption in the hands of private citizens. Because backdoors — regardless of promises that only law enforcement could use them and then only with a warrant — are exactly that: the end of any encryption that works, which is the goal of the surveillance state.

Credit Card Debt Hits \$1 Trillion

For the first time in history, U.S. credit card debt hit \$1 trillion last year, reported the Federal Reserve on January 8. This eclipsed the previous record set almost 10 years ago, just before the housing and credit bubbles burst. In addition, “non-revolving” (i.e., auto and student loan) debt is approaching \$3 trillion. These numbers have put credit card debt on “watch” at Seeking Alpha, a stock market analysis group that referred to the trillion-dollar number as “scary.”

A closer look at the statistics reveals that these may not be such “scary” numbers after all. For one thing, fewer than 40 percent of all households carry any sort of credit card debt. Among millennials ages 18 to 29, only a third even have a credit card.

Next, the ratio of income to credit card debt at the end of 2017 (before the new tax cuts) was already declining, with the ratio of credit card debt compared to the nation’s gross domestic economic output at about five percent, compared with 6.5 percent in 2008.

Also, credit card delinquencies remain way below the nine-percent historical average, at just 7.5



Written by [Staff](#) on February 5, 2018

Published in the February 5, 2018 issue of [the New American](#) magazine. Vol. 34, No. 03

percent, and far below the rate of 15 percent reached following the 2008 financial crisis.

There's another way to look at credit card debt: comparing outstanding balances to incomes. ValuePenguin performed such a service, showing that households with annual incomes of between \$25,000 and \$100,000 have less than \$7,000 in outstanding balances on their credit cards. Further, that analysis showed that the average has increased only slightly since 2013.

With almost two million more people working today than held jobs a year ago, and others enjoying wage and salary increases, that \$1 trillion in credit card debt becomes far less "scary." In a \$20 trillion economy that is growing at three percent a year, \$1 trillion in credit card debt may reflect that growth, as banks are willing to issue more cards to more credit-worthy individuals and those individuals, having perhaps learned lessons from the Great Recession, are using them more prudently.

State Department Announces World's Top 10 Religious Persecutors

In a January 4 announcement, the Trump administration's State Department followed recommendations made by the U.S. Commission on International Religious Freedom (USCIRF) in its annual report, designating Burma, China, Eritrea, Iran, North Korea, Sudan, Saudi Arabia, Tajikistan, Turkmenistan, and Uzbekistan as Countries of Particular Concern (CPC) — meaning they bear the closest scrutiny for their past records of religious persecution. The list mirrors the nations named by the Obama administration in April 2016 — also at the urging of the USCIRF, a bipartisan committee that monitors religious liberty around the world.

In a press release, the USCIRF stated that its members had hoped the administration would take its recommendation to add a half dozen more nations to the "concern" list. "Although USCIRF agrees with the 10 countries on the State Department's list, it does not go far enough," said USCIRF Chairman Daniel Mark. "Secretary [Rex] Tillerson should have also designated the Central African Republic, Nigeria, Pakistan, Russia, Syria, and Vietnam."

Additionally, for the first time, the State Department announced its "Special Watch List," a new category created with passage of the International Religious Freedom Act of 2016. The designation is reserved for countries that either engage in or tolerate severe violations of religious freedom — while not necessarily rising to the notoriety of the "Countries of Particular Concern." This year the State Department listed Pakistan as the sole nation to be added to the "Special Watch List."

The USCIRF had hoped that the State Department would have added Pakistan to the CPC list. "Pakistan continues to harass its religious minorities, has state-sanctioned discrimination against groups such as the Ahmadis, and tolerates extra-judicial violence in the guise of opposing blasphemy," said Mark.

In the U.S. Congress, Representative Chris Smith (R-N.J.), a particularly vocal champion of religious freedom, released a statement expressing his disappointment that the State Department had not added Vietnam to the CPC list, where it had held a perennial spot until being removed for no apparent reason a decade ago.

James Damore Brings Discrimination Suit Against Google

James Damore, the former Google software engineer who was fired in August, filed a class-action suit



Written by [Staff](#) on February 5, 2018

Published in the February 5, 2018 issue of [the New American](#) magazine. Vol. 34, No. 03

on January 8 against the Internet giant, alleging discrimination against white, male, and conservative employees.

Damore was terminated for circulating an internal memo that questioned Google's discriminatory and gender-biased work environment. After attending Google's "Diversity and Inclusion Summit," he was asked by Google's human resources department for feedback on the training, which prompted Damore to create the memo.

Also named as a complainant in the suit is another former software engineer, David Gudeman, who was terminated by Google in November of 2016, just days after the election of Donald Trump. In an internal thread, Gudeman had responded skeptically to a Muslim employee who claimed he was targeted by the FBI. Gudeman was disciplined and later fired for his political views.

The attorneys involved in the case are seeking other "potential class members" to join the suit against Google. Such plaintiffs would be "Google employees [who] have witnessed multiple instances in which hundreds of 'progressive' Googlers would target a single co-worker for harassment, and even potential violence, over a politicized matter, humiliating the person and sabotaging his career."

The suit lists many outright threats made against Damore and Gudeman by other employees. One e-mail, with the subject "You are a terrible person," read as follows: "Feel free to pass this along to HR. Keep them in the loop for all I care. May as well do it early. You're a misogynist and a terrible human. I will keep hounding you until one of us is fired. F*ck you." The e-mail was sent by Alex Hidalgo, a site reliability engineer at Google. Similar threatening e-mails were sent to Damore and Gudeman by other co-workers.

The complaint details how it was Google's policy to encourage rank-and-file employees to attack other employees for expressing political views that strayed from Google's liberal orthodoxy. On Fox News, Damore's attorney, Harmeet Dhillon, said Google's actions were "illegal under federal law; it's illegal under California law."

Twitter Employees Admit to Political Censorship

A new hidden-camera video by Project Veritas — published January 11 — features "nine current and former Twitter employees" admitting to "steps the social media giant is taking to censor political content that they don't like," according to Project Veritas.

The video opens with a montage of damning quotes before showing those quotes in context. Far from being less damning when seen in context, they are more so. The video focuses on something called "shadow banning."

Abhinav Vadrevu, a former software engineer at Twitter, said, "One strategy is to shadow ban so that you have ultimate control." He added, "The idea of a shadow ban is that you ban someone, but they don't know they've been banned because they keep posting, but no one sees their content." On the psychological side of the equation, this creates a situation where the users just think their posts — their ideas — aren't appealing to anyone. "So they just think no one is engaging with their content when in reality, no one is seeing it," Vadrevu said. He admitted that the practice "is risky" because "people will figure that sh*t out." He also said that it would cause "bad press" and that "it's like, unethical in some way, you know? So, I don't know."



Written by [Staff](#) on February 5, 2018

Published in the February 5, 2018 issue of [the New American](#) magazine. Vol. 34, No. 03

Olinda Hassan is a policy manager in Twitter's Trust and Safety Department, which she describes as "controversial." Her team makes the rules and regulations for the platform's millions of users. They are the gatekeepers. As Hassan explained, Twitter is "working on" a way to silence certain people and ideas on the platform. "Yeah, it's something we're working on — where we're trying to get the sh*tty people not to show up," she told the undercover journalist, adding, "It's a product thing we're working on."

The Project Veritas video shows Mo Norai, a former content review agent at Twitter, saying, "Let's say if it was a pro-Trump thing and I'm anti-Trump, I was like, 'I banned his whole account.' It goes to you, and then it's at your discretion. And if you're anti-Trump, you're like, 'Oh, you know what? Mo was right, f*ck it, let it go.'" Norai went on to say that "discretion" — which he described as "I guess how you felt about a particular matter" — plays a huge role in what content gets banned at Twitter. Norai said that during his time at Twitter, left-leaning posts that were tagged as possibly offensive were allowed to remain. "It would come through checked and then I would be like, 'You know what? This is okay. Let it go.'"

Pranay Singh is a direct messaging engineer at Twitter. He said that the suspension of WikiLeaks founder Julian Assange's Twitter account may have been because of "the U.S. government pressuring" Twitter. He said, "They do that." In fact, he said it happens "all the f*cking time." In Assange's case, he said the U.S. government doesn't like "people messing with their politics, and [Assange] has sh*t on a lot of people."

Singh helped explain the types of tweets that are likely not to make the cut. "Just go to a random (Trump) tweet and just look at the followers," he said. Those followers will "all be like guns, God, 'Merica, like and with the American flag and like, the cross." He said the way to get rid of those users — all of whom he assumes are bots, not real users, because, "Like who says that? Who talks like that?" — is to "just delete them." But since "there are hundreds of thousands of them" and that volume can't be handled by people, "you got to, like, write algorithms to do it for you."

Perhaps most shocking is the statement by Steven Pierre, a software engineer at Twitter. Speaking on hidden camera, he said that Twitter is developing a way to automate the whole process of what gets seen and what doesn't. "Every single conversation is going to be rated by a machine" that will decide whether the conversation is "positive" or "negative." If it's negative, "They may have a point, but it will just, like, vanish," he said. When asked whether this would "ban certain mindsets," he said no. "It's going to ban, like, a way of talking."

If that isn't *Pravda*, nothing is. Between filtering, banning, shadow banning, and manipulating what users see, Twitter is dangerously close to a thought-control platform.



Written by [Staff](#) on February 5, 2018

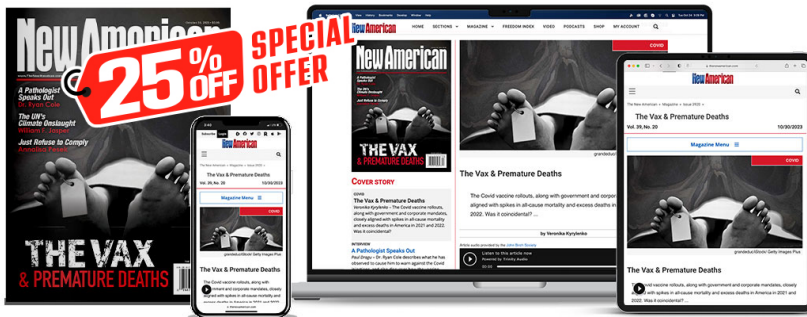
Published in the February 5, 2018 issue of [the New American](#) magazine. Vol. 34, No. 03

Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



[Subscribe](#)

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.