The Washington Post

Democracy Dies in Darkness

THE TECHNOLOGY **202**

A newsletter briefing on the intersection of technology and politics.

Subscribe to the newsletter ⊕

Hunter Biden laptop findings renew scrutiny of Twitter, Facebook crackdowns

By Cristiano Lima

Yesterday at 9:00 a.m. EDT

🎁 ⬆️ 💬 22

Happy Thursday! Today's top was reported with our stellar tech news analysis writer **Will Oremus**.

Below: A key tech nominee inches closer to confirmation, and the tech giants get fooled by hackers. First:

Hunter Biden laptop findings renew scrutiny of Twitter, Facebook crackdowns

Just weeks before the 2020 presidential election, Twitter and Facebook took rare steps to limit the circulation of an article by the New York Post detailing emails supposedly from the laptop of **Hunter Biden**, son of the now-president **Joe Biden.**

Facebook restricted the story's reach while its fact-checking partners looked into the veracity of the reporting. Twitter went a step further, locking the New York Post's account and blocking users from posting links to the story, over concerns it was based on hacked materials.

The actions ushered in a wave of backlash from Republicans — who accused tech platforms of suppressing the material to shield Biden — that continues to fuel GOP attacks on Silicon Valley.

Now, amid new reporting by The Washington Post, verifying the authenticity of thousands of emails purportedly from Hunter Biden's laptop, and the New York Times, which authenticated some messages in the cache, the social media policies are facing fresh scrutiny.

On Wednesday, my colleagues **Craig Timberg**, **Matt Viser** and **Tom Hamburger** reported that, "Thousands of emails purportedly from the laptop computer of Hunter Biden … are authentic communications that can be verified through cryptographic signatures from Google and other technology companies," based on an analysis two security experts conducted for The Post.

According to the report, "Neither expert reported finding evidence that individual emails or other files had been manipulated by hackers, but neither was able to rule out that possibility."

Republicans have seized on the laptop as proof of wrongdoing, while Democrats have suggested it could have been manipulated to include foreign misinformation. Ultimately, my colleagues wrote, The Post's forensic analysis is "unlikely to resolve that debate," given that the verdict on much of the purported laptop data remains inconclusive.

But the findings highlight the fact that tech companies appear to have acted both forcefully and preemptively against a perceived threat that to this day has not been publicly corroborated.

Republicans have seized on the findings as vindication in their feud with Silicon Valley.

Sen. **Marsha Blackburn** (R-Tenn.):

Sen. Marsha Blackburn ✓
@MarshaBlackburn

Hunter Biden's laptop was always real, but the mainstream media and big tech silenced you for talking about it anyway.

3:20 PM · Mar 17, 2022

♡ 3.3K   💬 Reply   ⬆ Share this Tweet

Twitter and Facebook declined to comment on the new findings.

But the findings are also resurfacing broader debates within civil society about where social media's obligations to curtail suspected misinformation begin and end.

One crucial question: What role, if any, should they play in restricting reporting by prominent news organizations, particularly when dealing with unverified or dubious sourcing?

"A company like Twitter should not be trying to make a determination on the veracity of information when it's impossible for them to have the type of information they would need to do so," **Evan Greer**, director of digital activist group Fight for the Future, told The Technology 202.

Looming over Twitter and Facebook's actions in 2020 were widespread fears of repeating 2016, when Russian hackers leaked troves of emails from Democratic officials.

Former Facebook security chief **Alex Stamos** told my colleague **Will Oremus** that, in retrospect, the platforms "overreacted" against the New York Post reporting on Hunter Biden, but that he understood why.

"The most effective Russian operation in 2016 was the [leak of hacked emails from the Democratic National Committee] and this smelled like the exact same playbook," he said on Wednesday.

Stamos said the companies were in a "no-win situation," likely facing allegations of censorship if they limited the article or criticism of amplifying potential misinformation if they didn't.

A slew of former intelligence officials expressed skepticism at the time about the veracity of the New York Post's reporting and warned it could be Russian-backed disinformation.

Twitter, which took more aggressive action, took the brunt of the heat in Washington.

While the company quickly reversed its initial ruling that the article violated its policies against hacked materials, it continued to block users from posting it under a separate rule against publishing users' private information. The company later changed course again, saying it would allow users to share the link because the information was widely available in publications beyond the New York Post.

Ultimately, the episode underscores the high-stakes trade-offs companies make when deciding whether to limit content where the risk of harm is unclear.

"This latest analysis shows how complex and difficult it can be to verify the authenticity of documents or digital files, regardless of how they have been obtained," Greer said. "That's true whether material was allegedly hacked or just given to a journalist by a willing source."

Our top tabs

Democrats inch closer to seizing majority at FTC

Democrat **Alvaro Bedoya**'s nomination to the Federal Trade Commission cleared a key procedural hurdle in the Senate on Wednesday, putting the party a step closer to retaking the majority at the agency.

The full chamber voted to discharge Bedoya's nomination from the Senate Commerce Committee, which had split along party lines on advancing the nominee earlier this month. The move puts Senate Majority Leader **Chuck Schumer** (D-N.Y.) in a position to soon schedule a vote to confirm Bedoya, whose nomination has been bogged down amid Republican opposition since September.

The expected addition of Bedoya, a renowned privacy scholar and surveillance critic, is poised to enable the agency's Democratic leadership to pursue more aggressive enforcement measures against the technology sector.

Apple and Meta forked over user data to hackers posing as law enforcement

Apple and Facebook parent company Meta provided " customer's address, phone number and IP address" to hackers masquerading as law enforcement officials, Bloomberg's **William Turton** reports, citing three people with knowledge of the matter.

"Cybersecurity researchers suspect that some of the hackers sending the forged requests are minors located in the U.K. and the U.S. One of the minors is also believed to be the mastermind behind the cybercrime group Lapsus$, which hacked Microsoft Corp., Samsung Electronics Co. and Nvidia Corp., among others," according to the report.

Meta spokesman **Andy Stone** said in a statement that the company reviews "every data request for legal sufficiency and use advanced systems and processes to validate law enforcement requests and detect abuse." An Apple representative referred Bloomberg News to a section of its law enforcement guidelines.

Inside the industry

How Google and Amazon bankrolled a 'grassroots' activist group of small business owners to lobby against Big Tech oversight (CNBC)

The Silenced No More Act just became law in Washington state (Protocol)

How China's TikTok, Facebook influencers push propaganda

Spam Texts From Your Own Number? 'Bad Actors' Sent Them, Verizon Says. (New York Times)

Before you log off

CNN International ✔
@cnni

Dramatic video shows the moment firefighters rescue a dog from Los Angeles flooding cnn.it/3wMH52P

Watch on Twitter

9:45 AM · Mar 30, 2022

♡ 264   💬 Reply   ⬆ Share this Tweet

Read 12 replies

That's all for today — thank you so much for joining us! Make sure to tell others to subscribe to The Technology 202 here. Get in touch with tips, feedback or greetings on Twitter or email.