Please break up Facebook, cofounder asks regulators

Enlarge / Mark Zuckerberg and Chris Hughes on Harvard's campus in 2004, well before Facebook started taking over the world.
Rick Friedman/Corbis via Getty Images

reader comments

96 with 58 posters participating

Share this story

Facebook cofounder Chris Hughes isn't just idly wondering if regulators might break up the tech behemoth he helped launch. He's going on a personal tour, meeting with state and federal officials to lay out in detail the way he thinks it could be done.

Hughes has met with members of Congress, the Justice Department's Antitrust Division, the Federal Trade Commission, and the office of New York Attorney General Letitia James to make a detailed case arguing Facebook is too big for its own good, according to separate reports from The Washington Post and The New York Times.

The breakup tour went public in May, when Hughes penned a lengthy op-ed in The New York Times saying his former colleague Mark Zuckerberg wielded too much power. "I'm disappointed in myself and the early Facebook team for not thinking more about how the News Feed algorithm could change our culture, influence elections and empower nationalist leaders," Hughes wrote at the time. "And I'm worried that Mark has surrounded himself with a team that reinforces his beliefs

instead of challenging them.”

Tech and antitrust law experts Scott Hemphill and Tim Wu had already been working on a detailed case against Facebook, and they reached out to Hughes following his public turn. The trio now work together to make their case.

Keeping competition away

While consumers and experts alike wonder if Facebook’s size and outsized global market power are what allow it to play fast and loose with user data and privacy, Wu and Hemphill argue a much more basic case of good old-fashioned unfair anticompetitive behavior.

Through “serial defensive acquisitions,” they say, Facebook has prevented competitors from entering the marketplace and cut off innovation before it can flourish.

In other words, when a small company looks promising, Facebook leaps in and snaps it up, eliminating competition and reaping profit from other developers’ innovations.

The most obvious case is Instagram. The photo-sharing service launched as an iOS app in 2010. Facebook snapped it up in 2012 for what was, at the time, a jaw-dropping $1 billion.

The Economist reported on the trend in 2018, noting that not only does an acquisition-heavy environment change the motivation for developers but also that not all deals are quite as voluntary as they seem.

“Big tech firms have been known to intimidate startups into agreeing to a sale, saying that they will launch a competing service and put the startup out of business unless they agree to a deal,” a source who participated in such strong-arming “negotiations” told The Economist.

Facebook alone has acquired more than 75 smaller firms in the

past 15 years. Forcing Facebook to divest some of those companies, such as Instagram and WhatsApp, is “low-hanging fruit,” a “plain vanilla violation” of the Sherman Act, the country’s oldest antitrust law, Wu told the Post.

Hughes has no current insider knowledge about Facebook operations, as he left the company and cashed out his stock in 2007. But his status as a former Facebooker who can speak to the personalities and motivations of the leaders still in the room helps bolster the case, Rep. David Cicilline (D-RI) told the Post.

The House Antitrust Subcommittee, of which Cicilline is chair, launched an investigation into Facebook and other tech firms last month. Cicilline told the Post it was “remarkable and significant” that Hughes had the “capacity and courage” to mount his criticisms against Facebook to members of the committee.

Back when Hughes parted ways with Facebook, the idea of an antitrust investigation into the company might have seemed absurd. But 12 years later, the company’s tactics that allowed it to amass 2.4 billion users; the ways it buys, sells, and trades those users’ data; and its dominance in the advertising marketplace are all the focus of several investigations.

In addition to the House probe, Facebook this week confirmed that it’s currently the target of an active antitrust inquiry at the FTC. The Justice Department’s Antitrust Division also said separately this week it is investigating “market-leading online platforms,” a category usually considered to include Amazon, Facebook, and Google at a minimum.

The last breakup of a US company for antitrust reasons happened in the early years of the Reagan administration, when AT&T—”Ma Bell”—split into the “baby bells” in 1984 as the result of a 1982 settlement with the DOJ.

35 years later, however, the companies have largely re-

aggregated and now comprise significant parts of AT&T and Verizon.

https://arstechnica.com/?p=1542111

Presidential candidate Tulsi Gabbard sues Google for ad censorship

Enlarge / Rep. Tulsi Gabbard (D-Hawaii).
Justin Sullivan/Getty Images

reader comments

248 with 104 posters participating

Share this story

Democratic presidential candidate Tulsi Gabbard sued Google on Thursday. She argued that the search giant illegally blocked her from buying ads on Google's platform for several hours on June 28—two days after she appeared in the first Democratic primary debate.

"Google plays favorites, with no warning, no transparency, and no accountability," Gabbard wrote in her lawsuit. "Google's arbitrary and capricious treatment of Gabbard's campaign should raise concerns for policymakers everywhere about the company's ability to use its dominance to impact political discourse."

Google says the brief suspension was triggered by the company's automated anti-fraud algorithms.

"We have automated systems that flag unusual activity on all advertiser accounts—including large spending changes—in order to prevent fraud and protect our customers," a Google spokesperson said in an email to Ars. "In this case, our system triggered a suspension and the account was reinstated shortly thereafter. We are proud to offer ad products that help campaigns connect directly with voters, and we do so without bias toward any party or political ideology."

Meanwhile, legal experts panned the complaint.

The lawsuit "has so many problems it's hard to know where to begin," argues attorney and writer Gabriel Malor.

Gabbard's lawsuit also doesn't impress Eric Goldman, a legal scholar at Santa Clara University. He described the lawsuit as "terrible" and argued that there was "a PR aspect to the filing."

The complaint often reads like a campaign white paper

In recent months, Democratic presidential hopefuls have competed to be the most anti-Google candidate. Sen. Elizabeth Warren (D-Mass.) has called for breaking up Google—a position shared by Bernie Sanders (I-Vt.). Gabbard has also endorsed Warren's position, and suing Google is a way for her to underscore that view.

Conventional legal complaints focus narrowly on the facts necessary to prove the plaintiff's argument—in this case that blocking Gabbard's ads broke the law. By contrast, Gabbard's complaint reads in places like a campaign white paper. It complains that the Federal Trade Commission failed to take stronger action after a 2012 investigation into Google's

business practices, that the Federal Communications Commission is rolling back network neutrality regulations under Trump, and that Facebook allegedly censored Warren campaign ads that called for the breakup of Facebook—issues that don't seem relevant to determining whether Google broke the law.

Meanwhile, the complaint is light on evidence of Gabbard's central claim—that Google deliberately sabotaged her campaign by blocking her from running ads.

Gabbard also offered no concrete evidence for her other claim—that Gmail routed her campaign emails to the spam folder at a higher rate than other presidential candidates.

"The complaint weaves a complicated conspiracy theory of how Google is out to get her, but the facts cited by the complaint told a thoroughly uncompelling conspiracy story," Goldman tells Ars by email.

The lawsuit makes unconventional legal arguments

The first count of Gabbard's lawsuit accuses Google of violating the First Amendment to the Constitution. The First Amendment bars governments from infringing freedom of speech—and generally gives private parties wide latitude to decide which content to publish.

But Gabbard argues that the First Amendment constrains Google because the company has dedicated "its platform for public use and public benefit, inviting the public to utilize Google as a forum for free speech. Google serves as a state actor by performing an exclusively and traditionally public function by regulating free speech within a public forum and helping to run elections."

Gabbard's complaint doesn't cite any legal precedents backing up this rather expansive interpretation of the First

Amendment, and there are a number of precedents pointing in the opposite direction. In the words of legal scholar Jonathan Peters, “Courts so far have held that private online service providers are not state actors for First Amendment purposes.”

Gabriel Malor also points out that Gabbard will need to contend with Section 230 of the Communications Decency Act, which gives online service providers broad immunity for their decisions about whether to publish content on their platforms.

https://arstechnica.com/?p=1542053

Car makers, California agree to emissions rules Trump admin is trying to kill

reader comments

68 with 51 posters participating

Share this story

Four major automakers have reached an agreement with California to produce more fuel-efficient cars for the US market, despite efforts by the Trump administration to roll back emissions regulations.

Honda, Ford, Volkswagen, and BMW of North America all agreed to a voluntary framework that will reduce emissions through

2026, the California Air Resources Board (CARB) said Thursday.

The deal requires the automakers to improve their overall fleet's average fuel efficiency by 3.7 percent per year, starting with the 2022 model year. It also promotes a transition to electric vehicles by giving companies that produce and sell more electric cars credits toward meeting that emissions standard, and by providing incentives for installing more emissions-reducing technologies.

"Few issues are more pressing than climate change," California governor Gavin Newsom said in a statement. "I now call on the rest of the auto industry to join us, and for the Trump administration to adopt this pragmatic compromise instead of pursuing its regressive rule change. It's the right thing for our economy, our people, and our planet."

More than California

The Obama administration in 2012 adopted a fuel economy standard that would gradually increase the average miles-per-gallon rating for most cars to 54.5mpg by 2025 (about 40mpg under real world conditions). The Environmental Protection Agency finalized that standard in December 2016.

Like many regulations from the tail end of the Obama administration, though, the fuel efficiency rule had no fans in the Trump administration. EPA administrator Scott Pruitt kicked off a rulemaking process in 2018 to dump those standards and replace them with something weaker.

California fought back. For decades, the smog-prone state has had a waiver allowing it to set more stringent fuel-efficiency guidelines than federal law calls for. CARB, determined to maintain its own higher standards, filed suit.

For a time, the Trump administration was theoretically negotiating with CARB to search for a compromise position, but

those talks, such as they were, collapsed in February.

California law is critical to carmakers because emissions regulations in California spread far beyond the Golden State's borders. Most states can't set their own fuel-efficiency guidelines; California is a special case. But the other 49 states *can* choose to adopt California's stricter standards instead of the federal guideline, and at least 16 states have said they will back California's emissions standard rather than support the federal rollback.

Ford, Honda, BMW, and Volkswagen are all among the 17 automakers that asked the Trump administration to negotiate with California to find a single, unified national standard.

Although the four companies agreed to stricter, voluntary terms with California, "a 50-state solution has always been our preferred path forward," they said in a joint statement. "These terms will provide our companies much-needed regulatory certainty by allowing us to meet both federal and state requirements with a single national fleet, avoiding a patchwork of regulations while continuing to ensure meaningful greenhouse gas emissions reductions."

CARB chair Mary D. Nichols echoed the sentiment, but she added a clear threat. "If the White House does not agree, we will move forward with our current standards but work with individual carmakers to implement these principles," she said. "At the same time, if the current federal vehicle standards proposal is finalized, we will continue to enforce our regulations and pursue legal challenges to the federal rule."

https://arstechnica.com/?p=1541721

The FTC is investigating Facebook. Again

Enlarge / The company is not having its best-ever week.

reader comments

30 with 25 posters participating

Share this story

Facebook’s legion of lawyers is certainly earning its keep this year: the company disclosed to investors Tuesday that it is under antitrust investigation by the Federal Trade Commission.

This is a completely different investigation than the $5 billion settlement, also made public yesterday, that Facebook and the FTC reached over Facebook’s privacy practices. Nor is it the same antitrust probe of big tech the Justice Department launched earlier this week.

Why antitrust?

Antitrust investigations focus on behavior regulators deem anticompetitive. The best-known kind of example is when two companies that compete directly against each other want to merge, drastically reducing or eliminating competition in their market. If there are only two companies in the entire US that make a certain kind of nail, for example, the FTC or DOJ would likely sue to block an acquisition between them from happening, because it would pose harm to competition and likely raise prices for nail-buyers everywhere, also affecting suppliers that need nails to build things like houses.

Anticompetitive behavior also includes collusion or price-fixing, as well as good old-fashioned strong-arming and other unfair tactics that prevent competitors from entering the marketplace.

Usually the determination of potential harm focuses on pricing. If you can't take your business to a competitor, the monopoly business can charge you whatever they want, and you can't do anything about it.

But focusing on pricing alone doesn't help when regulators look at companies like Facebook or Google, because the financial cost to the individual user is $0. Instead, we pay in different ways—primarily with our personal data.

In a June speech, DOJ Antitrust Division chief Makan Delrahim laid out his thinking for a way that privacy considerations could be an offshoot of a business' outsized market power and therefore of concern to antitrust regulators.

"Price effects alone do not provide a complete picture of market dynamics," Delrahim said. "Diminished quality is also a type of harm to competition. As an example, privacy can be an important dimension of quality. By protecting competition, we can have an impact on privacy and data protection."

What's more, he added, "Two companies can compete to expand privacy protections for products or services, or for greater openness and free speech on platforms. Where competition pushes companies to develop quality elements that better satisfy consumer preferences, our enforcement can protect that sort of competition, too."

Will Facebook care?

The winds of largely hands-off regulation have blown Facebook to smashing international success. But if those winds change, so might the company's fortunes.

In addition to the FTC and DOJ probes, Facebook and other big tech firms also face scrutiny from Congress, which last month launched a bipartisan investigation into the companies' reach and behavior.

And in the US, of course, regulatory cycles follow political cycles. Sen. Elizabeth Warren (D-Mass.) in March called for breaking up Amazon, Facebook, and Google as one of her many policy proposals in her campaign to be the Democratic nominee in the 2020 presidential race.

Regulation is one of the biggest risks for Facebook, the company said in its quarterly financial filing. The company warned it could have stalled growth or could outright lose some of its 2.4 billion users if "there are changes mandated by legislation, regulatory authorities, or litigation that adversely affect our products or users," or if it sees decreased engagement as part of changes it implemented in response to the GDPR in Europe and similar changes it made in the US.

"We have been subject to regulatory and other government investigations, enforcement actions, and settlements, and we expect to continue to be subject to such," Facebook added, which could "incur substantial costs or require us to change our business practices in a matter materially adverse to our business."

If it seems like all the regulators are suddenly piling on… well, they kind of are, and it's a global movement for a global company.

Germany's competition regulator, the Bundeskartellamt, said in February it was placing sweeping restrictions on how Facebook and its subsidiaries gathered and used user data.

Facebook is appealing the German order as well as a similar ruling from Belgium. It is also under investigation in Ireland.

https://arstechnica.com/?p=1541515

TV blackouts hit record high as customers get screwed by industry squabbles

Getty Images | AndreyPopov

reader comments

7 with 7 posters participating

Share this story

Broadcast TV stations are being blacked out on cable and satellite TV systems in record numbers this year, with 230 blackouts so far in 2019.

That beats the record of 213 blackouts set in 2017, even though 2019 is just seven months old. The 230 figure represents a huge rise over the eight blackouts seen in 2010 and 42 in 2011, according to a pay-TV industry advocacy group.

Blackouts has mostly been trending up in the past decade, though the number frequently goes down one year before rising again the next. There were 90 blackouts in 2012, 119 in 2013, 94 in 2014, 193 in 2015, 104 in 2016, 213 in 2017, and 165 in 2018.

These numbers, which are indicative of an industry battle

between pay-TV providers and programmers, were released this week by the American Television Alliance (ATVA). The lobby group represents TV providers from the cable, satellite, and telecom sectors.

Pay-TV companies have increasingly been refusing to pay the channel-carriage prices demanded by owners of broadcast networks. When a broadcaster demands a certain rate for carrying its TV channel and a cable or satellite company refuses to pay it, a blackout results.

Lobbyists for the pay-TV and programming industries each offer self-serving arguments about how the other is ruining broadcast TV and causing consumer prices to rise. “If their demands for higher fees are not met, broadcasters yank their signals from consumers, leaving you without your favorite programming indefinitely,” the ATVA says on its website. “Broadcasters black out their channels until their ransom demands are met. And when they are, it results in much higher prices for you, the consumer.”

The National Association of Broadcasters (NAB) didn’t dispute the blackout numbers provided by the ATVA, but it offered a different interpretation.

“We believe there’s a deliberate strategy on the part of pay-TV companies AT&T and Dish Network to force retransmission consent disruptions,” an NAB spokesperson told Ars. “AT&T and Dish have been involved in 85 percent of disruptions in the last few years; AT&T [via its DirecTV and U-verse TV services] has had seven impasses in the last 7 weeks (averaging one a week).”

The NAB claims that TV providers are creating the blackout problem in an attempt to convince Congress to change the law in their favor.

“This strategy is timed around Congress’s review of a satellite TV bill,” specifically a reauthorization of the

Satellite Television Extension and Localism Act (STELA), the NAB told Ars. “We think the strategy is to force disruptions, then cry to Congress that ‘the system is broken’ in hopes that Congress will add an amendment to the satellite TV bill.”

The ATVA argues that Congress should “modernize the retransmission consent rules, which currently favor broadcasters at the expense of consumers and competition.”

Retransmission consent

Broadcast stations are freely available to consumers with over-the-air antennas, but TV providers have to get retransmission consent from broadcast stations to carry their channels. Under US law, broadcasters can choose “must-carry” status, which forces cable operators to air their programming but doesn’t require payment. Alternatively, broadcast stations can use the retransmission consent model to demand carriage fees from TV providers, with the risk of blackouts occurring when the sides don’t agree on price.

The ATVA says that broadcasters collected $10.1 billion in retransmission fees in 2018, up from $9.3 billion in 2017. The retransmission fees totaled only $200 million in 2006, the group said.

“Since 2010, millions of Americans have seen dark screens instead of watching their favorite channels due to more than 1,000 broadcaster-initiated blackouts,” the lobby group said. ATVA members include AT&T, Verizon, Charter, CenturyLink, Dish, a lobby group for small cable companies, and other industry members.

On Saturday last week, CBS was blacked out on DirecTV in Los Angeles, New York, and other cities. Also recently, “Meredith Corporation caused a massive TV blackout on July 16, 2019, pulling its signal from millions of Dish Network customers in 12 television markets in 18 states,” the ATVA said last week.

“In addition to Meredith’s blackout of Dish Network customers, Nexstar is currently blacking out millions of DirecTV, U-verse and DireTV Now customers, in approximately 100 cities across the US, denying access to 125 local stations.”

Satellite TV struggles

A CableFax article points out that blackouts are affecting satellite TV systems more than cable networks, which have the luxury of increasing revenue from broadband.

“For the most part, cable operators have decided that video subscriber losses, at least within reason, don’t really matter all that much, so they don’t feel the same pressure to drive a hard bargain,” MoffettNathanson analyst Craig Moffett told Cablefax. “If the price of video rises, and video subscribers decide to leave as a result, so be it. Their broadband relationship with the customer will still be fine. Satellite operators don’t have the same luxury. They have to scrounge under the sofa cushions for every spare coin they can find.”

AT&T is both a pay-TV provider and broadband-network operator, but its home Internet service is only available in parts of its nationwide satellite-TV territory.

AT&T and other TV providers have complained for years about rising programming costs in general, not just for broadcast stations. One counter-strategy TV providers have used is to buy large programmers, like AT&T did with Time Warner in a deal finalized last year. But that doesn’t stop the AT&T-owned Time Warner from charging high prices for its content, and the industry consolidation hasn’t prevented TV users from being charged ever-higher prices.

AT&T claimed that its Time Warner merger would lower prices for consumers, but AT&T has since been raising them instead. AT&T is also starting to pull Time Warner shows off Netflix in order to make them exclusive to an upcoming service it calls

HBO Max.

Trading blame

NAB CEO Gordon Smith lambasted TV providers yesterday in a speech in which he pointed out that AT&T has played a role on both sides of programming disputes since it purchased Time Warner. AT&T buys carriage rights from other programmers so it can offer TV bundles through DirecTV and U-verse, but AT&T also charges other TV providers for access to Time Warner channels. AT&T isn't the only one in such a position, as Comcast has been the proud owner of NBCUniversal since 2011.

"AT&T collects $6 billion annually in affiliate fees from its own Warner Media cable properties like TNT, TBS, CNN and Cartoon Network," Smith said.

Despite that high price, "these cable networks' ratings pale in comparison to the ratings of local broadcast affiliates," Smith continued. "Last year, the typical Big Four TV broadcast affiliate delivered on average nearly four times more viewers every night than even the most-watched Warner Media channel."

Retransmission consent "is a free-market system that works," and the prices charged by broadcast networks are fair, Smith argued.

"If not for the compensation broadcasters receive for their highly-valued programming—programming that AT&T, Dish and others re-sell to customers—broadcasters would be unable to support investigative journalism and expensive sports coverage and invest in sophisticated weather operations that save lives and provide in-depth local news coverage," Smith said.

The ATVA responded, saying that retransmission consent fees "have been the fastest rising part of pay-TV bills for over a decade."

"Rather than using a calculated political pivot to deflect

blame and preserve their ‘special’ status enshrined in current law, broadcasters should stop demanding unacceptable price increases for channels with continually declining viewership,” the ATVA said. “Consumers should no longer have to pay more for what they are watching less.”

AT&T also disputed broadcaster arguments, telling Variety and other news outlets that broadcast stations “continue to give their signals away for free but also demand unsustainably growing fees for allowing customers the convenience of receiving their channels in a usual program guide or without switching an input.”

AT&T urges its DirecTV customers to use antennas to get broadcast stations during blackouts, and even provides the antennas at no extra cost.

https://arstechnica.com/?p=1541159

FTC fines Facebook $5 billion, imposes new privacy oversight

Enlarge / The company can afford to shrug it off.

reader comments

7 with 7 posters participating

Share this story

The Federal Trade Commission today announced a long-rumored, record-smashing $5 billion settlement with Facebook over allegations related to user privacy.

The fine is high, and the settlement demands more privacy oversight at the company. But what the deal does *not* do is find anyone, including CEO Mark Zuckerberg, personally responsible, nor does it mandate huge changes to the way Facebook collects data—only to the way it makes disclosures and honors user settings.

Facebook repeatedly "subverted users' privacy choices to serve its own business interests," the FTC said in the order (PDF). The company's actions violated a previous settlement requiring Facebook to adhere to certain privacy guidelines.

The commission voted 3-2 along party lines to support the settlement. The two commissioners who voted against adopting the settlement, Democrats Rebecca Kelly Slaughter and Rohit Chopra, said it went nowhere near far enough, leaving Facebook ample room to get up to mischief in the future.

What it's all about

The biggest set of charges in the settlement relate to Facebook allowing third-party app developers to access data about users' friends, without saying they were doing so—the heart of the Cambridge Analytica scandal.

"At least tens of millions of American users relied on Facebook's deceptive privacy settings and statements to restrict the sharing of their information," the complaint says, "When, in fact, third-party developers could access and collect their data through their friends' use of third-party developers' apps."

The settlement reflected several charges about how Facebook

handled third-party app permissions for years, all brought to light by investigations that began in the wake of the Cambridge Analytica revelations.

Additionally, the FTC said Facebook violated the earlier order by "misrepresenting" consumers' ability to opt out of facial recognition by using phone numbers provided for two-factor authentication for advertising purposes without notifying users and by storing user passwords without encryption.

The $5 billion penalty is equivalent to about 9% of Facebook's annual revenue, or 23% of its 2018 profit, FTC Chairman Joseph Simons said, adding that the fine is "unprecedented in global privacy enforcement" and "one of the largest civil penalties for any type of conduct in US history, alongside cases involving enormous environmental damage and massive financial fraud."

In addition to the blockbuster $5 billion deal, regulators also announced two separate, smaller settlements related to Facebook's privacy practices today. The first is a $100 million settlement between the FTC and Cambridge Analytica, the company of data scandal fame. The FTC charged Cambridge Analytica, along with developer Aleksandr Kogan and former CEO Alexander Nix, with deceiving customers by claiming they did not collect any personally identifiable data when, in fact, they did.

The US Securities and Exchange Commission also accused Facebook of deception, but of investors rather than of users. Facebook is paying $100 million to settle charges that, for two years, its disclosures "presented the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data," the SEC said.

The terms

In addition to the $5 billion fine, which goes straight to the US Treasury, the new order requires Facebook to establish and adhere to a new governance structure for reviewing user privacy on its services, including Instagram and WhatsApp.

The company's board of directors must form an independent privacy committee, removing "unfettered control" of decisions affecting user privacy from CEO Mark Zuckerberg. Members of that privacy committee will be nominated by a separate independent nominating committee, and they can only be removed by a supermajority of the eight-member board.

The agreement also requires that committee to designate specific compliance officers who will be responsible for handling privacy compliance at Facebook. Only that committee can remove those compliance officers, the FTC noted, not Zuckerberg or other Facebook employees.

In addition to FTC monitoring, a third-party entity will also regularly review Facebook's data collection practices for the next 20 years. That assessor's findings "must be based on the assessor's independent fact-gathering, sampling, and testing, and must not rely primarily on assertions or attestations by Facebook management," the FTC said.

Both Zuckerberg and the compliance officers must submit quarterly and annual privacy certifications to the FTC, guaranteeing the company's compliance. Both civil and criminal penalties are possible if those certifications are found to be false.

The company must also agree to a litany of other requirements, including greater oversight of third-party apps, beefed up disclosures about facial recognition, the establishment of a new data security program, and more.

Facebook in a statement said the settlement would bring "rigorous new standards for protecting your privacy."

The agreement "will require a fundamental shift in the way we approach our work" and will "mark a sharper turn toward privacy, on a different scale than anything we've done in the past," the company continued. "The accountability required by this agreement surpasses current US law and we hope will be a model for the industry."

Facebook's statement omits the fact that the US does not have a national privacy law.

Transparency not included

Slaughter said in her dissent (PDF) that the settlement "falls short" against the allegations in the case. "I don't think the terms in this order go far enough to change Facebook or ensure accountability," she said. "There are no substantive limitations on Facebook's data collection, use, and sharing. And there is no public transparency."

The record "more than justified initiating litigation against Facebook and Mr. Zuckerberg," Slaughter said. "When executives at large companies exercise control over decisions, including decisions to break the law, they should be held accountable the same way executives at smaller companies are."

Although going to court does carry the risk of losing your case, "even an adverse finding or a lackluster remedy can further the public good," she wrote. "Disappointing results help build the public case that there are deficits in the law that Congress must address."

Aside from the issue of suing Zuckerberg, Slaughter said, the $5 billion, while an objectively large sum of money, is nowhere near enough. "I regard the injury to the public and the institutions of our democracy to be quite substantial,"

she said. Facebook could and should easily pay much more, she said, since FTC orders, such as the 2011 one the company now stands accused of violating, clearly do not motivate it to behave better.

Chopra's dissent (PDF) voiced similar sentiments.

Nothing in the order gives Facebook any incentive to leave its lucrative behavioral advertising model behind, and so in the long run, nothing will change, Chopra said:

> *This thirst for data has led the company to harvest intimate, personal details about tens of millions of Americans on a scale and scope that are almost unimaginable. Facebook's data collection is both ongoing and increasing, as the company continues to add new means of surveillance that can be difficult to avoid. To facilitate further data acquisition, Facebook grants itself the right to surveil, own, and monetize users' private information by binding them to constantly evolving take-it- or-leave-it terms at sign-on.*

The $5 billion fine "makes for a good headline," he wrote, "but the terms and conditions, including blanket immunity for Facebook executives and no real restraints on Facebook's business model, do not fix the core problems that led to these violations."

A win for Facebook?

Technology expert Ashkan Soltani, who served as the FTC's chief technologist for a time during the Obama administration, said on Twitter that the settlement "was a *terrible* outcome for our leading privacy regulator and a very sweet deal for Facebook." He added that, "If this were a game of chess, Facebook just checkmated FTC, flipped the board so it couldn't be played again, and covered the whole thing up with a blanket."

Soltani is not alone in his assessment. Several lawmakers have already heaped scorn on the arrangement. “The FTC not only fell short, it fell on its face,” Sen. Edward Markey (D-Mass.) said. “Facebook is getting away with some of the most egregious corporate bad behavior in the age of the Internet,” he added. “This outcome is an insult to consumers.”

The frustration isn’t limited to Democrats, either. “This is very disappointing,” Sen. Josh Hawley (R-Mo.) said. “This settlement does nothing to change Facebook’s creepy surveillance of its own users and the misuse of user data. It does nothing to hold executives accountable. It utterly fails to penalize Facebook in any effective way.”

FTC Chairman Simons, for his part, pointed to the law as the major issue. For the second time in a week, he called on Congress to pass privacy legislation and give the FTC authority to enforce it.

“We are a law enforcement agency without the authority to promulgate general privacy regulations,” Simons said. “Our authority in this case comes from a 100-year-old statute that was never intended to deal with privacy issues like the ones that we address today.”

The commission only had two choices, he continued: “One, settle on excellent terms—or two, litigate for years and likely come away, even from a favorable court decision, with far less relief than we announced today. Would it have been nice to get more? To get $10 billion instead of $5 billion, for example? To get greater restrictions on how Facebook collects, uses, and shares data?”

Maybe so, Simons implied, but the agency “cannot impose such things by our own fiat.”

https://arstechnica.com/?p=1540807

After outcry, DoorDash promises workers will get 100% of tips

Enlarge / DoorDash CEO Tony Xu.
David Paul Morris/Bloomberg via Getty Images

reader comments

114 with 69 posters participating, including story author

Share this story

In recent months, food delivery company DoorDash has faced a growing backlash over a compensation formula that critics said amounted to DoorDash pocketing drivers' tips. On Tuesday evening, DoorDash CEO Tony Xu announced on Twitter that the company would change its compensation formula so that drivers' "earnings will increase by the exact amount a customer tips on every order."

"It's clear from recent feedback that we didn't strike the right balance," Xu tweeted.

Xu insists that DoorDash never intended to take drivers' tips. Rather, he said, the goal was to protect drivers from low earnings in cases where a customer failed to tip. If a driver's total pay for a job—DoorDash's base rate plus any customer tip—fell below a DoorDash-determined minimum, DoorDash would make up the difference.

Of course, this is mathematically equivalent to a system where DoorDash simply pays every worker a standard rate but confiscates the first few dollars of every tip.

A recent New York Times story explained how the DoorDash's current system works:

> *For my first order, the guarantee was $6.85 and the customer, a woman in Boerum Hill who answered the door in a colorful bathrobe, tipped $3 via the app. But I still received only $6.85. If the woman in the bathrobe had tipped zero, DoorDash would have paid me the whole $6.85. Because she tipped $3, DoorDash kicked in only $3.85. She was saving DoorDash $3, not tipping me.*

Now Xu says DoorDash is going to revamp its pay system to ensure that every dollar of tip goes to drivers. "We'll have specific details in the coming days," he tweeted.

There's no guarantee that the new formula will be better for workers. After Instacart changed its formula earlier this year, some shoppers complained that their average compensation per job fell as a result. Ultimately, the specific compensation formula probably matters less than how much DoorDash chooses to pay its workers, on average.

DoorDash isn't the only company to face a backlash over this issue. Instacart was featured alongside DoorDash in a February piece by NBC's Olivia Solon. Instacart changed its policy days later, while it took months of additional criticism from The New York Times and others before DoorDash changed its approach.

Slate's April Glaser has a helpful roundup of the policies of other delivery companies. Most told her that workers get 100% of tips. Glaser said she couldn't get a clear answer from Amazon about whether tips are counted against workers' guaranteed base pay.

https://arstechnica.com/?p=1540925

DOJ to approve T-Mobile/Sprint merger despite 13 states trying to block it

reader comments

90 with 60 posters participating, including story author

Share this story

The Justice Department plans to approve the T-Mobile/Sprint merger as part of a settlement involving the sale of spectrum licenses, wholesale access, and a prepaid wireless business to Dish Network, The Wall Street Journal reported today.

“The companies have spent weeks negotiating with antitrust enforcers and each other over the sale of assets to Dish to satisfy concerns that the more than $26 billion merger of the No. 3 and No. 4 wireless carriers by subscribers would hurt competition,” the Journal wrote, citing people familiar with the matter.

As a result of those negotiations, the DOJ is “poised to approve” the merger and could announce a settlement with T-Mobile and Sprint “as soon as this week, but the timing remains uncertain,” the Journal wrote.

Even if the DOJ approves the merger, T-Mobile and Sprint will still have to defend it in court because of a lawsuit filed against them by 13 states and the District of Columbia.

Dish, the second-biggest satellite TV provider after AT&T's DirecTV, has been buying spectrum for years without ever launching cellular phone and data service. Previous reports about a settlement involving Dish said that Dish would get wholesale access to the T-Mobile/Sprint network, spectrum, and prepaid wireless carrier Boost Mobile. Boost is owned by Sprint and is a network reseller.

Today's Journal report said the pending settlement "provides for Dish to acquire prepaid subscribers" but didn't say whether those will come from Boost. Boost's involvement seems likely, given that Federal Communications Commission Chairman Ajit Pai's approval of the T-Mobile/Sprint merger is contingent on the divestiture of Boost Mobile and a guarantee that Boost will have access to the T-Mobile/Sprint network.

"Dish would also get a multiyear agreement to use the wireless companies' network while it builds dedicated infrastructure," the Journal wrote. The report didn't say how much spectrum Dish will get.

Dish to pay $5 billion

Bloomberg reported last night that Dish "agreed to pay $5 billion for wireless assets" in its deal with T-Mobile and Sprint. The deal includes $1.5 billion for prepaid mobile assets and $3.5 billion for spectrum licenses.

"Under the terms of the deal, Dish can't sell the assets or hand over control of the agreement to a third party for three years," Bloomberg wrote.

Dish becoming a major carrier could solve the problem caused

by the T-Mobile/Sprint merger, that it would reduce the number of major nationwide competitors from four to three. But Dish has famously dragged its feet in using its assets to build a wireless network, with T-Mobile CEO John Legere calling Dish a spectrum hoarder in February of this year. Even under a best-case scenario presented by the settlement with the government, it sounds like it could take Dish several years to build its own network and become a major threat to AT&T, Verizon, and the combined T-Mobile/Sprint.

https://arstechnica.com/?p=1540839

Judge allows suit against AT&T after $24 million cryptocurrency theft

Enlarge / An AT&T store in New Jersey.
Michael Brochstein/SOPA Images/LightRocket via Getty Images

reader comments

47 with 35 posters participating

Share this story

When Michael Terpin’s smartphone suddenly stopped working in June 2017, he knew it wasn’t a good sign. He called his cellular provider, AT&T, and learned that a hacker had gained control of his phone number.

The stakes were high because Terpin is a wealthy and prominent cryptocurrency investor. Terpin says the hackers gained control of his Skype account and tricked a client into sending a cryptocurrency payment to the hackers instead of to Terpin.

After the attack, Terpin asked AT&T to escalate the security protections on his phone number. According to Terpin, AT&T agreed to set up a six-digit passcode that must be entered before anyone could transfer Terpin's phone number.

But the new security measures didn't work. In January 2018, "an AT&T store cooperated with an imposter committing SIM swap fraud," Terpin alleged in his August 2018 lawsuit against AT&T. The thieves "gained control over Mr. Terpin's accounts and stole nearly $24 million worth of cryptocurrency from him."

Terpin sued AT&T, seeking at least $24 million in actual damage and millions more in punitive damages. Terpin also asked the court to void terms in AT&T's customer agreement that disclaim liability for security problems—even in cases of negligence by AT&T. Terpin argued that these boilerplate terms are unconscionable because customers never have an opportunity to negotiate them.

But AT&T asked the judge to dismiss the case, arguing that Terpin didn't adequately explain how the phone hack led to the loss of his cryptocurrency. Terpin's lawsuit provided no details about how Terpin had stored his cryptocurrency, how the hackers had gained access to it, or if they might have been able to carry out a similar attack without control of Terpin's phone number. In any event, AT&T argued that it shouldn't be held responsible for the misconduct of the hackers who actually carried out the theft of cryptocurrency.

A mixed ruling

On Thursday, Judge Otis Wright—a man we once depicted as a hulking green giant preparing to smash the copyright trolls at Prenda Law—issued a ruling that provided some reason for each side to celebrate.

Wright agreed with AT&T that Terpin had not adequately explained how the hack of his account led to the theft of his cryptocurrency or why AT&T should bear responsibility. As a result, he dismissed claims that relied on Terpin's claimed $24 million loss.

However, Wright dismissed the claims with "leave to amend," meaning that Terpin has 21 days to file a new version of his lawsuit that more fully explains how the cryptocurrency was stolen and why AT&T should be held responsible.

At the same time, Wright allowed the case to move forward with Terpin's arguments against AT&T's one-sided customer agreement. Wright hasn't yet voided the terms, but he found Terpin's arguments on the issue plausible enough to let the case continue.

This kind of phone hacking incident is of particular concern in the cryptocurrency world because of the non-reversibility of most virtual currencies. If a hacker steals funds from a conventional bank account, a fast-acting victim can usually get the transaction reversed and the funds restored. By contrast, if a hacker steals someone's bitcoins, they're likely to be gone permanently, since no one has the authority to cancel transactions once they're committed to the blockchain.

As a result, cryptocurrency is much more of a "user beware" world than the conventional banking system. If you own a significant amount of cryptocurrency—and especially if you're publicly known to have a significant amount of

cryptocurrency—then it’s wise to store it in a way that doesn’t depend on the security of your phone number.

https://arstechnica.com/?p=1540505

Tech firms “can and must” put backdoors in encryption, AG Barr says

Enlarge / Graffiti urging people to use Signal, a highly encrypted messaging app, is spray-painted on a wall during a protest on February 1, 2017 in Berkeley, California.
Elijah Nouvelage | Getty Images

reader comments

175 with 116 posters participating

Share this story

US Attorney General William Barr today launched a new front in the feds’ ongoing fight against consumer encryption, railing against the common security practice and lamenting the “victims” in its wake.

“The deployment of warrant-proof encryption is already imposing huge costs on society,” Barr claimed in remarks at a cybersecurity conference held at Fordham University Tuesday morning. Barr added that encryption “seriously degrades” law enforcement’s ability to “detect and prevent a crime before it

occurs," as well as making eventual investigation and prosecution of crime more difficult.

The existence of encryption means "converting the Internet and communications into a law-free zone" that criminals will happily take advantage of to do more crimes, Barr added, likening it to a neighborhood that local cops have abandoned.

The cost of encryption, he said, is measured in "victims" who might have been saved from crime if law enforcement had been able to lawfully intercept communications earlier.

He also accused tech firms of "dogmatic" posturing, saying lawful backdoor access "can be and must be" done, adding, "We are confident that there are technical solutions that will allow lawful access to encrypted data and communications by law enforcement, without materially weakening the security provided by encryption."

A long-running battle

In his diatribe, Barr is only picking up where predecessors left off. In 2017, then-deputy AG Rod Rosenstein said in an interview that the tech community's "absolutist position" on strong encryption impeded law enforcement and was "unreasonable."

Federal law enforcement has been in a very public encryption face-off with consumer electronics companies, particularly Apple, since 2016.

In December, 2015, a gunman killed and seriously injured dozens of victims in an attack in San Bernardino, California. The FBI ended up in possession of the shooter's iPhone during the investigation but was unable to unlock the device, as the attacker had been killed and therefore could not be compelled to share his PIN.

The FBI demanded Apple cooperate in unlocking the phone by

building a backdoor, and the company effectively told the feds to go pound sand. (The FBI eventually accessed the phone without Apple's help.)

The relationship between the FBI and companies such as Apple that promote encryption has remained frosty ever since. Last year, an FBI official called Apple "jerks" about encryption, accusing the company of an "evil genius" approach to thwarting law enforcement.

"Responsible" backdoors

Rosenstein proposed a so-called "responsible encryption" scheme back in 2017, a call Barr echoed.

"I am suggesting that it is well past time for some in the tech community to abandon the posture that a technical solution is not worth exploring and instead turn their considerable talent to developing products that will reconcile good cyber security to the imperative of public safety and national security," Barr said.

FBI Director Christopher Wray said last year that developing a process for allowing government officials lawful entry into encrypted communications would "entail varying degrees of innovation by the industry," but he said he didn't "buy the claim that it's impossible."

But no matter how many times government officials try to will such an option into existence, what they claim to want isn't actually possible. Security experts and product makers have said time and time again that introducing a backdoor—an access portal for a specific entity to gain access through—into an encryption scheme weakens the whole thing.

Apple CEO Tim Cook has repeatedly said consumer privacy is of paramount importance to his company and that it's in "everyone's best interest" for everyone to be "blocked out,"

with no secret backdoors.

Senator Ron Wyden (D-Ore.) in a 2018 letter to Wray (PDF) said the quest for a way in to encrypted communications amounts to “a flawed policy that would harm America’s security, liberty, and our economy.”

“Building secure software is extremely difficult,” Wyden added, “and vulnerabilities are often introduced inadvertently in the design process. Eliminating these vulnerabilities is a mammoth task, and experts are unified in their opinion that introducing deliberate vulnerabilities would likely create catastrophic unintended consequences that could debilitate software functionality and security entirely.”

https://arstechnica.com/?p=1540289