There’s a partisan schism over the timing of a Google antitrust lawsuit

Enlarge / Attorney General William Barr .

reader comments

21 with 20 posters participating

Share this story

Attorney General William Barr is pressuring the career lawyers at the Department of Justice to complete work on a potential antitrust case against Google by the end of September, The New York Times reports. It’s the latest sign of a long-simmering dispute within the government about the timing and scope of the government’s attack on the Silicon Valley behemoth.

Antitrust enforcement against Google has become a rare issue of broad bipartisan agreement. Fifty states and territories have joined a coalition preparing to bring its own antitrust lawsuit against Google. That means that most Republican-controlled states are participating in the effort, as are most Democratic-controlled states.

Liberals have traditionally favored vigorous enforcement of antitrust law across the economy. Conservatives have traditionally favored more restraint, but they seem particularly keen to enforce antitrust law against technology platforms they view as biased against conservatives.

As the 2020 election has neared, fault lines have emerged over the timing of a possible lawsuit. Barr has pushed for Justice

Department lawyers to wrap up their work quickly so that he can make a final decision on whether to file a lawsuit by the end of September. Some career Justice staffers have objected to that timeline, arguing that it gives them too little time to digest millions of pages of documents they have obtained from Mountain View. Some staffers worry Barr is pushing for quick action to give Donald Trump an accomplishment he can tout in the November election.

There has been a similar schism at the state level, with Republican officials seeking quick action and Democrats preferring to take the time necessary to build a bulletproof case.

Media reports indicate that a case against Google is likely to focus on its search engine and its advertising platform. Separate teams have been working to build a case that Google violated antitrust law in each of these areas. It's possible that states—and the federal government—could file a lawsuit on one of these issues first, perhaps adding the second issue down the road.

According to the Times, the Republican attorney general of Texas, Ken Paxton, believes he is nearly ready to bring a case focusing on Google's advertising practices, so that could be the focus of a lawsuit if one is filed in the coming weeks.

But if a coalition of Republican states and the Trump administration file a lawsuit against Google without buy-in from Democrats, that could create an opening for Google to portray the case as a politically motivated witch hunt. Some of Google's critics view it as important for Democrats and Republics to stay united in order to give the issue bipartisan appeal.

https://arstechnica.com/?p=1703535

Facebook’s plan to prevent election misinformation: Allowing it, mostly

Enlarge / Mark Zuckerberg speaking at Facebook’s F8 developer summit in 2018.

reader comments

43 with 34 posters participating

Share this story

Although it may feel like the campaigns have been going on forever and will continue forever, linear time inexorably marches on and we are, at last, exactly two months away from the 2020 US presidential election. The logistics alone are more complicated than ever this year, thanks to the COVID-19 pandemic, and voters around the nation are likely to encounter complications of one kind or another.

Into this milieu we now add Facebook. The company has a bad track record of being used as a tool of misinformation and manipulation when it comes to elections. In a Facebook post today, company CEO Mark Zuckerberg outlined a whole bunch of new steps the company will be taking to “protect our democracy” this year. Some of those measures, alas, feel like shutting the barn door when the horse left so long ago you forgot you ever even had one.

“This election is not going to be business as usual,”

Zuckerberg began, accurately. Misinformation about voting, the election, and both candidates for the presidency is already rampant on Facebook and every other media platform, and it's being spread by actors both foreign and domestic. So what is Facebook going to do about it? "Helping people register and vote, clearing up confusion about how this election will work, and taking steps to reduce the chances of violence and unrest," Zuckerberg promised.

Voting (mis)information

Facebook has for several weeks been plugging its voter information center in both Facebook and Instagram. That landing page takes a user's location—approximate or specific, if enabled—to display voter-registration information, vote-by-mail eligibility, voter ID requirements, and other state and local information. It also contains a voting-related fact-checking section, covering topics such as, "Both voting in person and voting by mail have a long history of trustworthiness in the US."

That will continue, Zuckerberg said, and the company will not only continue to enforce its policies against voter suppression, but expand them:

> *We already remove explicit misrepresentations about how or when to vote that could cause someone to lose their opportunity to vote—for example, saying things like "you can send in your mail ballot up to 3 days after election day", which is obviously not true. (In most states, mail-in ballots have to be *received* by election day, not just mailed, in order to be counted.) We're now expanding this policy to include implicit misrepresentations about voting too, like "I hear anybody with a driver's license gets a ballot this year", because it might mislead you about what you need to do to get a ballot, even if that wouldn't necessarily invalidate your vote by itself.*

Facebook is expanding its fact-checking in general to add labels to content that “seeks to delegitimize the outcome of the election or discuss the legitimacy of voting methods, for example, by claiming that lawful methods of voting will lead to fraud.”

Unfortunately, a primary source of exactly that kind of misinformation is the sitting US president, Donald Trump. Facebook has been slow to fact-check claims made by Trump or his campaign, but it does seem to be making good on appending labels to posts explicitly relating to voter misinformation. For example, the social media giant labeled this post Trump shared today around 10:45am EDT:

The labels, however, require a user to click through to find out what, exactly, the facts might be.

The homestretch

Zuckerberg also announced that Facebook will not accept any new “political or issue ads” during the final week of the campaign—so, beginning around October 27.

“In the final days of an election there may not be enough time to contest new claims,” he wrote, explaining the suspension. However: “Advertisers will be able to continue running ads they started running before the final week and adjust the targeting for those ads, but those ads will already be published transparently in our Ads Library so anyone, including fact-checkers and journalists, can scrutinize them.”

Unfortunately, the ads that political advertisers place before the deadline are allowed to be full of lies, and Facebook will not fact-check them. That’s been the company’s long-standing policy, and it evidently has no intention of reversing course for the rest of this campaign season. Fact-checkers and journalists *will* be scrutinizing the ads, as quickly as they can, but they may not have the same reach as a paid-for ad campaign that could be actively spreading falsehoods.

The final week before November 3 will no doubt be a valuable homestretch for campaigns—but it may prove less important than in previous years, as voters nationwide are expected to take advantage of early voting, mail-in voting, and mailed or in-person absentee voting to avoid exposure to groups and crowding in the continuing pandemic.

The Trump campaign vigorously objected to Facebook’s decision. “In the last seven days of the most important election in our history, President Trump will be banned from defending himself on the largest platform in America,” the campaign’s deputy national press secretary, Samantha Zager, said in a statement, adding that the president will be “silenced by the Silicon Valley Mafia.”

This is, of course, also false; Facebook's prohibition only applies to paid advertising, not posts created or shared by any individual, page, or campaign. Neither will it prevent Trump (or his rival, Democratic candidate Joe Biden) from issuing new ads on any other broadcast, print, or online platform or stop him from holding press conferences, delivering interviews, hiring a skywriter, or getting his message out in any and every other way.

The big day—and the aftermath

Facebook's stance with content by and large tends to be reactive, not proactive. The company is, however, proactively looking at ways to mitigate what are extremely likely to be high-tension feelings on election night itself.

Polls begin closing on the East Coast at 7pm ET and continue to close in waves over the following several hours. Typically, millions of Americans wait with their eyes glued to their favorite cable or broadcast network waiting for returns to come in and each state to be called. As we learned in 2000, however, reports come in at their own pace—not when viewers desperate for news want them to.

While the outcome in a state such as California or Alabama is *likely* to be a foregone conclusion, we are just as likely to have to wait hours or perhaps even days to learn the final outcomes in key swing states thanks to the projected increase in mail-in and absentee voting. Facebook is working now to try to teach its more than 200 million US users that this wait is not fraudulent and is, instead, a sign the system is working properly.

"We'll use the Voting Information Center to prepare people for the possibility that it may take a while to get official results," Zuckerberg said. "This information will help people understand that there is nothing illegitimate about not having a result on election night."

Facebook will also work on and after Election Day to fact-check any claim of victory that is not backed up by its partners, Reuters and the National Election Pool. The election module will show results as they come in, and Facebook will "notify people proactively" as those results become available. Most importantly, Zuckerberg added, "If any candidate or campaign tries to declare victory before the results are in, we'll add a label to their post educating that official results are not yet in and directing people to the official results."

The platform is also trying to strengthen enforcement against "militias, conspiracy networks like QAnon, and other groups that could be used to organize violence or civil unrest in the period after the elections," Zuckerberg said.

The FBI determined extremist movements, including QAnon, to be threats more than a year ago, but the content was allowed to proliferate on social networks until very recently. Twitter banned QAnon activity in July, calling it "coordinated harmful activity" that spread offline into real-world injury. The conspiracy movement has been linked to several violent episodes, including a kidnapping and a murder.

Facebook, however, has a record of failing to act against violent threats until it's too late. The company cracked down on QAnon about two weeks ago, removing thousands of Facebook and Instagram groups, pages, and accounts.

As The Verge's Casey Newton pointed out, that's probably already too little, too late.

"On its face, [QAnon] seems no less a joke than the idea that TidePods secretly taste delicious," Newton wrote. "But as with the laundry detergent, thousands of Americans have now been poisoned by QAnon, and the consequences seem likely to be far more dire, and long-lasting."

https://arstechnica.com/?p=1703304

Why experts are overwhelmingly skeptical of online voting

Aurich Lawson / Getty Images

reader comments

120 with 68 posters participating, including story author

Share this story

If anyone was going to be enthusiastic about online voting, it would be Ben Adida. After starting multiple dot-com startups in the late 1990s and early 2000s, Adida earned a computer science PhD from MIT in 2006. Studying under legendary cryptographer Ron Rivest (the “R” in RSA) at MIT, Adida explored how to use advanced cryptography to hold provably secure elections.

Adida created open-source online voting software called Helios based on that research. And more recently, he founded VotingWorks, a non-profit organization that creates open-source software for ballot-marking machines and post-election auditing.

“If I felt like Internet voting was viable, I would be really well-positioned to do it,” Adida told Ars in a recent phone interview. “I did my PhD on it. I run Helios as a side project.”

But Adida told us that online systems like Helios are “great for student elections, not for public elections.”

“Every couple of months I get someone who says can we use Helios for a public election,” Adida said. “I say, ‘You really shouldn’t.'”

That theme was echoed by other election security experts I talked to in recent weeks. Take David Becker, the executive director of the Center for Election Innovation and Research. He’s generally an advocate for the use of digital technology in elections. For example, he’s a staunch supporter of the controversial touchscreen ballot-marking devices used in Georgia elections. But like Adida, he argues we’re nowhere close to having technology to securely cast votes on the Internet. “I’ve not seen any evidence that we can do so verifiably, securely, and auditably,” Becker told Ars last month.

In 2018, West Virginia experimented with allowing 144 overseas service members to vote online using an app called Voatz. And this February, West Virginia passed legislation to expand online voting to disabled voters. The state was widely expected to again use Voatz for this, but West Virginia switched to software called OmniBallot for the June 2020 primary. It’s not clear what voting technologies West Virginia will use in November’s election.

Voatz CEO Nimit Sawhney has an ambitious vision for the future of American democracy. In two hour-long interviews with Ars—one in June, the other this week—he argued that everyone should have the option to cast votes online. He’s frustrated by widespread skepticism about online voting among election security experts like Adida and Becker.

Enlarge / A look at the Voatz app interface (Android version)
“How can you claim it’s settled science that Internet voting can never be safe?” he asked in a June interview. “Three hundred years ago we knew the Earth was flat and the Sun was revolving.”

Few of the experts I talked to said online voting could never be safe. But almost all of the independent experts I interviewed said it would be many years—if not decades—before it was feasible to build a secure voting system online.

Voatz is far from the only company working on online voting—other online voting systems have gotten equally harsh reviews from security experts. In June, we covered research by MIT computer scientist Michael Specter and the University of Michigan’s Alex Halderman that analyzed OmniBallot.

“We find that OmniBallot uses a simplistic approach to

Internet voting that is vulnerable to vote manipulation by malware on the voter's device and by insiders or other attackers who can compromise Democracy Live, Amazon, Google, or Cloudflare," the researchers wrote. "Using OmniBallot for electronic ballot return represents a severe risk to election security and could allow attackers to alter election results without detection."

MIT researchers found serious flaws

Voatz offers what seems like a simplified voting solution. Registered voters start with a smartphone app available for both iOS and Android. Votes are transmitted to servers hosted on Amazon Web Services and a copy is stored to a blockchain. The blockchain supposedly offers extra security by making it harder to tamper with votes later.

Last year, after it has already been utilized in a state election system, researchers from MIT undertook one of the first in-depth, independent reviews of Voatz software. "We find that Voatz has vulnerabilities that allow different kinds of adversaries to alter, stop, or expose a user's vote," the researchers wrote in February.

The researchers didn't have access to Voatz servers, so they focused their analysis on Voatz's mobile app. One of their big findings was that Voatz's protections against on-device malware were ineffective. The Voatz app comes with software called Zimperium that scans a smartphone for known malware and prevents the app from running if it is detected. But the MIT researchers demonstrated that it was possible to modify the Voatz app to prevent Zimperium from running in the first place.

Once these security checks are disabled, the Voatz app can be modified to undetectably change voters' choices. "It is straightforward to modify the app so that it submits any attacker-desired vote, yet presents the same UI as if the app

recorded the user’s submitted vote,” the researchers wrote.

The MIT study got a scathing response from Voatz. The company complained that the researchers had studied an outdated version of the Android app. And without access to the real Voatz servers, Voatz wrote, the researchers “fabricated an imagined version of the Voatz servers, hypothesized how they worked, and then made assumptions about the interactions between the system components that are simply false.”

https://arstechnica.com/?p=1699485

NSA spying exposed by Snowden was illegal and not very useful, court says

reader comments

46 with 31 posters participating

Share this story

The National Security Agency’s bulk collection of phone metadata from telecom providers was illegal, a federal appeals court ruled yesterday. The court also found that the phone-metadata collection exposed by former NSA contractor Edward Snowden was not necessary for the arrests of terror suspects in a case that the US government cited in defending the necessity of the surveillance program.

The ruling by the US Court of Appeals for the 9th Circuit upheld the 2013 convictions of "four members of the Somali diaspora for sending, or conspiring to send, $10,900 to Somalia to support a foreign terrorist organization." But the Somalis' challenge of the NSA spying program yielded some significant findings. In part, the ineffectiveness of the phone-metadata collection helped ensure that the convictions would be upheld because the illegally collected metadata evidence wasn't significant enough to taint evidence that was legally collected by the government. The government got what it needed from a wiretap of defendant Basaaly Saeed Moalin's phone, not from the mass collection of metadata.

The court's three-judge panel unanimously "held that the metadata collection exceeded the scope of Congress's authorization in 50 U.S.C. § 1861, which required the government to make a showing of relevance to a particular authorized investigation before collecting the records, and that the program therefore violated that section of FISA [Foreign Intelligence Surveillance Act]," the ruling said.

The judges also wrote that "the government may have violated the Fourth Amendment when it collected the telephony metadata of millions of Americans, including at least one of the defendants." But the judges didn't make a ruling on the potential Fourth Amendment violation because it wasn't necessary to decide the case. While "the Fourth Amendment requires notice to a criminal defendant" when prosecutors want to use evidence from surveillance at trial, the judges "did not decide whether the government failed to prove any required notice in this case because the lack of such notice did not prejudice the defendants," the ruling said.

US admits metadata "not necessary"

The NSA's bulk collection that "swept up the full call records of every customer of America's biggest telephone companies,"

authorized by the USA Patriot Act in 2001, "was banned in 2015 as part of the USA Freedom Act," a Project on Government Oversight report notes. The program was replaced by a more targeted collection of phone-company records, which was reportedly halted in 2018.

Moalin has been disputing his conviction since shortly after Snowden's revelations in 2013. As the Brennan Center for Justice said in November 2015, "*Moalin* is the only instance identified by the government where the NSA's mass surveillance program has been used in a terrorism prosecution."

The NSA told Congress in 2013 that the Moalin case demonstrated the value of the mass phone-records collection. But in 2016, US government officials said in a filing at the 9th Circuit that Moalin's telephony metadata "did not and was not necessary to support the requisite probable cause showing for the FISA Title I application."

In yesterday's ruling, judges said that classified evidence confirmed that the metadata wasn't necessary:

> *Our review of the classified record confirms this representation. Even if we were to apply a "fruit of the poisonous tree" analysis, we would conclude, based on our careful review of the classified FISA applications and related information, that the FISA wiretap evidence was not the fruit of the unlawful metadata collection. Again, if the statements of public officials created a contrary impression, that impression is inconsistent with the facts presented in the classified record. Because the wiretap evidence was not "unlawfully acquired," suppression [of that evidence] is not warranted.*

It's not clear what evidence the government cited in its application for that wiretap because the application is classified. But the judges wrote that "under established Fourth Amendment standards, the metadata collection, even if

unconstitutional, did not taint the evidence introduced by the government at trial."

Mass surveillance

Besides being illegal and ineffective, the NSA spying program violated the privacy of millions of Americans. "[T]he NSA collected Moalin's (and millions of other Americans') telephony metadata on an ongoing, daily basis for years," the judges wrote. Referring to a ruling from a different case on cell-phone location information, the 9th Circuit judges said that "telephony metadata, 'as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls… permit something akin to… 24-hour surveillance.' This long-term surveillance, made possible by new technology, upends conventional expectations of privacy."

Judges noted that the NSA metadata-collection program caused a "public outcry" when it was revealed, for good reason:

> *Also problematic is the extremely large number of people from whom the NSA collected telephony metadata, enabling the data to be aggregated and analyzed in bulk… A couple of examples illustrate this point: A woman calls her sister at 2:00 a.m. and talks for an hour. The record of that call reveals some of the woman's personal information, but more is revealed by access to the sister's call records, which show that the sister called the woman's husband immediately afterward. Or, a police officer calls his college roommate for the first time in years. Afterward, the roommate calls a suicide hotline. These are simple examples; in fact, metadata can be combined and analyzed to reveal far more sophisticated information than one or two individuals' phone records convey.*

https://arstechnica.com/?p=1703409

National Institutes of Health disses FDA on plasma as COVID treatment

Enlarge / Francis Collins, director of the U.S. National Institutes of Health, reportedly objected to the FDA's decision to grant an Emergency Use Authorization to plasma treatments.

reader comments

88 with 60 posters participating, including story author

Share this story

Last week, the FDA announced that it was issuing an emergency use authorization for the treatment of COVID-19: the blood plasma of people who have recovered from a COVID-19 infection. But controversy quickly engulfed that announcement after it became clear that the head of the FDA had exaggerated the effectiveness of the treatment when explaining why it was being approved.

The FDA's salesmanship of blood plasma—which is a treatment of unknown efficacy—was taken as evidence that the emergency use authorization was the product of political pressure exerted by a Trump administration anxious to have some good news to promote its reelection campaign. Additionally, health experts

at the National Institute of Health (NIH) didn't agree with the decision and had tried to block it a week ago. Now, the NIH may be striking back, releasing a document that basically says it's looked at the evidence and is not convinced.

Not so fast

While the CDC and FDA have led some aspects of the coronavirus response, the NIH is the employer of Anthony Fauci and the largest biomedical research organization in the world. So it certainly has things to say about how to handle the pandemic, and it maintains a COVID-19 Treatment Guidelines Panel. This, as its name implies, maintains guidelines on different aspects of care for the disease. So, given that the FDA has just given an Emergency Use Authorization to a treatment, it essentially forced the NIH to respond in some way.

And the NIH's response is both accurate and forceful. "There are currently no data from well-controlled, adequately powered randomized clinical trials that demonstrate the efficacy and safety of convalescent plasma for the treatment of COVID-19," the document says. The document makes clear that the Panel has reached that conclusion by examining all the published data as well as a number of unpublished studies. It contrasts that with the FDA, which based its decision on a subset of the population enrolled in a single study that lacked a control arm.

Even with that carefully selected population, the Panel notes, the analysis "found no difference in 7-day survival overall." It was only when groups were split out based on the amount of anti-SARS-CoV-2 antibodies present that a small difference emerged.

But the NIH remains unimpressed, noting that, without randomization and a control group, other factors could have accounted for this difference. And, in any case, it's clear that the levels of useful antibodies present vary from donor

to donor.

The Panel sums up the situation bluntly. “There are insufficient data to recommend either for or against the use of convalescent plasma for the treatment of COVID-19,” it concludes, before going on to say “Convalescent plasma should not be considered standard of care for the treatment of patients with COVID-19.” In fact, the document raises the possibility that using antibodies from other sources could dampen the production of the COVID-19 patient’s own antibodies and thus limit future protections.

Is this a warning?

It’s important to emphasize that everything the NIH’s document says is accurate. There aren’t any large, well-designed studies of the efficacy of post-infection plasma as a treatment. And the small studies cited by the FDA in its emergency use authorization don’t indicate that it’s an effective therapy. So, while doctors may be authorized to use it, it certainly shouldn’t be viewed as the standard of care. Nevertheless, the NIH’s blunt dismissal of the evidence presented by the FDA to support its decision is striking.

Given that members of the NIH’s leadership, including its director Francis Collins, had reportedly attempted to put the FDA’s authorization on hold, it’s very tempting to speculate that this is a way of calling out the FDA for making a decision with limited scientific support. It also comes on the heels of a former NIH director, Harold Varmus, calling out the Centers for Disease Control for similar reasons. It’s not clear, however, whether these public criticisms will be enough to keep these agencies focused on scientific data as the election grows ever closer.

https://arstechnica.com/?p=1702880

Trump administration forces Facebook and Google to drop Hong Kong cable

Enlarge / Police on the streets of Hong Kong, where demonstrators continue to protest the erosion of freedoms.

reader comments

113 with 62 posters participating

Share this story

Google and Facebook have withdrawn plans to build an undersea cable between the United States and Hong Kong after the Trump administration raised national security concerns about the proposal. On Thursday, the companies submitted a revised plan that bypasses Hong Kong but includes links to Taiwan and the Philippines that were part of the original proposal.

One of the original project's partners, Hong Kong company Pacific Light Data Communication, has been dropped.

Federal law requires a license from the Federal Communications Commission to build an undersea cable connecting the United States with a foreign country. When Google and Facebook submitted their application for an undersea cable connecting the US to Hong Kong, Taiwan, and the Philippines, a committee of federal agencies led by the Justice Department recommended against approving the connection to Hong Kong, citing the "current national security environment."

The Trump administration cited “the [People’s Republic of China] government’s sustained efforts to acquire the sensitive personal data of millions of U.S. persons” as a reason to deny the application.

The proposed cable’s “high capacity and low latency would encourage U.S. communications traffic crossing the Pacific to detour through Hong Kong before reaching intended destinations in other parts of the Asia Pacific region,” the government argued.

Until recently, Hong Kong enjoyed a significant amount of autonomy from China’s government in Beijing, allowing Hong Kong to offer its citizens substantially stronger civil liberties than those enjoyed on the mainland. That, in turn, gave companies greater comfort doing business in Hong Kong.

But in recent months, the firewall between Hong Kong and the mainland has collapsed. A new national security law gives the mainland government the power to arrest Hong Kongers for vague offenses like “separatism” and “subversion.” As a result, Western governments and companies are increasingly treating Hong Kong as just another city in China.

https://arstechnica.com/?p=1702497

AT&T reportedly trying to sell DirecTV after massive customer losses

reader comments

163 with 130 posters participating

Share this story

AT&T is reportedly trying to sell DirecTV to private-equity investors just five years after buying the satellite provider. The negotiations with potential buyers come after millions of customers ditched DirecTV over the past two years and could value DirecTV at much less than the $49 billion AT&T paid for it.

“AT&T is seeking private-equity investors to buy the majority of its DirecTV satellite-television business, helping it cope with a major drag on its operations, according to people familiar with the situation,” Bloomberg wrote yesterday. AT&T and its advisers at Goldman Sachs “have been in talks with private-equity suitors about the satellite TV unit,” with potential bidders including Apollo Global Management and Platinum Equity, The Wall Street Journal reported.

AT&T could end up selling DirecTV for far less than it paid five years ago. “Any deal for the satellite TV service would be sizable but likely a far cry from the $49 billion AT&T paid for it in 2015,” the Journal wrote, quoting sources familiar with the talks as saying that “a deal could value the business below $20 billion.”

7 million subscribers lost since mid-2018

A sale is by no means a certainty, and AT&T could retain a minority stake in DirecTV even if a sale occurs, the reports said. “AT&T is looking to sell just over 50 percent of the asset, which would allow the telecom giant to take a fast-shrinking business off its books while still enjoying the

benefits of a still-large distribution network," the Journal wrote. AT&T previously considered a sale of DirecTV last year but decided to keep the satellite business.

AT&T's 2015 purchase of DirecTV happened under then-CEO Randall Stephenson, who retired this year. The new talks with potential buyers "were spurred by Chief Executive John Stankey," who replaced Stephenson in July, the Journal wrote, adding that "Mr. Stankey has said the company should sharpen its focus on core connectivity services."

AT&T has been reporting big customer losses each quarter for the past two years, with AT&T's rising TV prices helping push users to other TV or online streaming services. After a Q2 2020 loss of 954,000 customers, AT&T was down to 18.41 million customers across DirecTV, U-verse TV, and AT&T-branded online TV services. That's a loss of more than 7 million customers since mid-2018 when AT&T had 25.45 million subscribers in those categories.

AT&T declined to comment, according to Bloomberg. We contacted AT&T today and will update this article if we get a response.

https://arstechnica.com/?p=1702178

Google offers to help others with the tricky ethics of AI

Yuchiro Chino | Getty Images

reader comments

66 with 57 posters participating

Share this story

Companies pay cloud-computing providers like Amazon, Microsoft, and Google big money to avoid operating their own digital infrastructure. Google's cloud division will soon invite customers to outsource something less tangible than CPUs and disk drives—the rights and wrongs of using artificial intelligence.

The company plans to launch new AI ethics services before the end of the year. Initially, Google will offer others advice on tasks such as spotting racial bias in computer vision systems or developing ethical guidelines that govern AI projects. Longer term, the company may offer to audit customers' AI systems for ethical integrity and charge for ethics advice.

Google's new offerings will test whether a lucrative but increasingly distrusted industry can boost its business by offering ethical pointers. The company is a distant third in the cloud-computing market behind Amazon and Microsoft, and it positions its AI expertise as a competitive advantage. If successful, the new initiative could spawn a new buzzword: EaaS, for ethics as a service, modeled after cloud-industry coinages such as SaaS, for software as a service.

Google has learned some AI ethics lessons the hard way—through its own controversies. In 2015, Google apologized and blocked its Photos app from detecting gorillas after a user reported the service had applied that label to photos of him with a Black friend. In 2018, thousands of Google employees protested a Pentagon contract called Maven that used the company's technology to analyze surveillance imagery from drones.

Soon after, the company released a set of ethical principles for use of its AI technology and said it would no longer compete for similar projects, but it did not rule out all defense work. In the same year, Google acknowledged testing a version of its search engine designed to comply with China's authoritarian censorship and said it would not offer facial recognition technology, as rivals Microsoft and Amazon had for years, because of the risks of abuse.

Google's struggles are part of a broader reckoning among technologists that AI can harm as well as help the world. Facial recognition systems, for example, are often less accurate for Black people and text software can reinforce stereotypes. At the same time, regulators, lawmakers, and citizens have grown more suspicious of technology's influence on society.

A deeper examination

In response, some companies have invested in research and review processes designed to prevent the technology going off the rails. Microsoft and Google say they now review both new AI products and potential deals for ethics concerns, and they have turned away business as a result.

Tracy Frey, who works on AI strategy at Google's cloud division, says the same trends have prompted customers who rely on Google for powerful AI to ask for ethical help, too. "The world of technology is shifting to saying not 'I'll build it just because I can' but 'Should I?'" she says.

Google has already been helping some customers, such as global banking giant HSBC, think about that. Now, it aims before the end of the year to launch formal AI ethics services. Frey says the first will likely include training courses on topics such as how to spot ethical issues in AI systems, similar to one offered to Google employees, and how to develop and implement AI ethics guidelines. Later, Google may offer consulting

services to review or audit customer AI projects, for example to check if a lending algorithm is biased against people from certain demographic groups. Google hasn't yet decided whether it will charge for some of those services.

Google, Facebook, and Microsoft have all recently released technical tools, often free, that developers can use to check their own AI systems for reliability and fairness. IBM launched a tool last year with a "Check fairness" button that examines whether a system's output shows potentially troubling correlation with attributes such as ethnicity or ZIP code.

Going a step further to help customers define their ethical limits for AI could raise ethical questions of its own. "It is very important to us that we don't sound like the moral police," Frey says. Her team is working through how to offer customers ethical advice without dictating or taking on responsibility for their choices.

"Legally compelled to make money"

Another challenge is that a company seeking to make money from AI may not be the best moral mentor on curbing the technology, says Brian Green, director of technology ethics at the Markkula Center for Applied Ethics at Santa Clara University. "They're legally compelled to make money and while ethics can be compatible with that, it might also cause some decisions not to go in the most ethical direction," he says.

Frey says that Google and its customers are all incentivized to deploy AI ethically because to be broadly accepted the technology has to function well. "Successful AI is dependent on doing it carefully and thoughtfully," she says. She points to how IBM recently withdrew its facial recognition service amid nationwide protests over police brutality against Black people; it was apparently prompted in part by work like the Gender Shades project, which showed facial analysis algorithms were less accurate on darker skin tones. Microsoft and Amazon

quickly said they would pause their own sales to law enforcement until more regulation was in place.

In the end, signing up customers for AI ethics services may depend on convincing companies who turned to Google to move faster into the future that they should in fact move more slowly.

Late last year, Google launched a facial recognition service limited to celebrities that is aimed primarily at companies that need to search or index large collections of entertainment video. Celebrities can opt out, and Google vets which customers can use the technology.

The ethical review and design process took 18 months, including consultations with civil rights leaders and fixing a problem with training data that caused reduced accuracy for some Black male actors. By the time Google launched the service, Amazon's celebrity recognition service, which also lets celebs opt out, had been open to all for more than two years.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1702049

Apple won't let Facebook tell users about 30-percent Apple tax on events

Enlarge / Facebook wanted the event purchase screen on iOS to look like the screenshot on the left. But Facebook says Apple nixed the idea.

reader comments

294 with 158 posters participating

Share this story

Apple nixed a message in the Facebook app for iOS warning users that Apple would take 30 percent of event payments, Facebook says.

Facebook announced a new feature for paid online events earlier this month. It allows small businesses to host virtual cooking classes, workout sessions, happy hours, and other events and charge people to participate.

In its announcement, Facebook said it was not taking a cut of customers' payments. That means that on Android, "small businesses will keep 100% of the revenue they generate," Facebook says. But the story was different on iOS thanks to Apple's 30-percent cut of in-app purchases.

The screenshot above shows how the social media giant wanted to alert users to the 30-percent charge. The iOS version of the app is at the left. Below the "Purchase" button it says, "Apple takes 30% of this purchase."

But Facebook says Apple forced the company to delete the notice, dubbing it a violation of the App Store's policy against showing "irrelevant" information to users.

Apple's rules state that an app developer shouldn't "include irrelevant information, including but not limited to information about Apple or the development process."

Facebook says it disagrees with this policy. "We of course do think this is relevant information and are still hoping to

make that information available in the app experience," a spokesperson told Ars by email. "Now more than ever, we should have the option to help people understand where money they intend for small businesses actually goes."

It's the latest example of major tech companies chafing under Apple's restrictive app store rules—and especially its demand for 30 percent of app makers' revenues. Earlier this month, Epic sued Apple, arguing that its 30-percent take of in-app payments violated antitrust law.

In June, Apple attracted criticism after rejecting the email app Hey. The email provider had refused to implement in-app payments in its iOS app, requiring users to subscribe on Hey's website instead. Apple partially backed down after an uproar.

https://arstechnica.com/?p=1701932

Russian tourist offered employee $1 million to cripple Tesla with malware

reader comments

70 with 54 posters participating

Share this story

Tesla's Nevada Gigafactory was the target of a concerted plot

to cripple the company's network with malware, CEO Elon Musk confirmed on Thursday afternoon.

The plan's outline was divulged on Tuesday in a criminal complaint that accused a Russian man of offering $1 million to the employee of a Nevada company, identified only as "Company A," in exchange for the employee infecting the company's network. The employee reported the offer to Tesla and later worked with the FBI in a sting that involved him covertly recording face-to-face meetings discussing the proposal.

"The purpose of the conspiracy was to recruit an employee of a company to surreptitiously transmit malware provided by the coconspirators into the company's computer system, exfiltrate data from the company's network, and threaten to disclose the data online unless the company paid the coconspirators' ransom demand," prosecutors wrote in the complaint.

Musk: "This was a serious attack"

Until Thursday afternoon, the identity of Company A was uncertain, although there was plenty of Twitter speculation—and several sourceless blog reports—that Tesla's site in Nevada was the target. In a Tweet responding to one of the unconfirmed reports, Musk wrote: "Much appreciated. This was a serious attack."

> *Much appreciated. This was a serious attack.*
>
> *— Elon Musk (@elonmusk) August 27, 2020*

Tuesday's charging document, which was filed in federal court in Nevada, detailed an extensive and determined attempt to infect Company A's network. Defendant Egor Igorevich Kriuchkov, 27, allegedly traveled from Russia to Nevada and then met with the unnamed employee on multiple occasions. When Kriuchkov's initial $500,000 bid failed to clinch the deal, the defendant doubled the offer, prosecutors said.

Wining, dining, and boozing

According to the complaint, Kriuchkov wined, dined, and boozed the employee, and when discussing especially sensitive details, conducted conversations in cars. When FBI agents couldn't conduct physical surveillance in restaurants or bars, the employee recorded them.

One alleged meeting occurred on August 7 in a car Kriuchkov rented. Referring to the employee as CHS1—short for confidential human source No. 1—prosecutors described it this way:

> *During this meeting, which the FBI had consensually recorded, KRIUCHKOV reiterated some of the details of the criminal activity previously proposed to CHS1. KRIUCHKOV described the malware attack as he did before, adding that the first part of the attack (DDoS attack) would be successful for the "group" but the Victim Company's security officers would think the attack had failed. KRIUCHKOV again listed prior companies the "group" had targeted. KRIUCHKOV stated each of these targeted companies had a person working at those companies who installed malware on behalf of the "group." To ease CHS1's concerns about getting caught, KRIUCHKOV claimed the oldest "project" the "group" had worked on took place three and a half years ago and the "group's" co-optee still worked for the company. KRIUCHKOV also told CHS1 the "group" had technical staff who would ensure the malware could not be traced back to CHS1. In fact, KRIUCHKOV claimed the group could attribute the attack to another person at Victim Company A, should there be "someone in mind CHS1 wants to teach a lesson."*
>
> *During the meeting, CHS1 expressed how concerned and stressed CHS1 had been over the request. CHS1 stated if CHS1 were to agree to install the malware, CHS1 would need more money. KRIUCHKOV asked how much, and CHS1 responded US $1,000,000.*

> *KRIUCHKOV was sympathetic to the request and said he understood, but would have to contact the "group" before agreeing to the request. KRIUCHKOV confided that the "group" was paying KRIUCHKOV US $500,000 for his participation in getting CHS1 to install the malware, and he was willing to give a significant portion of the payment (US $300,000 to US $450,000) to CHS1 to entice his involvement.*

> *CHS1 said CHS1 would need money upfront to ensure KRIUCHKOV would not have him install the software and then not pay him. Again, KRIUCHKOV asked how much, and CHS1 responded US $50,000. KRIUCHKOV said this was an acceptable amount and a reasonable request but he would have to work on this because he only had US $10,000 with him due to U.S. Customs restrictions on the amount of money he could bring into the country. KRIUCHKOV also questioned what would prevent CHS1 from taking the up-front money and then not following through on installing the malware. CHS1 stated CHS1 was sure KRIUCHKOV or the "group" would figure a way to apply leverage against CHS1 to ensure CHS1 held up his end of the arrangement. CHS1 and KRIUCHKOV discussed the timing of the next meeting, and KRIUCHKOV said he would return to Reno on or around August 17, 2020.*

Absolutely insane

Besides targeting an iconic car maker, the plot is notable for other reasons. One is its sheer audacity and recklessness. As security researcher and reformed teenage cybercrime hacker Marcus Hutchins noted on Twitter: "One of the benefit of cybercrime is criminals don't have to expose themselves to unnecessary risk by conducting business in person. Flying into US jurisdiction to have malware manually installed on a company's network is absolutely insane."

> *One of the benefit of cybercrime is criminals don't have to expose themselves to unnecessary risk by conducting business*

> *in person. Flying into US jurisdiction to have malware manually installed on a company's network is absolutely insane.*
>
> *— MalwareTech (@MalwareTechBlog)* ***August 27, 2020***

A chilling observation, from Craig Williams, director of outreach as Cisco's security arm Talos Labs, was what might have happened had the plot succeeded.

"This does bring into question the risk added if the system responsible for your self driving car comes under attacker control—due to malicious insider or otherwise," he wrote. "The entire thing is extremely exciting and concerning."

> *So I suppose this means my guess was correct. This does bring into question the risk added if the system responsible for your self driving car comes under attacker control — due to malicious insider or otherwise. The entire thing is extremely exciting and concerning.* ***https://t.co/oYKnDWKem1***
>
> *— Craig Williams (@security_craig)* ***August 28, 2020***

Musk didn't elaborate on his two-sentence Twitter confirmation, and Tesla representatives didn't respond to an email seeking comment for this post.

The plot and its cast of characters—replete with villains, heroes and whatever Musk is—make for an interesting backstory and possibly a dramatic TV reenactment. For now, readers will have to content themselves with additional reading in Wednesday's coverage of the complaint.

https://arstechnica.com/?p=1701893