Nxxx,2015-07-25,B,003,Bs-BW,E1

F.C.C. Clears Way for AT&T and DirecTV to Merge, With Conditions

By EMILY STEEL

Federal regulators have approved AT&T's $48.5 billion takeover of the satellite company DirecTV, creating a major new force in the communications industry.

The Federal Communications Commission announced its approval of the acquisition on Friday, attaching conditions intended to address the potential harms of the merger. Earlier this week, the Justice Department announced that it would not challenge the acquisition. The regulators were reviewing whether the deal would serve the public interest or stifle competition.

The combination of AT&T, one of the country's largest telephone and Internet providers, with DirecTV, the country's largest satellite provider, is the biggest media merger this year and will create the country's largest television distributor with about 26 million subscribers, surpassing Comcast, the current leader.

The deal comes during a period of intense merger activity in the media sector, when some of the country's largest cable, satellite and telecom companies are seeking to get even larger as they face new forms of digital disruption and adapt to changing viewer habits.

Other mergers waiting in the wings for regulatory approval include Charter Communication's proposed acquisition of Time Warner Cable and Bright House Networks — deals that together total $67.1 billion. The European telecommunications company Altice has proposed a $9.1 billion deal that would give it a controlling stake in Suddenlink Communications, a regional cable provider. And Verizon Communications recently closed a $4.4 billion deal for AOL.

Friday's regulatory green light left some industry observers more optimistic about the potential for future deals. Many had been wary after Comcast's proposed $45 billion takeover of Time Warner Cable collapsed under regulatory pressure.

"The fact that this deal closed with probably pretty reasonable conditions gives a little bit more confidence that Charter and Time Warner Cable would close, and maybe down the road opens the door for other deals," said Amy Yong, a media analyst with Macquarie Group.

Some public interest groups, though, were disappointed. "I thought after the Comcast-Time Warner Cable deal that maybe the commission was going to travel down a little different road in consolidation and begin to say no to some of these deals," said Michael Copps, a former Democratic member of the F.C.C. and a special adviser to the Common Cause public interest group.

Approval came with a number of conditions, including some aimed at introducing more competition into the broadband Internet market, an issue emphasized by Tom Wheeler, the F.C.C. commissioner, in comments earlier this week.

The commission is requiring AT&T to expand its high-speed, fiber-optic broadband Internet service to 12.5 million customer locations and eligible schools and libraries. That's about 10 times its current size. The F.C.C. said this addresses the concern that the merger would eliminate one choice for television service in the areas where AT&T and DirecTV previously competed. By expanding Internet service, the commission said, consumers will have more options to use services that rely on broadband to deliver video, such as Netflix, Amazon and Hulu.

AT&T also will be required to offer broadband services to people with low incomes at discounted rates.

Mr. Copps questioned whether the conditions were sufficient, saying that the commission did not have a good track record in making sure that they are fulfilled. "I have seen so many lofty merger commitments before and seen the companies find loopholes in them and weasel their way out of them," Mr. Copps said.

But one of the commissioners, Mignon L. Clyburn, defended the broadband rationale. Ms. Clyburn noted that while she thought the public interest benefits were significant, she had concerns about the deal's impact on smaller cable companies and independent programmers. To that end, she asked the F.C.C. chairman to start a proceeding to look at the "challenges and barriers to independent and diverse programming."

JONATHAN ALCORN/REUTERS

DirecTV satellite dishes. The company's merger with AT&T will create the country's largest television distributor.

Another concern about the deal is that AT&T is the only major Internet service provider whose customers face "data caps" for broadband service. The merger could increase the incentive of AT&T to deploy such usage-based pricing to limit access to online video in favor of its own traditional television service. As a condition of the deal, regulators forbade AT&T from deploying discriminatory practices that would disadvantage online video services.

"What they are basically saying is you have to treat everybody like you treat yourself, and so I think that is probably the most important protection against anticompetitive practices," said Gene Kimmelman, the chief executive of Public Knowledge, a consumer advocacy group, and a former antitrust official at the Justice Department.

The company also will be required to submit its so-called interconnection agreements for review by the F.C.C. Those agreements allow a company like Netflix to pay a fee to a distributor, like Comcast or AT&T, for better service, when they create a lot of traffic for the network. The commission said that the condition recognized the importance of those agreements to online video service and said that it would monitor them to make sure that AT&T would not deny or impede access to its networks in anticompetitive ways.

The conditions remain in effect for four years after the merger closes. AT&T also is required to retain an internal compliance officer and an independent, external compliance officer to make sure that the company abides by the deal conditions.

"We'll now be able to meet consumers' future entertainment preferences, whether they want traditional TV service with premier programming, their favorite content on a mobile device, or video streamed over the Internet to any screen," Randall Stephenson, chairman and chief executive of AT&T, said in a statement.

Leaked Fed Staff Forecast Reflects Gloomier Expectations for U.S. Economy

By BINYAMIN APPELBAUM

Staff economists at the Federal Reserve are more pessimistic about the nation's economic prospects than the senior Fed officials who set monetary policy, according to an internal document the central bank mistakenly put online.

The release of the staff economic forecast — presented to officials at the Fed's June policy meeting but scheduled to remain confidential until 2021 — is at least the fourth time in recent years that the Fed has sprung an embarrassing leak.

Representative Jeb Hensarling, the Texas Republican who is chairman of the House Financial Services Committee, said it showed that the Fed needed to improve the way that it safeguarded confidential information. Mr. Hensarling's committee is investigating a 2012 leak of Fed information to a private firm.

"It regrettably appears once again that proper internal controls are not in place to safeguard confidential Federal Reserve information," he said in a statement.

The Fed said on Friday that the forecast went online in late June in a form that was readable only with special computer software. It said a staff member noticed the mistake earlier this week, and that it was now publicizing the problem in part to level the playing field by making the information available to the general public.

In a further twist, the Fed said Friday evening that some of the information it published inadvertently in June — and republished intentionally Friday morning — was inaccurate. It released a second version which it said accurately reflected the contents of the staff forecast presented to officials at the June meeting.

The Fed also said that it had asked its inspector general to investigate.

"We have already implemented procedures to prevent an inadvertent posting of these materials," a Fed spokeswoman said in a statement. The Fed in recent years has sought to provide more information about its decision-making. Last year it published the "FRB/US" model — basically a set of equations — that its staff uses to forecast economic activity, allowing anyone with sufficient expertise to produce their own forecasts using the Fed's tools.

ALEX WONG/GETTY IMAGES

The Federal Reserve's chairwoman, Janet L. Yellen, testifying at a Senate committee hearing. The Fed mistakenly published a confidential report in late June.

The Fed said on Friday that the most recent update, published June 29, inadvertently included the June round of staff forecasts.

The Fed published the minutes of its June meeting on July 8, in keeping with its normal procedures, including a summary of the staff forecast.

The minutes said the staff moved its forecast for 2015 growth "a little lower." The detailed data showed the staff predicted the economy would expand by 1.55 percent in 2015.

The minutes also described the staff forecast as predicting that inflation will return to a 2 percent annual pace by 2018. The staff actually forecast that inflation would average 1.92 percent in 2018, and that it would not reach the Fed's 2 percent target in the next five years, rising to 1.97 in 2020.

Fed officials serving on the policy-making Federal Open Market Committee have said that they plan to raise interest rates later this year, and investors are eager for information about the exact timing. Analysts cautioned that the new disclosures reflected the views of staff members, and that the forecasts of Fed officials, published in June, were more optimistic.

Fiat Chrysler Issues Recall Over Hacking

From First Business Page

men planned to make their findings public early this week. The vulnerability existed far beyond just the Jeep, they said. Other vehicles across Chrysler's lineup of cars and trucks used the same system, called Uconnect, that had let them in. Hundreds of thousands of vehicles could be affected.

Fiat Chrysler software specialists scrambled to make a patch available to plug the hole, and released one on the automaker's website on July 16, the day after the call to Washington. The company also planned to issue a technical service bulletin — a notice mainly used by dealers, but not considered a recall.

Officials at the safety agency, however, wanted to know more about the exact functions that could be taken over by hackers. In N.H.T.S.A. parlance, if the result presented an "unreasonable risk to safety," a recall would be required. And if drivers were vulnerable to an attack where they could lose control of their cars, that would certainly seem to qualify, even though a recall for a web security threat had never before taken place.

In the meantime, the researchers made their findings known on Tuesday in an article published by the news technology site Wired, telling how they had taken control of a cooperating driver's car from 10 miles away as it sped down a St. Louis highway. (It was the same day, coincidentally, that Mr. Rosekind was visiting Michigan for a speech in which he addressed the need for improved web security in vehicles.)

N.H.T.S.A. officials decided that the vulnerability was simply too dangerous not to require a formal recall. Additionally, without a recall, the automaker would not be required to file regular compliance reports on how many affected vehicles had been fixed.

After further conversations between Washington and the company's headquarters in Auburn Hills, Mich., Fiat Chrysler settled Thursday on a recall affecting 1.4 million vehicles. (A small percentage of that number, the company said, involves certain 2015 models getting a separate software patch unrelated to the remote Jeep hacking.)

Fiat Chrysler issued a public statement saying that security "is a top priority," as is retaining consumer confidence in its vehicles. Fiat Chrysler will send affected owners a USB drive they can plug into their vehicles to install an update to block the hacking vulnerability. Owners can also download the update directly onto their own portable drive.

The recall affects certain vehicles equipped with 8.4-inch touch screens from the 2013 model year onward. That includes some Jeep Cherokees and Grand Cherokees, Dodge Durangos, Ram pickup trucks, Chrysler 200 and 300 sedans, Dodge Chargers and Vipers. (The company set up a VIN search tool to let consumers check if their vehicle is affected.)

The automaker also said it had "applied network-level security measures" on the Sprint cellular network that communicates with its vehicles as another step to block the vulnerability.

On Friday, Mr. Valasek, one of the two researchers, posted on social media that when he tried connecting again to his test Jeep, the pathway through Sprint's network had been blocked.

Precise aspects of what Fiat Chrysler knew about possible Uconnect problems before this month remain unclear. In documents filed with regulators on Friday, the company said that testing in January 2014 identified "a potential security vulnerability" with a communications port used with the system. A supplier began work on security improvements shortly thereafter, the company said, and those changes made it into later production vehicles. But the software patch for other potentially affected vehicles was not released until this month.

WHITNEY CURTIS FOR THE NEW YORK TIMES

A Fiat Chrysler spokesman, Berj Alexanian, declined to comment on the precise timeline of when the patch was developed, but said that since its release the company has "taken more steps to ensure the confidence and security of our customers," including deciding, "in an abundance of caution, to continue the distribution under the auspices of a recall."

"This will maximize awareness of the software's availability and expedite its proliferation," he said.

One thing remains clear, however: The repercussions of the first hacking-related auto recall are only beginning.

"This was a wake-up call for automakers," said Michelle Krebs, a senior analyst with Autotrader.com. "I will bet emergency meetings are being called at many auto companies."

Web security specialists say that while intrusions into consumers' computers and phones result in financial damage, or possibly issues like identify theft, the danger posed by vehicles is unique in its potential to inflict physical harm.

"The transformation you've seen is that hacking has moved into the safety realm," said Jon Allen, a security specialist with Booz Allen Hamilton. "Autos take it to a new level."

Two technology researchers hacked wirelessly into a Jeep Cherokee through its dashboard connectivity system, controlling the engine, the brakes and the steering.

On Capitol Hill, lawmakers called for ensuring that other automakers do not face similar problems.

"Both automakers and N.H.T.S.A. should be immediately taking steps to verify that other similar vulnerabilities do not exist in other models that are on the road," said Senator Edward Markey, Democrat of Massachusetts.

Mr. Markey, along with Senator Richard Blumenthal, Democrat of Connecticut, recently drafted legislation to set federal standards for web security protection in vehicles.

The chairman of the House Energy and Commerce Committee, Fred Upton, Republican of Michigan, and the panel's top Democrat, Frank Pallone Jr. of New Jersey, also issued a statement, saying that "cars today are essentially computers on wheels, and the last thing drivers should have to worry about is some hacker along for the ride."