2018 Outlook

IP, Privacy, Tech & Telecom

Bloomberg Law®

Contents

Blockbuster High Court Case May Reshape Patent Litigation

- Patent infringement defense strategies may be roiled if challenge process scrapped
- Fate of thousands of invalidated patent claims unclear

By Peter Leung

A patent challenge procedure popular among tech giants and derided by critics as a patent death squad may be facing its own executioner.

The U.S. Supreme Court is weighing whether the procedure, which allows challengers to attack patents at the Patent and Trademark Office rather than in court, is unconstitutional.

Congress designed the process, known as inter partes review, as a faster, cheaper way to invalidate weak patents. If the high court kills IPRs, alleged infringers in many instances will only be able to knock out patents in court. Such a ruling may call into question the fate of all the patents the office has invalidated during the five years the process has been in place. The high court likely will issue its ruling in the case, *Oil States Energy Services LLC v. Greene's Energy Group LLC*, by the end of June.

"Killing IPRs could lead to the resurrection of all of the 'zombie patents' that were killed by the process and that will wreak havoc on the economy," Robert L. Stoll, partner at Drinker Biddle & Reath LLP and former commissioner of patents at the PTO, told Bloomberg Law. "Also, other revocation procedures at the PTO would come into question."

From the time the Patent Trial and Appeal Board (PTAB), which handles IPRs, started in September 2012 through October 2017, 7,685 petitions challenging patents were filed, 92 percent of which were IPRs, according to PTO statistics. The board has issued final written decisions on 1,817 of the IPR petitions, invalidating at least one patent claim in 81 percent of those decisions. The PTAB maintains a fast pace, issuing final written decisions within 12 months of agreeing to institute trial.

Killing IPRs—and possibly other proceedings at the patent office such as covered business method challenges—would force patent litigants, especially defendants, to change their strategies. Tech giants like Apple Inc., Alphabet Inc.'s Google, and Samsung Electronics Co. Ltd. have frequently used IPRs to kill infringement lawsuits based on what they argue are weak patents that should never have been granted. Losing that option would likely force them to attack more patents in district court, which is generally costlier and more time-consuming.

Large companies are lined up on both sides of the fight. Drug companies like Shire Pharmaceuticals and AbbVie Inc. that often have blockbuster products secured by just a handful of patents stand to gain if the Supreme Court rules the process unconstitutional, as do companies like InterDigital Inc. that derive significant income from patent licensing. Killing IPRs would take away some uncertainty surrounding their patent rights.

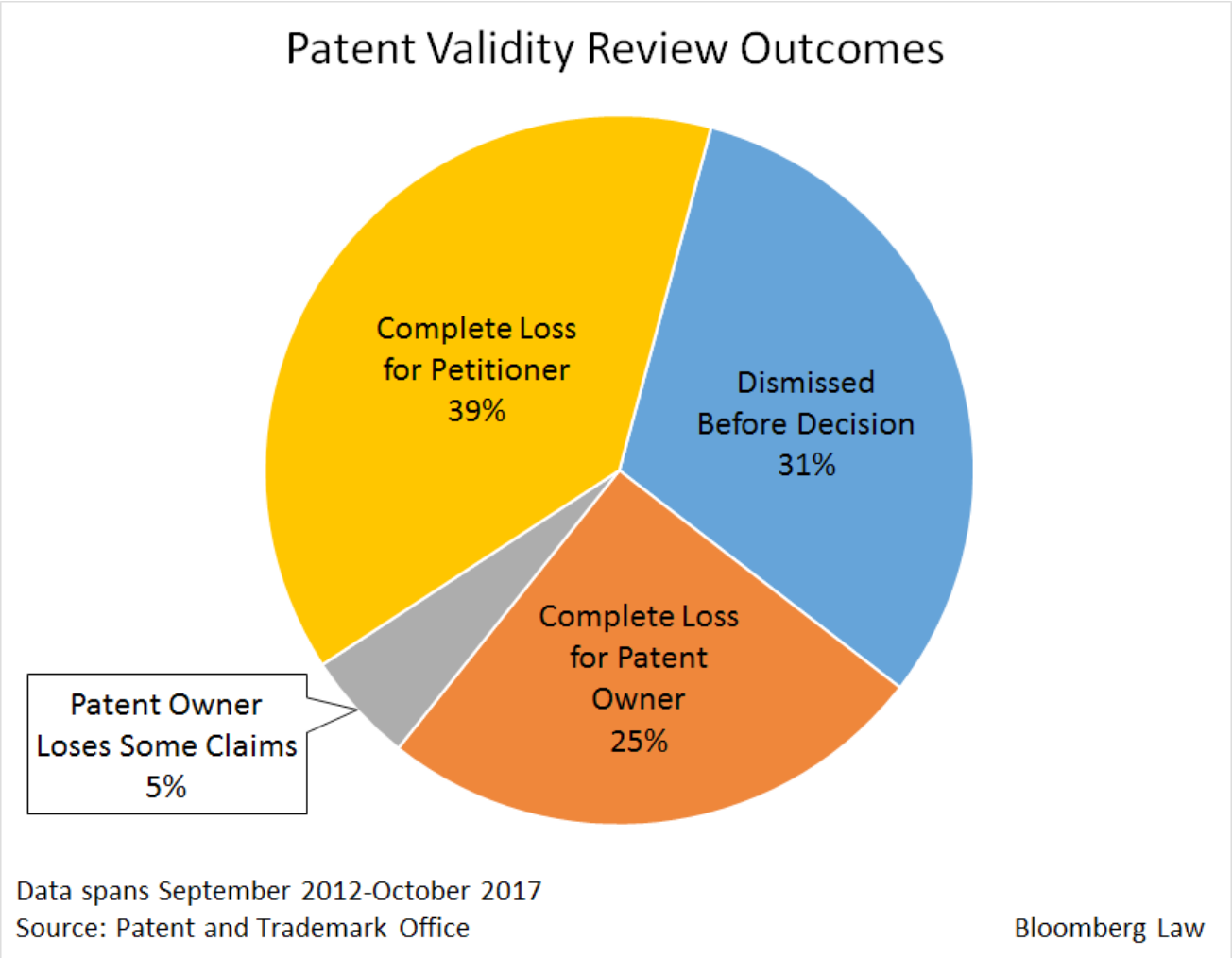
Changed Strategies

In a world without IPRs, an accused infringer lacking that option for getting a patent quickly eliminated could look to district court to knock it out by filing a motion to dismiss, which can be done early in a case.

However, the grounds for such attacks differ from those at the PTO. In court, early motions to dismiss are often based on arguments that a patent covers ineligible subject matter, a tactic that grew more successful and popular with defendants after the Supreme Court, in two rulings, made ineligibility easier to show. IPRs, by contrast, only consider arguments that a patent is either obvious or not novel because it's anticipated by earlier research. Courts can also knock out patents on those grounds, but generally not early on.

The high court in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l* and *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.* made it easier to invalidate patents for covering an ineligible abstract idea or law of nature. Such challenges are especially effective against patents that involve software, business methods, or medical diagnostics. Getting rid of IPRs could push defendants to dedicate even more resources to preparing subject matter eligibility attacks.

The elimination of IPRs could also shift the balance of power in settlement discussions from alleged infringers back to patent owners. Critics, such as companies specializing in patent monetization, say defendants have been less willing to settle or take a license since IPRs became available; many try to get a patent invalidated instead. That trend has driven down the value of patents overall, the critics say.



Private or Public Rights?

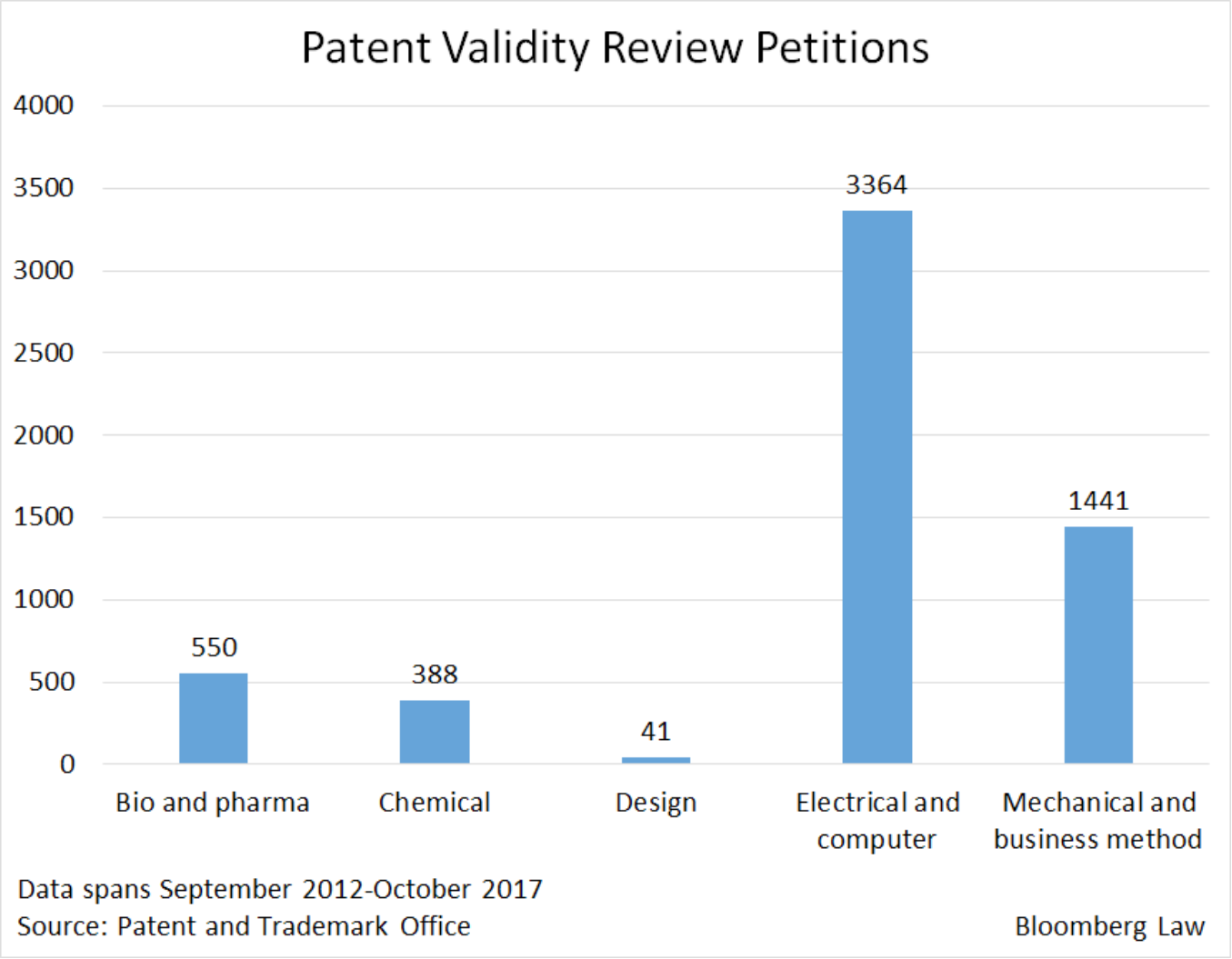
The question for the Supreme Court in *Oil States* is whether Congress properly established the IPR procedure in a 2011 patent law overhaul known as the America Invents Act. Greene's Energy Group LLC persuaded the patent office to invalidate an Oil States Energy Services LLC patent related to extracting oil through hydraulic

fracturing, or fracking. Oil States argues that patents are private property rights that can only be taken away through a jury trial in a court sanctioned under Article III of the Constitution—not in an administrative trial-like proceeding at the PTO, which is part of the executive branch.

The patent office has argued that patent rights can be canceled by a non-judicial body because they are public rights, which are rights integrally related to federal government action. The Constitution authorized the creation of a patent system, and Congress, through legislation, delegated that power to the executive branch, the PTO says. The patent office's power to conduct IPRs stems from its authority to grant patents in the first place, it argues.

The justices' questions during Nov. 27 oral argument in the case suggested several possible approaches to the property rights issue. Justice Neil Gorsuch compared patents to land grants, suggesting that he believed patents are private property rights, while Justice Ruth Bader Ginsburg seemed open to the idea that the PTO is simply correcting its mistakes rather than making decisions about property.

IPRs: Too Big to Fail?



It's unclear what would happen to the thousands of patent claims that have already been invalidated through IPRs if the high court says the process is unconstitutional. The justices may hesitate to dismantle the process and throw the patent system into disorder and uncertainty, intellectual property practitioners told Bloomberg Law.

"My personal opinion is that the Supreme Court is going to affirm the constitutionality of IPRs, for both practical and historical reasons," Stoll said. He noted that the constitutional concerns about IPRs could also apply to post-grant patent review procedures that predate the 2011 overhaul law.

There is precedent for allowing patent office rulings to stand even while declaring the proceedings themselves unconstitutional. In 2007, there were challenges to how judges were appointed to the Board of Patent Appeals and Interferences, the PTAB's predecessor. Congress passed a bill reappointing the judges in a proper manner, but there were still challenges to whether the earlier decisions were valid. The Supreme Court denied review in *Translogic Tech. Inc. v. Dudas,* allowing the decisions to stand.

Others say the practical impact of reviving patents knocked out in IPRs may be limited. The court could restore the invalidated patents, but the PTAB's written decisions are basically blueprints for validity challenges, and defendants can make many of the same arguments in court, Erika H. Arner, patent partner with Finnegan, Henderson, Farabow, Garrett & Dunner LLP, told Bloomberg Law. "From a practical standpoint, it's just not realistic," she said.

On the other hand, the Supreme Court may be more concerned with the constitutional law question than the effect on the patent system.

"Some have argued that IPRs are 'too big to fail,' but don't forget, the Supreme Court was just one vote away from striking down Obamacare," Q. Todd Dickinson, senior partner at Polsinelli PC and former PTO director, told Bloomberg Law via email.

Functioning of Patent System at Stake

Though IPRs have been available for just five years, they have been an important part of patent litigation strategy.

A ruling that the process is unconstitutional would be a win for companies that rely on smaller but valuable patent portfolios, like drug companies that develop new treatments, because it would allow them to concentrate efforts on enforcing their patents in court. Meanwhile, large tech companies, which have been among the most active filers of IPRs as a tactic to head off infringement lawsuits, would be forced to change their approach, such as to seeking more invalidations from courts.

With everything from litigation strategies to the fate of previously invalidated patents in the balance, the Supreme Court's decision promises to have a major impact on the functioning of the entire patent system.

To contact the reporter on this story: Peter Leung in Washington at pleung@bloomberglaw.com

To contact the editor responsible for this story: Mike Wilczek at mwilczek@bloomberglaw.com

Is Copying Ever OK? Software Practices on Line in Copyright Case

- Software developers, industry look to outcome of Google, Oracle dispute to confirm legitimacy of some software copying
- Denial of common industry practice could slow innovation, increase cost of new products, critics say

By Anandashankar Mazumdar

The software industry's ability to easily create new products that are compatible with existing ones hangs on the outcome of a closely watched federal court case.

The U.S. Court of Appeals for the Federal Circuit will weigh whether copying bits of code from Oracle America Corp.'s Java programming language by Alphabet Inc.'s Google was a fair use under copyright law, or whether it infringed Oracle's copyright to the tune of $9 billion. Fair use allows limited copying from protected works that would otherwise be infringing. Following a Dec. 7 oral argument, a ruling is likely in the first half of 2018.

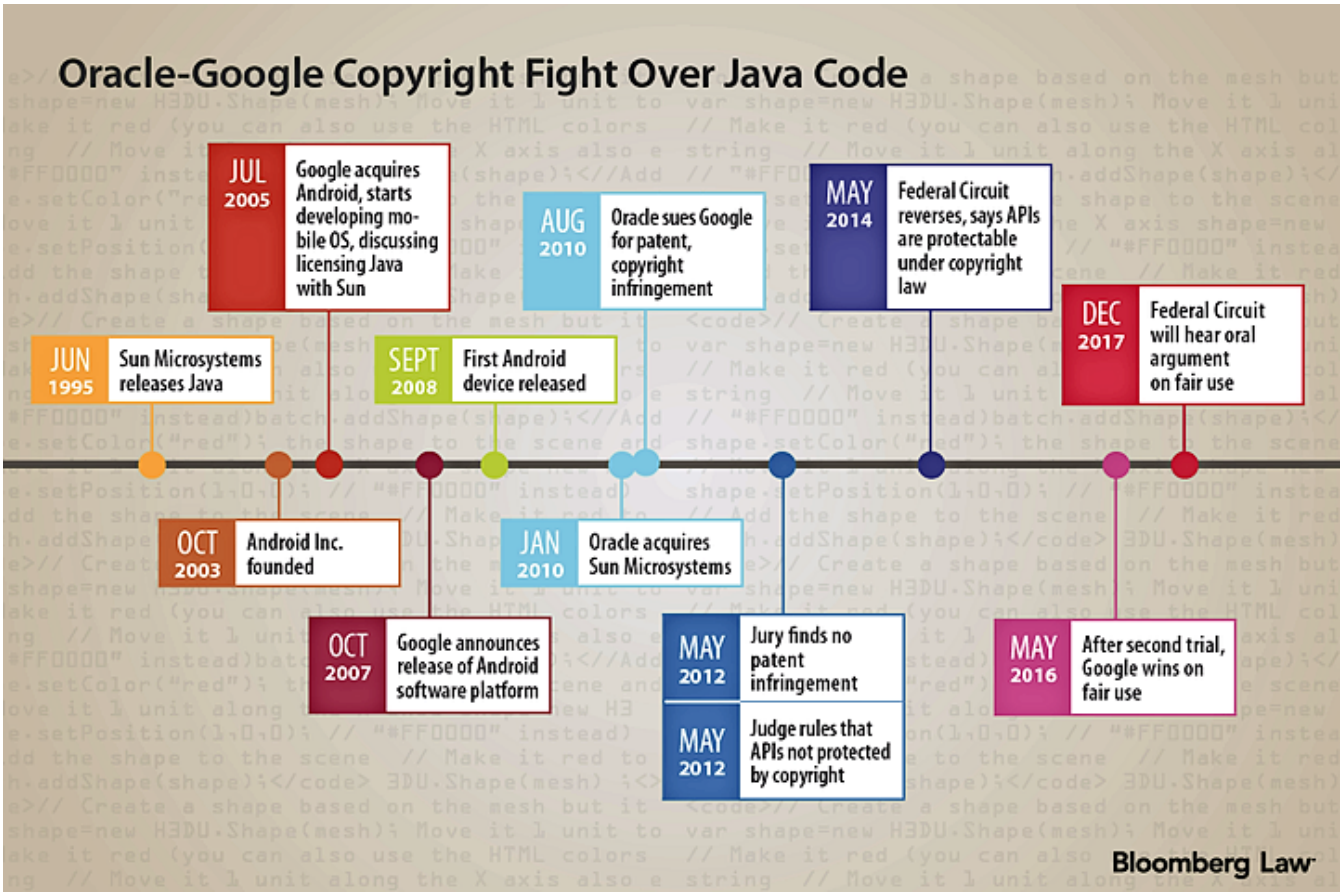
The case pits software developers' ability to make products that work together against creators' rights to control how their software is used. The decision will impact companies beyond the two tech giants. It may affect the speed and variety of technological products available to consumers, businesses, and developers (*Google, Inc.*, Fed. Cir., No. 17-1118, argument scheduled 12/7/17).

"Anything you buy has software. And if it gets more expensive to make software, prices go up, features will go down," Joshua Bloch, a computer science professor at Carnegie Mellon University, Pittsburgh, told Bloomberg Law.

Google argues that if Oracle wins, competing developers who want their products to work in any computer environment may either have to spend more to get permission to use bits of protected software or be limited in which markets they can enter. Consumers would face higher prices and less competition—and may ultimately have to choose among silos of compatible product lines, it said.

Oracle, for its part, has argued that software creators should be able to control new uses of their copyrighted works, including in new markets or environments. Some software creators—particularly small ones—are worried that a Google win on the fair use question would empower large companies to poach new markets before copyright holders can enter them.

Whichever way the Federal Circuit rules, the case is likely to end up at the doorstep of the U.S. Supreme Court, where it would face uncertain prospects.



Copying Code: Standard Practice?

Google says its copying of some of the Java code was a standard software industry practice, in which application program interfaces, or APIs, can be freely copied. APIs are bits of code that are shorthand for larger chunks of frequently re-used code.

Reimplementation of APIs allows companies to make software and devices that work together, such as the way almost any manufacturer's keyboard or mouse can be plugged into most computers.

Knowing that the commercial success of a computer depends on having a wide variety of software that can be used on it, Google copied the Java APIs to make it easier for programmers who already knew Java to develop apps for Android devices, Google argues.

The strategy paid off. Android is now the most successful mobile operating system in the world, running on 70 percent of smartphones. Oracle says it deserves a multibillion-dollar damages award because Google infringed its Java copyright when it copied the code.

Developers in 'Scary Place'

Software developers supporting Google's position fear that an Oracle win will throw their industry into turmoil.

"We are in a scary place, because for the last I-don't-know-how-many years of computing, the concept has been that the reimplementation of APIs is a good thing for everybody," software developer Geir Magnusson Jr., chief technology officer and co-founder of Sourcepoint Technologies Inc., told Bloomberg Law.

An Oracle win could encourage more use of open source tools, Bloch said. But adoption of open source will take time while standards are rewritten, because many existing open sources standards were created with the assumption that APIs can be reimplemented.

Possible Next Steps

However the appeals court rules, one or both sides are likely to seek Supreme Court review. There's no guarantee the high court would take the case, especially because there is no split among federal appeals courts on the issues.

That leaves the matter open to a certain level of gaming in litigation. It's not clear that a different federal appeals court would have ruled that APIs are protected by copyright law, as the Federal Circuit did the first time it ruled in 2014. That makes appealing to the Federal Circuit important for those who don't want to risk having a different appeals court decide that APIs aren't copyright-protected.

The Federal Circuit, however, ordinarily can't exercise jurisdiction over copyright cases. But because Oracle's original complaint against Google included patent issues, Oracle was able to appeal to the Federal Circuit, instead of to the U.S. Court of Appeals for the Ninth Circuit, even after the patent issues were no longer part of the case.

That gives plaintiffs who want to make sure a case goes to the Federal Circuit an incentive to incorporate some kind of patent issue. Doing so could prevent the emergence of a circuit split.

"People might say it's almost malpractice not to tack on a patent claim so your appeal can go to the Federal Circuit," Pamela Samuelson, a copyright law professor at the University of California and co-director of the Berkeley Center for Law and Technology, said.

If the Federal Circuit doesn't affirm, at a minimum, that what Google did is fair use, software developers will have ongoing uncertainty over what is allowed, Jeffrey T. Pearlman, a lecturer at Stanford Law School and co-author of a brief supporting Google that was filed with the Federal Circuit by Bloch and 75 more computer scientists, told Bloomberg Law.

"There's a cloud that hangs over" whether reimplementing APIs is allowed without permission, Pearlman said. This cloud "makes them refrain from behaviors that may be legal and certainly beneficial to the industry."

To contact the reporter on this story: Anandashankar Mazumdar in Washington at amazumdar@bloomberglaw.com

To contact the editor responsible for this story: Mike Wilczek at mwilczek@bloomberglaw.com

Runaway Ransomware in 2018? Look for Enforcers to Take Notice

- Growing ransomware threat, regulator interest will converge in 2018 to up enforcement risk for companies
- Regulators will apply general data security standards in scrutinizing attacked companies

By Daniel R. Stoller

Ransomware attacks on companies are on the rise, opening the door to federal and state enforcement actions based on regulators' claims of inadequate corporate cybersecurity.

The attacks are launched by hackers who encrypt computer data and threaten not to release a decryption key unless ransom is paid, generally in the form of cryptocurrency, such as bitcoin.

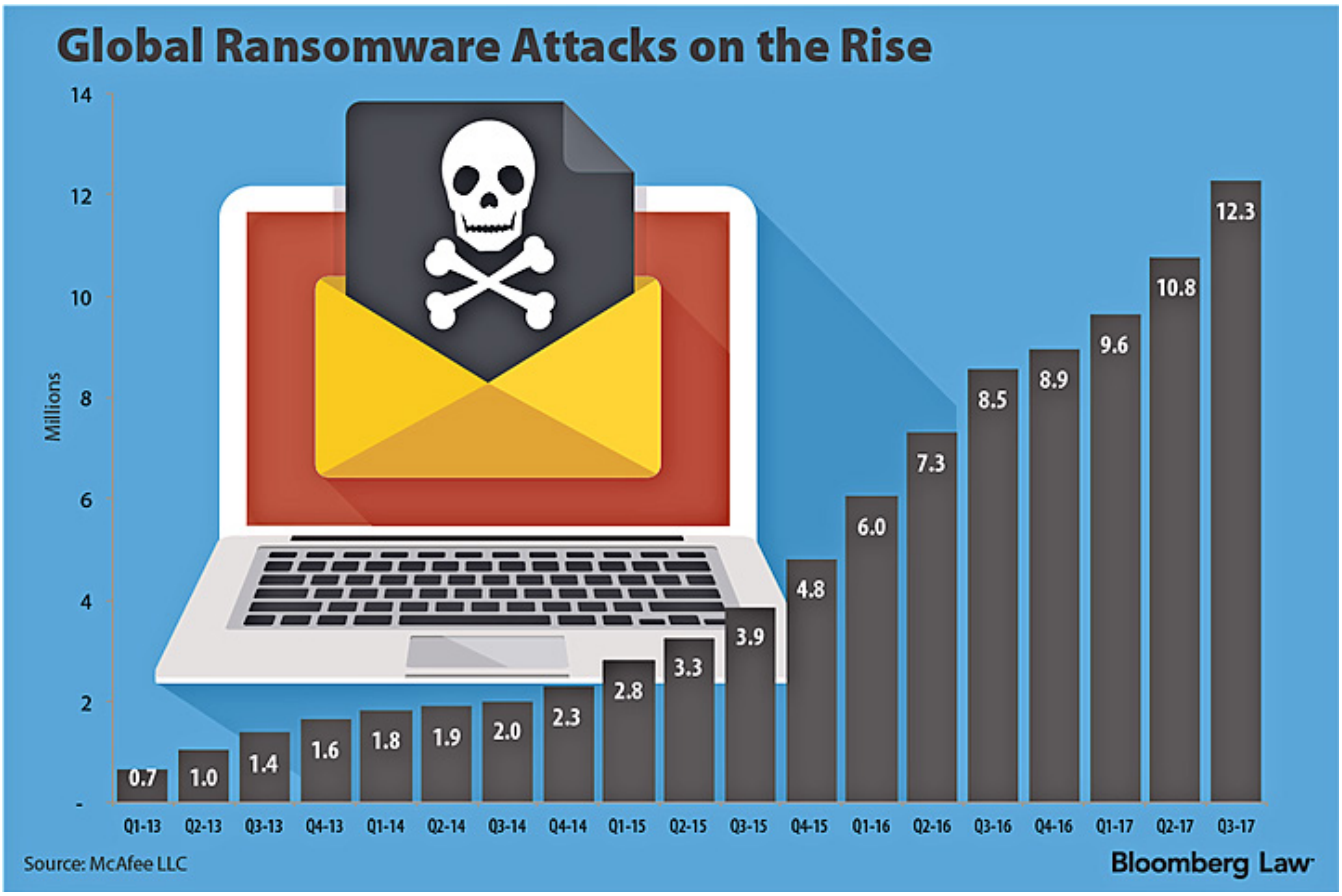
"Regulators are going to heighten their ransomware focus in 2018 and hammer companies on data security and cybersecurity shortcomings," Paul Ferrillo, cybersecurity and litigation counsel at Weil, Gotschal & Manges LLP in New York, told Bloomberg Law.

The Federal Trade Commission, the Securities and Exchange Commission, and the Department of Health and Human Services are likely to be the most active federal enforcers in 2018, as ransomware strikes cause more actual and reputational damage, cybersecurity attorneys said.

Attorneys general in California and New York, who have been active in data security enforcement and have strong data security guidelines in place, are likely to lead ransomware enforcement efforts by the states, cybersecurity attorneys predicted. To date, there have been no federal or state ransomware enforcement actions, Bloomberg Law data show.

"Ransomware has hit a critical mass from an aggregate global cyberthreat perspective across key critical infrastructures," Peter Tran, general manager and senior director in the worldwide advanced cyber defense practice at RSA Security in Boston, told Bloomberg Law. The threat has reached the "top of mind" for regulators, and industry will "likely see increased policy, regulatory compliance and enforcement focus and pushes in 2018," he said.

The attacks will increasingly focus on U.S. companies, according to the Sophos Lab 2018 threat report. Across the world, 17 percent of all ransomware attacks in 2017 hit the U.S., the report showed. U.S. companies, especially those in the healthcare, financial services, and government contracting industries, "will continue to be heavily targeted with ransomware," according to the report.



System Lockdown

Ransomware attacks have been hitting more large companies than individuals, a trend that will likely expand in 2018, Dmitri Alperovitch, co-founder and chief technology officer at threat intelligence company CrowdStrike Inc. in Arlington, Va., said.

Hackers will continue to focus ransomware attacks on companies in 2018 because it is a great business model, U.S. Deputy Attorney General Rod J. Rosenstein said at a recent event. Ransomware payments are quickly approaching $1 billion annually, he said. These attacks are "more sophisticated and targeted attacks that focus on particular businesses or sectors," he said.

One reason is that cybercriminals now sell their software as a service to hackers. Ransomware as a service allows less-sophisticated hackers to launch crippling strikes with a lower entry cost while the software developers reap the profits, according to the Sophos report.

Ransomware attacks show that hackers can "hold entire networks hostage while demanding millions of dollars in ransom from businesses who need to get their operations back up and running," Alperovitch said.

The 2017 Not-Petya global ransomware attack cost FedEx Corp. $300 million, the U.S.-based shipping giant said in its first quarter fiscal year 2018 earnings report.

Companies, especially critical infrastructure operators such as telecommunications stalwart AT&T Inc., gas conglomerate Exxon Mobil Corp., and health-care service provider Kaiser Permanente, stand to lose millions of dollars in revenue, including lost profits, business continuity costs, and ransomware payments. Companies

can also face a drop in stock valuation from direct harm stemming from ransomware strikes. The reputations of businesses hit with ransomware attacks can also be damaged if federal or state authorities spotlight alleged lax data security practices, cybersecurity attorneys said.

Reputational damage can be disastrous for a company that is seen as indifferent to or failing to respond and protect consumers after a ransomware attack, attorneys said.

5 Ransomware Tips

1. Use the latest iterations of cybersecurity safeguards
2. Back up software and systems to preserve core data
3. Train employees in basic cybersecurity hygiene
4. Conduct regular critical systems cybersecurity audits
5. Stash cryptocurrency to pay ransom when appropriate

Federal Enforcers

An increasing number of federally regulated companies in the U.S. are being caught up in ransomware attacks, and regulators have put companies on notice that they will be pursuing enforcement actions in 2018, Joseph Moreno, cybersecurity partner at Cadwalader, Wickerhsam & Taft LLP in Washington told Bloomberg Law.

"Regulators will take a tough approach as they try to break the economic relationship between cybercriminals and businesses," Mark Sangster, vice president at cybersecurity company eSentire Inc. in Kitchener, Ontario, told Bloomberg Law.

Although there has been little direct ransomware guidance from federal regulators, that doesn't mean they aren't watching how companies prepare for and respond to ransomware attacks, cybersecurity attorneys said. Federal regulators will rely on general data security standards and past enforcement actions as the basis for ransomware data security actions in 2018, the attorneys said.

Federal regulators have "given fair warning" to companies that lax data security leading to ransomware strikes can result in an enforcement action, Moreno, a former special assistant U.S. attorney and counsel in the Justice Department's national security division, said.

For example, the SEC's 2011 cybersecurity breach notification guidance, the lessons learned from dozens of FTC data security enforcement actions, as well as HHS's 2017 ransomware fact sheet, could be the basis for regulatory investigations into whether companies adequately protected consumer data or properly reported ransomware attacks, Moreno said.

States on Alert

Like the feds, state regulators and attorneys general will likely use existing general data security standards, including data breach notification requirements, to investigate corporate security following a ransomware attack.

California's standard for reasonable data security and the New York Department of Financial Services' cybersecurity rules would come into play in 2018 ransomware enforcement, Norma Krayem, co-chair of the privacy team at Holland & Knight LLP in Washington, told Bloomberg Law.

Other states will be looking to the California and New York standards as a basis to create their own cybersecurity standards in 2018, she said. New York's financial sector cybersecurity rules are "just the tip of the spear of what we may see in 2018," she said.

The confluence of increasing ransomware threats and regulator interest in 2018 and beyond will make next year, at a minimum, a dangerous one for companies that don't strive to maintain reasonable security.

"Ransomware attacks aren't going away anytime soon," Alperovitch said.

By Daniel R. Stoller

To contact the reporter on this story: Daniel R. Stoller in Washington at dstoller@bloomberglaw.com

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com

2018 Brings New EU Privacy, Cyber Regime, But Some Laws Up in Air

- Full legal picture not clear as EU privacy and cybersecurity schemes near effective dates
- Good faith corporate compliance efforts advised to help mitigate risk

By George Lynch

Game-changing new European Union privacy and cybersecurity laws take hold early in 2018, triggering the need for a wholesale shift for companies that transfer personal data outside the 28-nation bloc.

But an incomplete adoption of implementing legislation so far by member countries, and a surprising lack of harmonization among laws will leave companies scrambling to adjust. Billions of dollars in transatlantic trade flow between the EU and U.S. every day, making compliance, however demanding, essential for companies doing business in the EU.

The new regime brings a raft of changes. The potential for steep fines, along with a risk of private lawsuits, makes 2018 a much-anticipated year of reckoning for U.S. companies.

Of the two new laws, the General Data Protection Regulation (GDPR) is the more seismic. It covers privacy and data protection in the processing of EU citizens' personal data, and upends and replaces the EU's previous, 22 year-old privacy scheme. EU regulators will be empowered to impose fines of up to 20 million euros ($23.5 million) or 4 percent of a company's global revenue, whichever is higher.

At issue is the fact that the GDPR gives countries leeway in crafting their own national laws. Up to one-third of a country's provisions can stray from the text of the GDPR, including whether employers have access to employee criminal records and other types of employee data processed by employers.

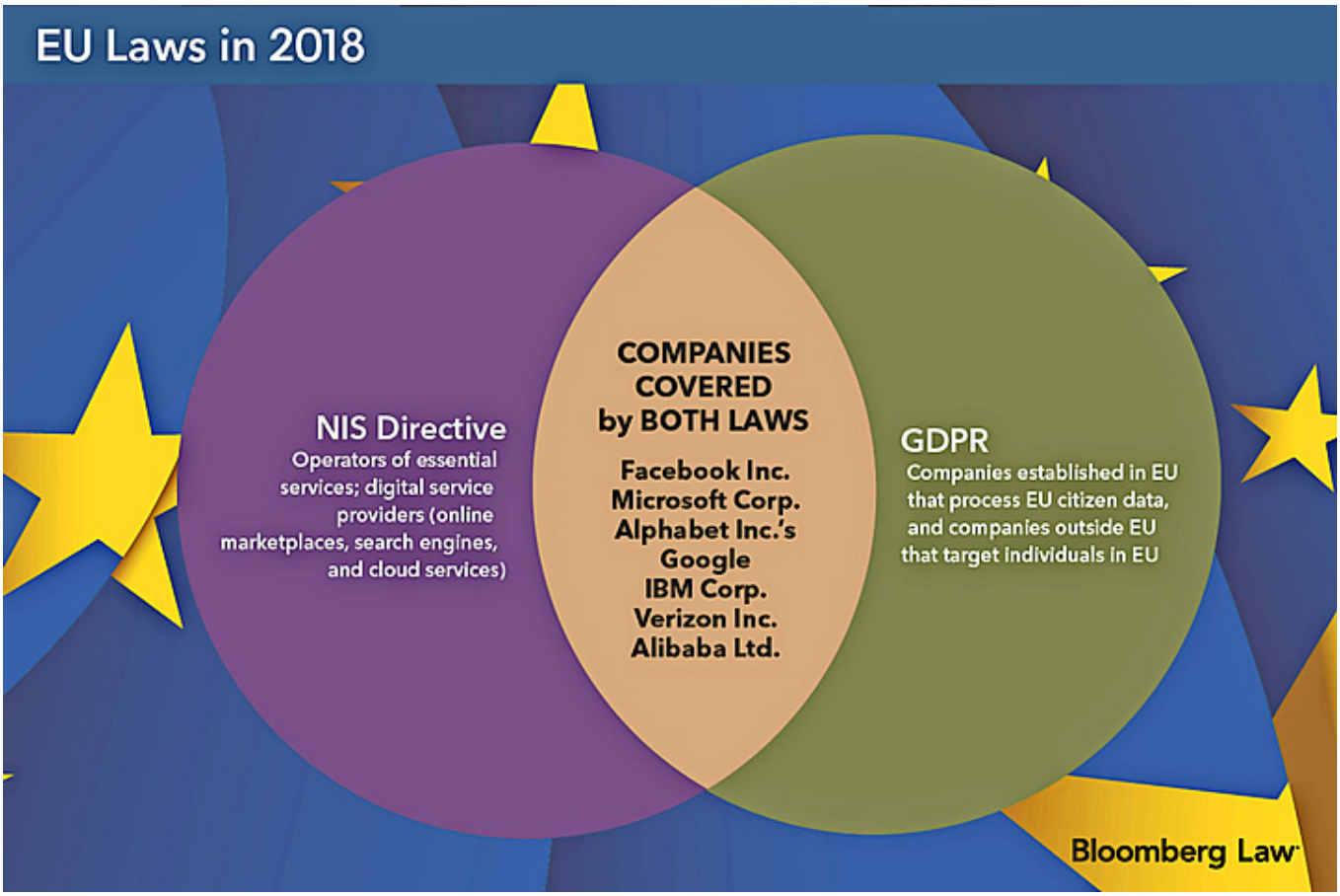
Prospect of Compliance: `Mind-Boggling'

"The prospect of having to comply with 20+ Member State laws in addition to the GDPR is mind-boggling," Wim Nauwelaerts, a data protection partner at Sidley Austin LLP in Brussels, told Bloomberg Law. "Divergences at the member state level will impact key decisions that practically every cross-border business is facing, such as 'do we have to appoint a [data protection officer] DPO,' and 'can we run background checks on new hires.'"

The variance in member states' GDPR implementation laws, enacted or under review, is wider than first anticipated, privacy attorneys told Bloomberg Law.

The resulting uncertainty clouds the ability of companies and attorneys advising them to properly prepare even for basic decisions, such as choosing the location for a company's data processing operations, Nauwelaerts said.

The second EU-wide standard, the Network and Information Security (NIS) Directive, is a new requirement that sets cybersecurity standards for operators of essential services and digital service providers, which include companies that provide EU citizens with search engines, cloud services, or online marketplaces, such as Amazon.com Inc.



EU Laws 2018

Fuller Picture to Emerge

The GDPR will take effect across the EU May 25, 2018, even though most of the 28 EU member countries aren't expected to enact implementing legislation until a few months before it is effective. As of Dec. 5, only Germany and Austria had passed final GDPR laws.

The NIS Directive enters into force May 9, 2018, but directives require countries to adopt national laws to take effect. It's unclear whether countries will enact NIS laws in time for companies to get new compliance programs in place. So far, only two have: Germany and the Czech Republic.

"Most regulators want to see you made a good faith effort to move the ship in the right direction even if you haven't completely complied to every obligation to the last degree."
-Ann LaFrance, partner, Squire Patton Boggs LLP in London

In addition, a company covered by the GDPR and NIS could be responsible for fulfilling different compliance requirements and answering to different regulators.

Risk of Noncompliance

"Businesses that are active across the EU risk being noncompliant if they focus on the GDPR only," Nauwelaerts said.

Many companies covered by both the GDPR and NIS Directive will face layers of compliance from more than one regulator. For example, a company covered by both laws might have to answer to two sets of regulators and face different notification standards stemming from the same data breach, such as in the timing and content of notifications and differences in the regulators who must be notified of a cyberattack.

Also, the GDPR requires companies to report data breaches to the data protection authority in the country in which they process data. The NIS Directive requires companies to report cybersecurity incidents to a regulator to be designated by each member state, which varies by industry.

When it comes to setting up compliance programs, "not many companies are able to do NIS and GDPR at the same time," Jorg Hladjk, data protection of counsel at Jones Day LLP in Brussels, told Bloomberg Law.

Companies: Show Your Work

"Most regulators want to see you made a good faith effort to move the ship in the right direction even if you haven't completely complied to every obligation to the last degree," Ann LaFrance, a data protection partner at Squire Patton Boggs LLP in London, told Bloomberg Law.

Few companies will achieve full compliance before the GDPR and NIS Directive take effect, so they need to be prepared to defend their compliance programs—however imperfect—to regulators and consumers. Individual consumers are free under the GDPR system to file private lawsuits to recover damages for violations, such as a company using an individual's data without a valid legal basis.

"The bottom line is that the onus is on the companies to be compliant. They have to do their risk assessment and take responsibility," Rohan Massey, a partner at Ropes & Gray LLP in London and leader of the firm's privacy and cybersecurity practice in Europe, told Bloomberg Law.

Meticulous documentation by a company of the steps it has taken to comply and the reasoning behind those decisions will go a long way toward demonstrating its good faith effort at compliance, and could help mitigate the risk of formal enforcement actions by privacy regulators.

Demonstrating good faith compliance to regulators may also help companies prepare to defend against possible litigation, Tim Wybitul, data protection partner at Hogan Lovells LLP in Frankfurt, told Bloomberg Law. Because the GDPR is so complex, companies should be aware that it will be easy for attorneys representing consumers to point out compliance errors, he said.

Because the variations in national laws are still unknown, the best companies can do is to look for common denominators among the implementation laws as they are released and document good faith efforts to comply, Hladjk said.

"Companies need to have the ability to go back to regulators and say 'This is why we made decisions, this is why we didn't go forward, this is why we are waiting, this is why our program isn't fully developed by May 25, but will be by a later date for these reasons,'" Massey said.

By George Lynch

To contact the reporter on this story: George Lynch in Washington at glynch@bloomberglaw.com

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com

Social Media in Crosshairs as Lawmakers Eye Online Immunity

- Legislation to amend publisher immunity law may impact social media practices
- Tech groups concerned companies will face increased liability risks

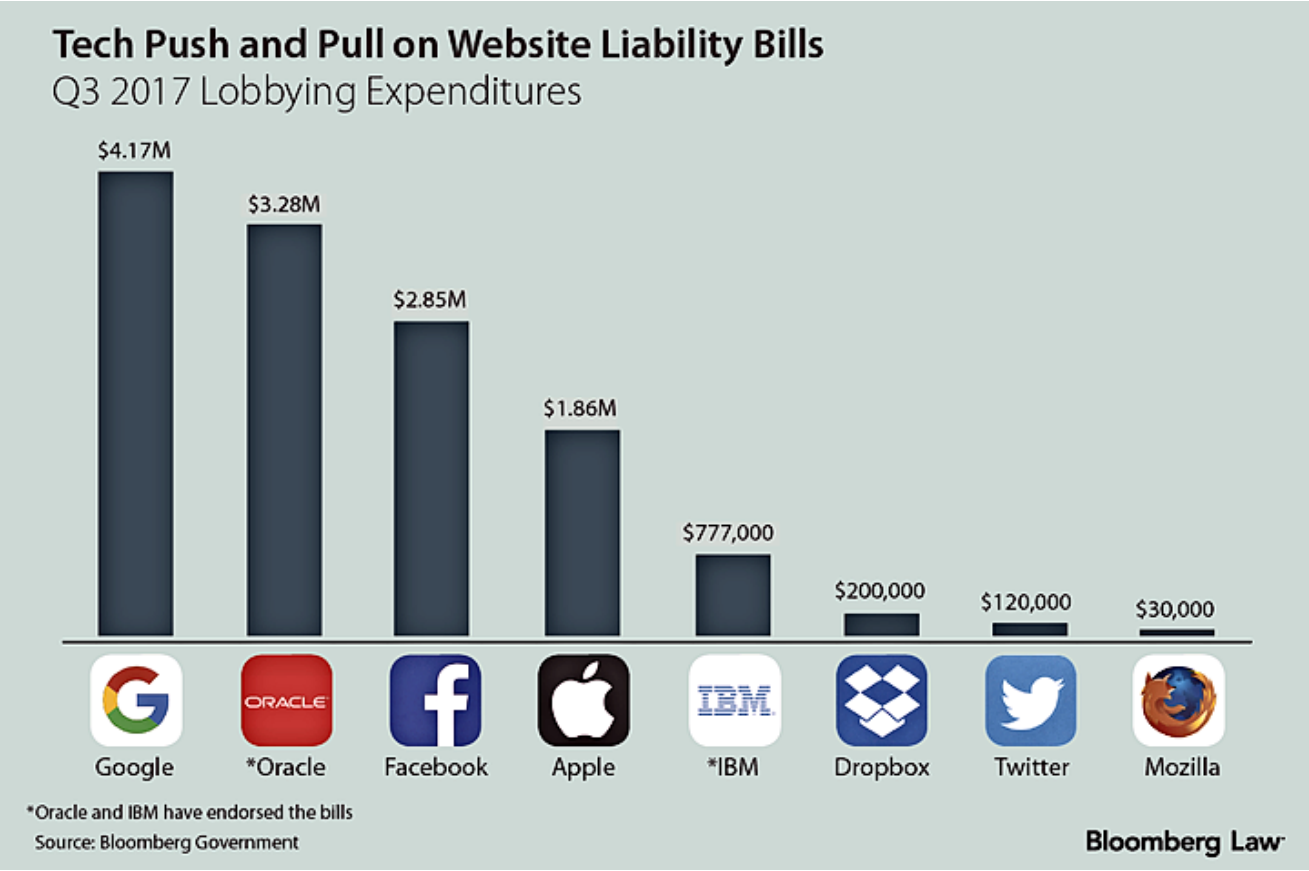
By Alexis Kramer

Social media is thriving under the cover of a 21-year-old federal law that says websites aren't liable for the content their users post online. Congress appears poised to scale back that exception in 2018—but it's unclear by how much.

Lawmakers are weighing changes that may disrupt social media's business model, under which the platforms are lucrative conduits for digital communications and aren't responsible for the keystrokes of their global legions of users.

Pending House and Senate bills (H.R. 1865, S. 1693) would amend current law—Section 230 of the Communications Decency Act—to hold websites liable for knowingly publishing content that facilitates sex trafficking. The legislation likely will change the way websites police content, attorneys and technology trade groups told Bloomberg Law.

"The chilling effect could be substantial," Santa Clara University law professor Eric Goldman said.



The measures would affect not just major social networks like Facebook Inc. and Twitter Inc., but any platform that allows users to post their own content—from vacation rental websites to message boards to crowdfunding sites.

Big and small tech companies alike are wrestling with lawmakers over revisions to the legislation and are already considering changes to their content-monitoring practices. The bills as drafted would only target sex-trafficking content. But tech companies are worried that lawmakers may decide to expand the legislation or write new measures to hold online publishers responsible for terrorism-related content or foreign political ads.

"Once that door is open, it's a lot easier to push forward than get it unlocked in the first place," Kevin M. Goldberg, a First Amendment and internet law attorney and member at Fletcher Heald & Hildreth PLC in Virginia, said.

Big Tech's Big Lobbying Effort

Alphabet Inc.'s Google, Facebook, Twitter, Apple Inc., and Dropbox Inc. are among the tech companies lobbying to influence lawmakers on the issue, Bloomberg Government data show. Google spent $4.17 million and Facebook spent $2.85 million in the third quarter of 2017 alone on those efforts, according to the data.

Rep. Ann Wagner (R-Mo.) and Sen. Rob Portman (R-Ohio) introduced the bills following a two-year Senate probe, led by Portman, into classified ad site Backpage.com LLC's alleged facilitation of sex trafficking. Courts have repeatedly held that Section 230 protects Backpage from claims it enables sex traffickers to advertise their victims online.

Tech companies opposed the effort. They argued that the bills, despite their aim, would create liability risks for companies making good faith efforts to rid their sites of sex-trafficking content.

Portman made some changes to his bill in November to assuage critics' concerns that it would result in companies doing less to monitor content so they could believably claim they don't know what's on their sites. Language that would bar "knowing conduct that assists, supports, or facilitates" sex trafficking was changed to a prohibition on "knowingly assisting, supporting, or facilitating" such crime. The Internet Association, a trade group whose members include Facebook and Google, reversed course and backed the bill with those changes.

The fate of the legislation remains unclear. The House bill has yet to advance, and other tech trade groups, including TechFreedom and Engine, say the Senate bill is still problematic. Sen. Ron Wyden (D-Ore.), an original author of the Section 230 language, has opposed the Senate version, which was unanimously approved Nov. 8 by the Senate Commerce, Science and Transportation Committee. He vowed to block the bill from reaching a floor vote because, according to Wyden, it would place a heavy compliance burden on smaller companies and startups and harm innovation.

Business Model Overhaul?

Portman's changes appeased some critics. But the House bill remains broad, holding websites liable for "knowing or reckless conduct" that furthers sex trafficking. Either way, critics say the "knowing" or "knowingly" standards are vague, overly broad, and could subject companies to liability for merely monitoring their sites for illegal content and failing to take it all down.

Some internet services may not be able to keep up with the mandated level of accuracy in detecting and removing certain content, Sonali Maitra, a technology attorney at Durie Tangri in San Francisco, said. Those companies, she said, would face a difficult choice: vastly limit user content, or drastically reduce monitor-and-remove efforts to avoid being accused of knowing about sex-trafficking content.

"It would put smaller companies in a very precarious situation," Rachel Wolbers, policy director at Engine, an advocacy group for tech startups, said. Startups and smaller internet publishers that lack resources to boost policing efforts by investing in automated filtering tools or hiring employees to read through every post may simply stop moderating content, she said.

Many companies will be forced to assess the minimum amount of policing needed to avoid potential liability risks, Goldman said. "There would be a substantial transition period after the law is passed where sites figure out what they can and can't do," he said.

Supporters say the bills are narrowly tailored and wouldn't put a heavy burden on social media.

The legislation only targets bad actors, according to Christine Raino, senior director of public policy at Shared Hope International, an anti-sex trafficking advocacy group. "It shouldn't impact companies' good faith efforts to look for criminal activity on their platforms," she said.

Portman spokesman Kevin Smith told Bloomberg Law that the bill "protects good actors and only targets rogue online businesses like Backpage that actively facilitate sex trafficking." Wagner told Bloomberg Law that she is working with the Department of Justice and House Judiciary Committee to make sure her bill "has the ability to really put criminals behind bars and to take these websites down."

Down the Slippery Slope

The bills would enable sex-trafficking victims to obtain relief in court from publishers for harms they suffered as a result of content found on their sites. But despite its benefits, concerns persist that any change to Section 230 may create a slippery slope toward more alterations.

Lawmakers, for example, could propose changes to Section 230 to target terrorist content or foreign political ads, Goldberg said. That could raise particular concerns for social media companies that have not only benefited from such immunity in the past but are now at the heart of a political firestorm over how Russia may have used their platforms to influence the 2016 U.S. presidential election.

Google, Facebook, and Twitter have all escaped liability under the law for claims that they allowed the Islamic State group to use their sites to spread propaganda and recruit fighters. In 2017, Google won dismissal of one, and Facebook won dismissal of two such complaints under Section 230. Bloomberg Law data show nine pending cases that allege at least one of the three platforms provided material support to terrorism.

State attorneys general are pushing for wider changes to Section 230 that would allow them to prosecute website operators for alleged crimes under state law. Section 230, while generally immunizing publishers for content on their sites, says they can be held liable for federal criminal charges. The two bills would broaden that exemption and include state criminal claims, but only if they relate to sex trafficking. Fifty state attorneys general asked Senate and House lawmakers in August for a broader exemption for all state criminal laws.

Exceptions in the Wings

Debate over the bills' language will continue. Attorneys and tech trade groups want to see further changes to the Senate bill that would ease monitoring efforts for publishers. TechFreedom and Engine have proposed a notice-and-takedown system whereby websites could avoid liability by, upon receiving notice of an alleged sex-trafficking post, reporting it to law enforcement and cooperating with removal orders. The groups want lawmakers to specify when websites have a duty to take down content and further clarify the knowledge standard.

Regardless of the final form, legislation narrowing Section 230 would drive social media, sharing economy companies, and other online content publishers to change their policies and practices—and could open the door to further changes in a law that's served as a foundation for the internet's freewheeling content culture for more than two decades.

"If this law goes through, there's a long line of other victims who believe there should be an exception under Section 230," Goldman said.

By Alexis Kramer

To contact the reporter on this story: Alexis Kramer in Washington at akramer@bloomberglaw.com

To contact the editor responsible for this story: Keith Perine at kperine@bloomberglaw.com

Cryptocurrency Exchanges Face Ramped-Up Regulation, Court Battles

- Online platforms that trade Bitcoin, other digital assets, likely to draw more attention in 2018
- Many exchanges aren't regulated in U.S. outside of enforcement for fraud, market manipulation

By Michaela Ross

Online sites that exchange bitcoins and other digital assets will face heightened legal and regulatory challenges in 2018, regardless of whether the value of the assets continues to skyrocket.

Hundreds of companies and people raised funds in 2017 through the sale of the assets, known as cryptocurrencies, coins, or tokens. Those initial coin offerings (ICOs) became popular among investors and buyers in part because of how easy they are to conduct.

It's not always clear what existing regulations apply to the cryptocurrency industry as its technology continues to evolve, making it difficult for exchanges to comply. Token exchanges have also operated with fewer safeguards for purchasers than other types of exchanges, meaning users may be exposed to unexpected risk.

Regulators are starting to pay attention. Cryptocurrency and digital asset exchanges are likely to be hit hard with legal and regulatory challenges in 2018 because they're usually more established and easier to identify than the companies or people developing the coins, financial attorneys and digital asset trade and advocacy groups told Bloomberg Law.

"I think that this is all a lot closer than people think, because quite frankly the amounts of money involved now are too significant for regulation and litigation not to be coming," James Taylor-Copeland, the founder of Taylor-Copeland Law who specializes in cryptocurrencies and blockchain litigation, told Bloomberg Law.

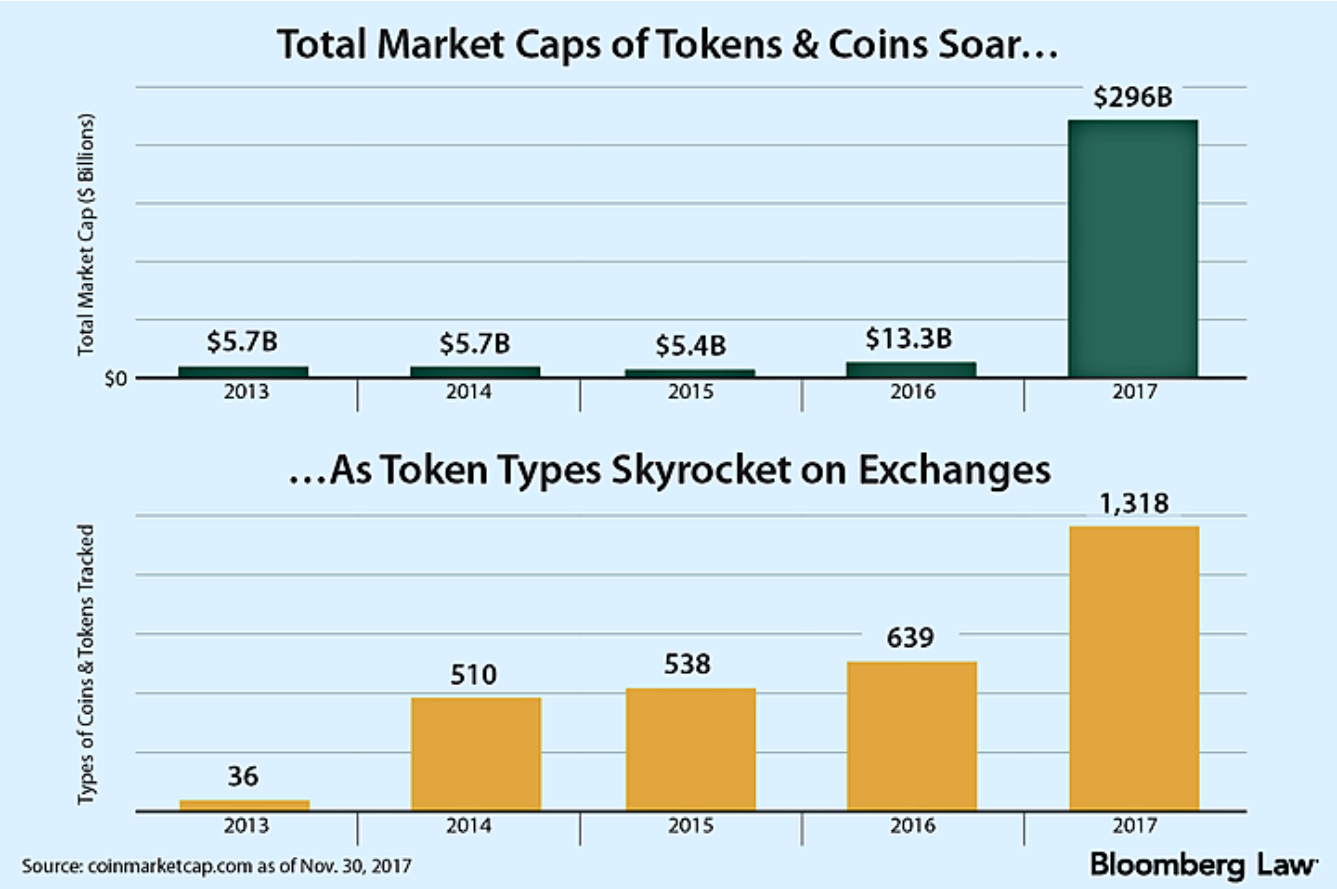
More than 1,300 token types tracked by industry research site coinmarketcap.com had a collective value of $295.6 billion as of Nov. 30. That's up from about 600 token types worth about $17.7 billion at the beginning of 2017, the site's data show.

More Lawsuits, Enforcement

The building global regulatory wave may impact how cryptocurrencies and assets are structured and valued. More lawsuits and heightened enforcement may encourage exchanges, such as Bitfinex and Poloniex, to be more mindful of transparency and consumer protection, leading to more credible operations, financial attorneys, digital asset think tanks, trade and advocacy groups said.

Still, those observers warn that stringent regulation, frivolous lawsuits or excessive caution by exchanges may make it tough for purchasers to trade some assets, causing valuation swings. Exchanges leery of legal breaches may limit the token types they issue or restrict who can trade on their platforms. That could discourage new issuers from developing new businesses or raising funds using the technology.

"If enforcement actions close or suspend trading on these alternative coin exchanges, the terrain for future ICO issuances could look very different," Andrew Hinkes, a dispute resolution attorney at Berger Singerman LLP, told Bloomberg Law.



Several U.S. agencies are likely to issue guidance or fines, or launch enforcement actions against exchanges that are manipulating markets, committing fraud, or aren't registered with the proper agency. International regulators, including in China and the U.K., have cracked down on token exchanges or issued early warnings to investors that some platforms can be risky and fraudulent or don't comply with securities laws, according to Bloomberg Law data.

Class action lawsuits from retail investors who fueled the market's heady growth will swell if the market cools, as expected, and fraud is exposed, financial and commercial litigation attorneys, digital asset think tanks and advocacy groups said.

"The bottom line is, if someone has $1 million worth of *x* coins and they lose that because of something an exchange does or a third party does, they're going to file a lawsuit," Stephen Palley, corporate and commercial litigation attorney at Anderson Kill P.C., told Bloomberg Law. "When you're trying to figure out who to sue, you look for the most obvious, you look for defendants who are easiest to identify and who have assets."

Eagle-Eyed Regulators

U.S. regulators—including the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and Internal Revenue Service (IRS)—will likely issue specific guidance for exchanges and fine those that don't comply, attorneys, think tanks and groups said.

"They are clearly engaged, they are clearly looking at this," Brian Knight, a senior research fellow at the Mercatus Center at George Mason University, told Bloomberg Law.

Bitfinex pulled out of the U.S. market in August, citing a "more challenging" regulatory landscape ahead.

A top priority for U.S. regulators will likely be determining how to classify digital coins. Some tokens are used like securities, while some are accepted as currencies. Others can be traded for goods or services. Regulatory classifications largely will dictate which agency mandates exchanges will need to observe.

"There's going to be some burden being placed on these exchanges to do some diligence as to what these tokens actually are," Knight said.

Federal agencies' regulatory approaches to regulating digital currencies have been generally thoughtful in light of the fast-moving technology, financial attorneys and token trade and advocacy groups said. Regulators' push to tighten industry oversight should be balanced against the spirit of innovation that has fueled the industry's growth, they said.

The SEC warned platforms in a July investigative report that it is illegal to trade security-like tokens without registering with the agency or getting an exemption.

"In addition to requiring platforms that are engaging in the activities of an exchange to either register as national securities exchanges or seek an exemption from registration, the Commission will continue to seek clarity for investors on how tokens are listed on these exchanges and the standards for listing; how tokens are valued; and what protections are in place for market integrity and investor protection," SEC Chairman Jay Clayton said in a Nov. 8 speech.

The CFTC considers virtual currencies to be commodities that can also be used as securities. The commission has fined two exchanges that traded derivatives of virtual currencies, or offered margin or leverage trading without first registering with the agency. In October, the agency also clarified its oversight of exchanges in cases of fraud or manipulation.

The Treasury Department's FinCEN, which mainly combats money laundering and other financial crimes, asserted its authority to regulate cryptocurrency exchanges by requiring them to register as money services businesses. The agency has already filed enforcement actions against two exchanges, including issuing a $110 million fine to what had been one of the world's largest exchanges by volume, BTC-e, in July, for violating money-laundering laws.

"Treasury's FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual currency exchanges and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards," Jamal El-Hindi, Acting Director for FinCEN said in a July statement.

The IRS, which summoned U.S. exchange Coinbase Inc. to produce thousands of records to investigate its users' possible tax evasion, may issue guidance for exchanges, Peter Van Valkenburgh, research director at Coin Center, a blockchain advocacy group, told Bloomberg Law.

"Tax implications for exchanges are complicated in part because the IRS has never issued really clear guidance on the reporting an exchange is supposed to do in regards to its customers' tax information," Van Valkenburgh said.

Lawsuit Surge?

Private lawsuits against exchanges also may start answering questions about how platforms should operate and whether assets are securities, Marco Santori, who leads Cooley LLP's fintech practice, told Bloomberg Law.

"I think one of the overlooked paths for this to take is that the private litigants who bring cases alleging violation of SEC law will have to demonstrate in court that the underlying asset was a security," Santori said.

Several class action cases have already been filed. There are many potential offenses customers might cite to file more lawsuits, commercial litigation attorneys said.

Investors who didn't realize their tokens were a security may also file suits if they see values drop, Knight said.

Most token platforms also don't have traditional protections that exchanges for registered securities or derivatives are required to have, such as asset-loss insurance, the SEC and CFTC have warned. The lack of these guardrails may make them more vulnerable to future consumer complaints, Hinkes said.

Token purchasers and traders may also target exchanges for alleged trading glitches, slow responses to trade orders or to flash crashes, market manipulation, trading against their own customers, artificially inflating trading volumes, and insufficient cybersecurity, David C. Silver, plaintiff attorney in several class action suits against exchanges, told Bloomberg Law.

There have been dozens of hacks or theft of digital assets on some of the world's largest exchanges, such as Mt. Gox in 2014 and Bitfinex in 2016. The high amount of instantly liquid tokens held on token exchanges, unlike securities exchanges, make them prime targets for hackers.

Tokens, similar to stocks, are also subject to being split into two entities, but with differing values, a technical process called "forking." And exchanges haven't always built the needed internal infrastructure to recognize the new assets, triggering some allegations of theft, Van Valkenburgh said.

Regulators and courts likely will tackle that and other questions in the year ahead, as they catch up with the burgeoning technology. The big question heading into 2018 is how much the new regulation and litigation will impact cryptocurrency exchanges trying to operate alongside traditional exchanges and financial offerings.

By Michaela Ross

To contact the reporter on this story: Michaela Ross in Washington at mross@bloomberglaw.com

To contact the editor responsible for this story: Keith Perine at kperine@bloomberglaw.com

Net Neutrality Rules Hinge on 2018 Battles in Courts, Congress

- Court challenge could turn on the issue of broadband classification
- Some GOP lawmakers seek permanent solution through legislation

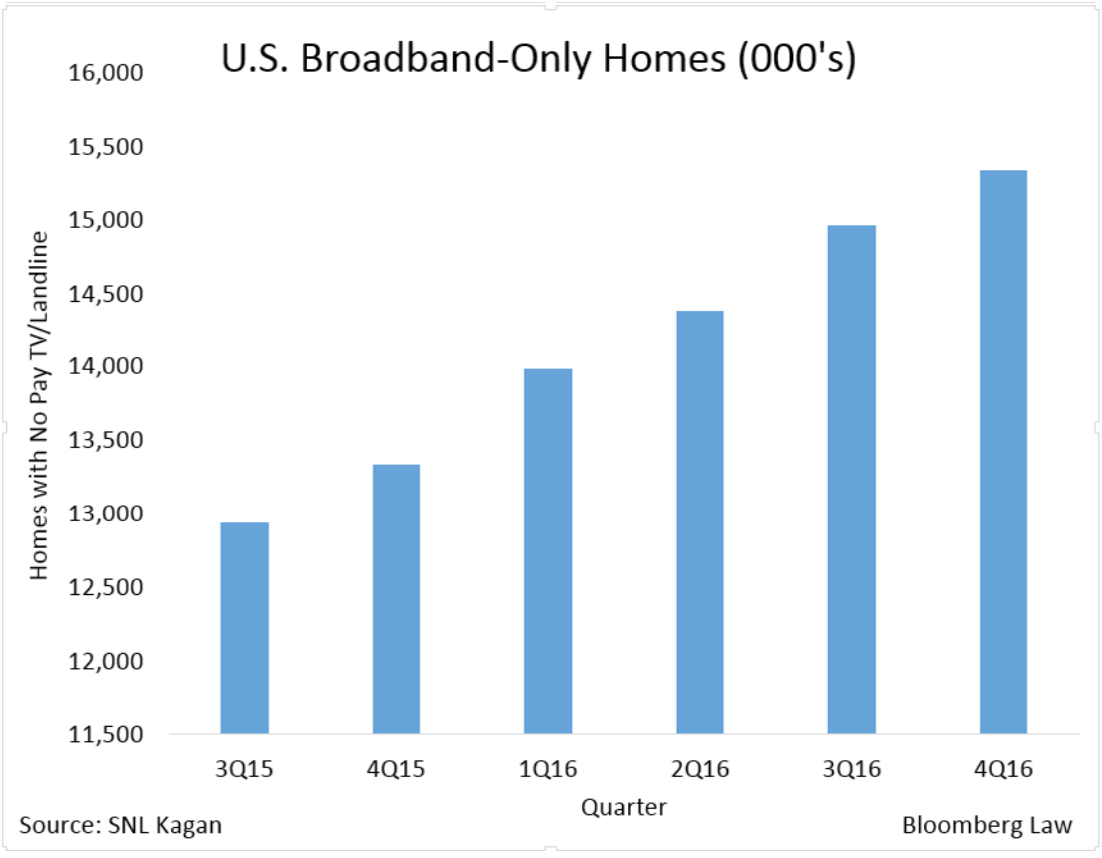
By Tara Jeffries

The fight over net neutrality rules for internet service providers such as AT&T Inc. and Comcast Corp. enters a new phase in 2018, as a likely court challenge to the Federal Communications Commission's decision to scrap most of the rules plays out.

The FCC rolled back rules barring providers from blocking or slowing data on their networks on a 3-2 party-line vote Dec. 14. The commission, led by GOP Chairman Ajit Pai, also undid its classification of broadband as a common carrier service, akin to traditional telephone providers, under communications law.

Pai's move sparked fresh regulatory upheaval in the internet ecosystem, including among broadband providers and tech giants such Amazon.com Inc., Alphabet Inc.'s Google, and Facebook Inc.

"The way things are setting up, there's just tremendous uncertainty," Mark Bartholomew, a State University of New York at Buffalo School of Law professor who specializes in net neutrality, among other subjects, told Bloomberg Law. "There's uncertainty about what the result of a lawsuit challenging Pai's reversal of the 2015 rules–what the outcome of that–will be," he said, referring to the Obama-era rules the FCC swept away.



Opponents of the FCC's move promised to challenge it in court. The coming fight pits the FCC, its GOP congressional allies, and ISPs against the tech giants, congressional Democrats, and public policy groups. Regardless of how courts decide the issue, Congress is likely to face renewed pressure to weigh in and settle the question of net neutrality for good.

How the debate is settled—in the courts or on Capitol Hill—will determine how much leeway the ISPs have to manage their own networks and position themselves competitively against the major content providers. Content companies, for their part, fear they'll be forced to pay for data "fast lanes"—or that ISPs will favor their own content on their networks as subscribers demand fast and seamless data streaming at ever-higher volumes.

Telling It to the Judge

Pai's opponents will probably argue in court that the FCC shouldn't be allowed to change its rules just because its chairmanship passed from a Democrat to a Republican. One likely argument: that the 2016 decision upholding the Obama-era net neutrality rules from the U.S. Court of Appeals for the District of Columbia Circuit—where the new challenges to the change are also likely to be heard—puts the rules on firm legal footing. That decision looms over the FCC as it prepares to defend its reversal once a lawsuit has been filed, analysts said.

The FCC is "somewhat tied up in a legal pretzel," Chip Pickering, CEO of Incompas, a tech trade group that plans to challenge the FCC, told Bloomberg Law. "The facts, the law, the politics make it very difficult for the FCC to change the policy."

Pai argues the agency acted legally. "There's no question that what we did was lawful," he told reporters Dec. 14.

The FCC will also likely cite a 2005 Supreme Court case, Natl. Cable & Telecomms. Assn. v. Brand X Internet Servs., blessing the classification of cable internet service as an information service. That precedent "is directly on point," GOP Commissioner Brendan Carr, formerly the agency's general counsel, told Bloomberg Law.

Despite the Democratic-controlled FCC's win at the D.C. Circuit in 2016, it's not clear which way the court would come down now. If that or another appeals court pauses the rule rollback—something opponents are likely to seek—ISPs and their tech customers may face prolonged uncertainty, analysts said.

"The first thing they'll do is try to get a stay," Berin Szoka, president of the policy group TechFreedom, told Bloomberg Law.

"I don't think that either side in this case will have a slam dunk," Ryan Radia, research fellow and regulatory counsel at the think tank Competitive Enterprise Institute, told Bloomberg Law.

Will Congress Act?

ISPs and content providers have both urged Congress to pass a bill to avoid more back-and-forth on net neutrality whenever a different party controls the FCC. Leading Republicans say that lawmakers should weigh in.

"It's way better to have Congress heard from on this—something we haven't addressed in over 20 years—than to have this constant cloud of uncertainty based upon politics and changing legal opinions," Senate Commerce, Science and Transportation Committee Chairman John Thune (R-S.D.) told Bloomberg Law.

Rep. Marsha Blackburn (R-Tenn.) said Dec. 14 that lawmakers will soon unveil a net neutrality bill that bans blocking and throttling.

But if Republicans want to pass net neutrality legislation, they may have to do it on their own. Democrats, hoping to regain control of at least one chamber in 2018, aren't inclined to negotiate with the GOP majority, aides say.

"There's enough opposition to a compromise that I still think the odds of a compromise are low," Radia said. "What happens early in the litigation will be a big determinant of that."

The Right Enforcer?

The FCC's move shifts enforcement power over ISPs to the Federal Trade Commission. The FTC has a track record of moving against companies that allegedly engage in deceptive practices, such as if an ISP slows data after saying it wouldn't. But Pai's opponents think the FTC doesn't set enough preventive rules, only stepping in after companies err.

The two agencies Dec. 11 announced a draft memorandum of understanding to divvy up regulatory responsibilities for broadband providers. Even so, the commissioners on both bodies are divided, along party lines, as to how effective a broadband enforcer the FTC may be.

Acting FTC Chairman Maureen Ohlhausen, a Republican, said in a Dec. 14 statement after the FCC vote that the FTC "is ready to resume its role as the cop on the broadband beat, where it has vigorously protected the privacy and security of consumer data and challenged broadband providers who failed to live up to their promises to consumers."

Carr, an FCC Republican, told Bloomberg Law that the FTC's broader reach makes it better suited to police the internet. But FTC Commissioner Terrell McSweeny, a Democrat, told Bloomberg Law the agency doesn't have the expertise to police bad behavior, such as discriminatory conduct, by ISPs.

Regardless of how the net neutrality debate plays out in the courts and Congress, the issue will not be decided anytime soon. The losing side in court likely will appeal the decision to the U.S. Supreme Court. That means more suspense for ISPs and content providers who could end 2018 as they begin it: waiting for regulatory certainty.

The debate is "a gift to the legal profession in Washington," Roslyn Layton, a visiting scholar at the American Enterprise Institute, told Bloomberg Law. "It's such a wild card."

--With assistance from Alexei Alexis and Michaela Ross.

To contact the reporter on this story: Tara Jeffries in Washington at tjeffries@bloomberglaw.com

To contact the editor responsible for this story: Keith Perine at kperine@bloomberglaw.com.

FCC's Media Deregulation Push Faces Legal Headwinds

- Court battles brewing over FCC efforts to relax national, local limits on scale of media companies
- Agency facing tough battle amid market concentration, statutory authority questions

By Kyle Daly

Broadcasters, consumer advocates, and regulators are bracing for extended legal fights in 2018 over media ownership rule changes that could usher in a wave of industry consolidation and reshape local journalism and TV programming nationwide.

Federal Communications Commission chief Ajit Pai has made changing the nation's media ownership rules a central issue in his first year. The commission is in the midst of unwinding several long-standing restrictions on media acquisitions. Opponents will battle the agency in court in 2018—and possibly beyond.

Pai's strategy of easing ownership limits in several layers will spark overlapping legal battles and could put more media properties in the hands of a small group of large companies.

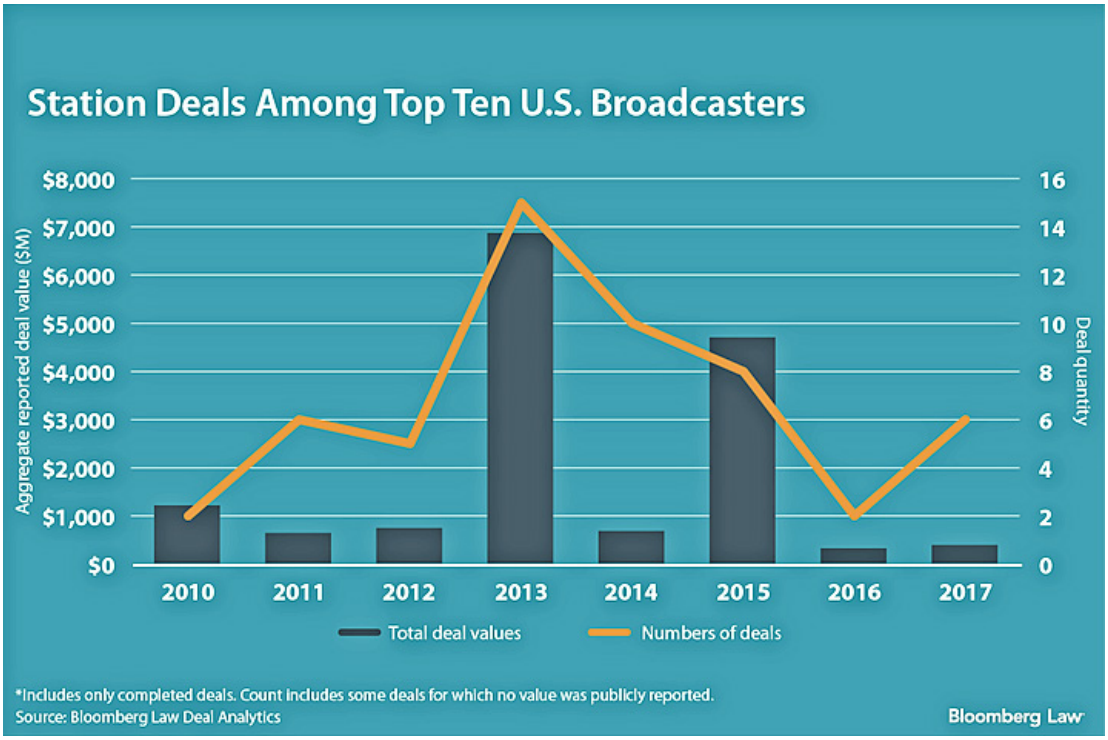
The outcome of those clashes will affect the future shape of the media industry. Loosening ownership limits could be a boon for broadcasters that want to be cross-platform juggernauts in the internet-driven world. Consolidation also could deliver to struggling media companies a lifeline by being acquired.

"There's been a pent-up demand for these changes for a long, long time," said David Rehr, a professor at George Mason University's Antonin Scalia Law School and former head of the National Association of Broadcasters, an industry trade group. "It may bring some new players into the market. It also, I think, will allow for a more efficient organization of broadcast television. But there will be opposition to this, of course."

The industry reorganization may not entirely favor consumers, advocacy groups say. Industry consolidation likely will disproportionately benefit deep-pocketed mega-broadcasters such as Sinclair Broadcast Group Inc., which is trying to acquire Tribune Media Co. Companies like Sinclair could cut local newsroom resources, impose their own political ideologies, and limit diversity of voices in local markets, say consolidation opponents, such as public-interest groups Free Press and Public Knowledge.

The industry has already undergone considerable consolidation in recent years. Five broadcasters owned 37 percent of the country's 1,790 local full-power TV stations as of the end of 2016, according to a Pew Research Center analysis. The top five station owners in the U.S. are Sinclair, Nexstar Media Group Inc., Gray Television Inc., TEGNA Inc., and Tribune, in order from largest to smallest.

Broadcast mergers totaled $12.9 billion in the five-year period from 2013 to 2017, compared to $4.0 billion in the five years before that, Bloomberg Law data show.



Among the biggest potential deals out there is the proposed $3.9 billion merger of Sinclair and Tribune, now pending FCC approval. And other big broadcasters could be eyeing more potential takeover targets. Rupert Murdoch's Fox Broadcasting, for one, may become an aggressive station buyer after being spun off from Twenty-First Century Fox Inc., if regulators approve the sale of that company's other assets to Walt Disney Co. At that point, Fox will "be in a mood to expand," and will "have the ability" to buy up more stations around the country, Murdoch told analysts Dec. 14.

Substantial further consolidation can't proceed without the changes in rules that dictate the maximum size and local market dominance of U.S. broadcasters that Pai has enacted or has in the offing. Under these, top station owners can substantially grow both their national footprint and hold over individual markets.

The FCC on Dec. 14, for instance, voted to begin writing a new rule to raise the limit on the market share a single broadcaster is permitted to own nationally. In November, it raised the limit on how much media an owner can control in a single market. Such changes, critics warn, could mean more consumers will have access to only the kinds of programs, and local news coverage, favored by station owners in their areas.

Each court case challenging Pai's moves will hinge on a different set of legal questions, and timing of court rulings will vary. Any panel decision from a federal appeals court will likely face a request for a full-court rehearing, and then U.S. Supreme Court review. Even if any challenges to a Pai change to ownership rules get an initial decision in 2018, that won't be the final word.

In the meantime, broadcast owners, including diversified companies such as Meredith Corp. that own both broadcast and publishing units, will likely ramp up acquisitions in light of the changes to media ownership rules, said CFRA Research analyst Tuna Amobi. "Right now, I think there's ample appetite from virtually all of the top broadcasters out there that want to take advantage of the relaxation of these rules."

Lifting National Ownership Cap

The December vote allows Pai to begin the process of easing limits on the national market share one broadcaster can own, currently at 39 percent of U.S. households.

Challengers to the national cap removal will argue that the FCC has no authority to modify the cap. Only Congress can alter the cap, they say.

Public interest groups, led by Free Press, have contended as much in their challenge to Pai's first major ownership limit relaxation effort. The FCC voted in April to bring back a discount for certain TV stations in the formula for calculating a broadcast company's national market share—a change that made the proposed Sinclair-Tribune deal possible.

The FCC shouldn't have restored the discount for ultra-high-frequency (UHF) stations because it's technologically obsolete since the transition of television signals from analog to digital in 2009, the groups said in their lawsuit filed in May in the U.S. Court of Appeals for the District of Columbia Circuit.

The FCC hasn't denied that the UHF discount is obsolete. But Pai has said the Democratic-controlled FCC shouldn't have eliminated the discount in 2016 without also reviewing the ownership cap. He plans to revisit the two issues together in the rulemaking launched Dec. 14.

GOP Commissioner Michael O'Rielly, who otherwise supports relaxing limits, shares Free Press' view that Pai lacks the authority to change the cap. But O'Rielly, who still voted for the rulemaking, says he wants to see the question "litigated out."

The FCC will likely counter that limiting national market share matters less now than it used to. Competition from online video, consolidation among cable companies, and sinking viewership for traditional television make the national cap less relevant, the FCC said in a draft of the rulemaking proposal released ahead of the vote.

Few expect the courts to settle in 2018 the issues of the national cap and the UHF discount, Bloomberg Intelligence analyst Matthew Schettenhelm said. If Pai acts quickly to eliminate or raise the cap, the UHF discount challenge could be rendered irrelevant, and arguments in that case could be rolled into an ownership cap change challenge.

Tough Fight Looms

The national cap rulemaking follows a party-line vote in November allowing companies to own more than one top-four TV station in a single market. The FCC also removed a rule that blocked TV stations in a single market from merging if the move would result in fewer than eight independently owned stations.

The restriction that barred companies from owning any combination of a newspaper, TV station, and radio station in a market was also lifted. These changes will soon be challenged in court, says Free Press, which plans to file its own lawsuit.

Underlying any challenges will be the premise that the FCC is abandoning its duty to preserve an independent press that serves local communities and the public interest. Allowing a handful of moneyed broadcast owners to swallow up locally run outlets could silence community voices and freeze women and minorities out of station ownership, media consolidation opponents say.

The FCC's rule changes "are appalling," said Andrew Jay Schwartzman, a senior counselor at Georgetown University's Law Center who has led challenges to the FCC's past deregulatory efforts. It "really threatens diversity of media."

FCC attorneys will counter that the traditional media industry is already under existential threat, and an infusion of resources from a moneyed owner will support local journalism. The restrictions Pai is targeting only make it harder for local TV stations and newspapers to survive, he's long said.

"The media ownership regulations of 2017 should match the media marketplace of 2017," Pai said at the November vote relaxing the rules.

The legal challenge to the local ownership changes is likely bound for the U.S. Court of Appeals for the Third Circuit. The court since 2003 has repeatedly turned back changes to media ownership rules for failing to demonstrate their effect on diversity in the industry. "We know it's going to go back to the same panel at the Third Circuit," Schettenhelm said. "Given this panel's history, the FCC's got a tough fight ahead of it."

Such jurisdictional issues and questions surrounding the FCC's statutory authority make it far from certain that the FCC will prevail on its recent and planned ownership rule changes, multiple broadcast attorneys privately say.

Updating media ownership rules to address an industry sea change is a signature Pai initiative. But he faces a series of fierce court battles that will take time to reach anything resembling a conclusion. The broadcast industry is unlikely to end 2018 with any more certainty than it now has.

"This is just the beginning," BIA/Kelsey broadcast analyst Mark Fratrik said.

To contact the reporter on this story: Kyle Daly in Washington at kdaly@bna.com

To contact the editor responsible for this story: Keith Perine at kperine@bna.com

Bloomberg Law®