No, cops aren’t using SiriusXM to find criminals. Here’s how they do it



reader comments

111 with 64 posters participating

Share this story

An Ars reader this week drew our attention to a news story out of Southern California. The case involved a man wanted on suspicion of attempted murder and other alleged crimes. He fled from one county to another, but according to the article, sheriff’s deputies were able to locate him by “sending a ‘ping’ to his Sirius satellite radio,” after which the suspect was found and arrested.

The mysterious “ping” grabbed the reader’s attention, as well as several Ars staffers: what, exactly, did law enforcement

do? How did it work? And what are the implications for everyone driving around with a SiriusXM satellite radio in their car?

The case

A representative for Sirius was unable to say if the company was involved in any specific way in this particular case or even if the case did indeed involve an actual Sirius product. Whatever happened, calling it a "Sirius radio ping" was probably a misnomer, the company told Ars, as Sirius satellite radio itself is a one-way operation. The actual radios have no geolocating capacity and can't "ping" anything back to anyone.

That said, however, Sirius isn't just a radio company—it offers a variety of "connected car solutions." Among those solutions is SiriusXM Guardian, which is available on the Fiat Chrysler Uconnect infotainment system. Cars that have telematics equipment installed by the manufacturer—in this case, Fiat Chrysler—can send data over mobile networks using Sirius' connected services. Those cars, Sirius said, are a small subset of the total number of vehicles that have satellite radios installed.

Sirius additionally told Ars that it sporadically works with law enforcement bodies to comply with valid vehicle-location court orders. The company stressed that it does so by remotely activating the installed telematics hardware in a car, rather than by interacting in any way with the actual satellite radio.

The San Diego County Sheriff's Department, which apprehended the suspect in its jurisdiction, said the man was driving a Jeep Wrangler. Uconnect has indeed been available in Jeep vehicles for several model years. The Imperial County Sheriff's Office (where the suspect fled from) confirmed to Ars both that the suspect was one of the registered owners of the car and also that there was a Uconnect subscription

registered to the vehicle.

The Uconnect privacy policy confirms that the service automatically collects user location data and that the company may share it, among other reasons, “to comply with applicable legal or regulatory obligations, including as part of a judicial proceeding, in response to a subpoena, warrant, court order, or other legal process, or as part of an investigation of or request by law enforcement or a government official.” It seems that is what happened in this case.

The context

The majority of new model cars, from all automaker groups, now have some kind of onboard connectivity platform available to buyers. Those platforms—such as BMW’s iDrive, Volkswagen’s Car-Net, Ford’s Sync, and General Motors’ OnStar—have similar language disclosing the potential sharing of location data in their terms of service or privacy policies.

This kind of tracking, which is not particularly new, is sold as a benefit to subscribers, who can access the stolen vehicle assistance feature after filing a police report about the theft. Such cases pop up in local media from time to time, including a California story from 2016 and a Florida example from 2017.

The ability for your car to be precisely tracked, though, comes with exactly the kind of privacy concerns you would think. In 2017, Forbes delved into the world of “cartapping,” in which law enforcement agencies used telematics services such as Sirius or OnStar to locate or eavesdrop on individuals under investigation.

Attorneys for defendants arrested after such location data was gathered tried to have the evidence thrown out, Forbes found, but in multiple cases, judges declined. In one instance, a judge ruled that accessing the onboard OnStar device in a

vehicle was not materially different from planting a GPS tracker on a suspect's car. In another, a different judge determined that someone in the car turned on OnStar services and the police just happened find drugs in the car when showing up to have a look.

"Location information is highly sensitive and deserves protection under the Fourth Amendment," American Civil Liberties Union staff attorney Nathan Freed Wessler told Ars. The technological ability for police to track almost any car in detail with essentially the push of a single button is new, legally speaking, and needs to be done carefully. "If police are going to use onboard telematics data at all, they should have to go to a judge and get a warrant," Wessler added.

It is unclear if Imperial County authorities had a court order for the vehicle location information in this case; the San Diego County authorities told Ars the suspect was allegedly suicidal during the 2:30am chase and that Imperial County law enforcement were concerned for his safety. In such exigent circumstances, Wessler said, where there is an "imminent threat" to someone's life or safety, an exception to needing a court order is fine in principle—but it's important that kind of exception not be abused.

https://arstechnica.com/?p=1640011

Unable to unlock gunman's iPhones, the FBI (once again)

asks for Apple’s help



reader comments

70 with 47 posters participating, including story author

Share this story

In a move that may signal another high-stakes clash over encryption, the FBI is asking Apple for help decrypting two iPhones believed to have belonged to Mohammed Saeed Alshamrani, the man suspected of carrying out a shooting attack that killed three people last month at the Naval Air Station in Pensacola, Florida.

The request came in a letter FBI General Counsel Dana Boente sent to her counterpart at Apple on Monday, NBC News reported. Boente said that, although FBI investigators obtained a search warrant to examine the phones, investigators have been unable to guess the passcodes needed to unlock them and decrypt their

contents. Complicating matters, 21-year-old Alshamrani fired a round into one of the phones. A second lieutenant in the Saudi Royal Air Force, Alshamrani died in the December 6 shooting. An FBI spokeswoman confirmed the sending of the letter but declined to describe its contents, citing an ongoing investigation.

In a statement, Apple officials wrote: “We have the greatest respect for law enforcement and have always worked cooperatively to help in their investigations. When the FBI requested information from us relating to this case a month ago, we gave them all of the data in our possession, and we will continue to support them with the data we have available.”

Company representatives didn’t say whether Apple would comply with the government’s request.

A new standoff?

The letter and Apple’s response may be the first steps in reviving a national standoff over encryption and the responsibilities technology companies face in helping law enforcement bypass it in their products. In 2016, the FBI obtained a court order requiring Apple to help unlock and decrypt the iPhone used by Syed Rizwan Farook, who killed 14 people and injured 17 others in a 2015 shooting rampage in San Bernardino, California.

Specifically, the FBI wanted Apple to create a custom firmware version that would bypass a protection that wipes an iPhone clean after 10 failed attempts to enter a passcode. In court documents and congressional testimony, FBI officials said they had no other way to access the contents of the iPhone so that investigators could determine if Farook and his wife (who also participated and died in the shooting) acted in concert with others to carry out the deadly attack. The government invoked an 18th-century law called the All Writs in seeking Apple’s

assistance.

Apple vigorously resisted the FBI request. In a spirited letter to Apple customers, company CEO Tim Cook warned that once the backdoor was created, it would pose a threat to all iPhone users. Cook argued that if Apple was compelled to bypass the protections on the shooter's iPhone, it would set a dangerous precedent that would undermine the privacy and security of people everywhere.

"The government suggests this tool could only be used once, on one phone," he wrote. "But that's simply not true. Once created, the technique could be used over and over again, on any number of devices."

The dispute was resolved six weeks after the government obtained the order when government lawyers dropped the case and reported that FBI investigators had decrypted Farook's iPhone 5C and no longer needed Apple's help. Then FBI Director James Comey later suggested that the agency paid more than $1.3 million to an unnamed company to crack the phone's encryption.

Critics of the government request said the FBI reversal bolstered their argument that the extraordinary assistance investigators sought was unnecessary because they had other less-intrusive means to decrypt the contents of the phone. The US Justice Department's Office of Inspector General later concluded that FBI personnel failed to exhaust all of the remedies available in unlocking Farook's iPhone.

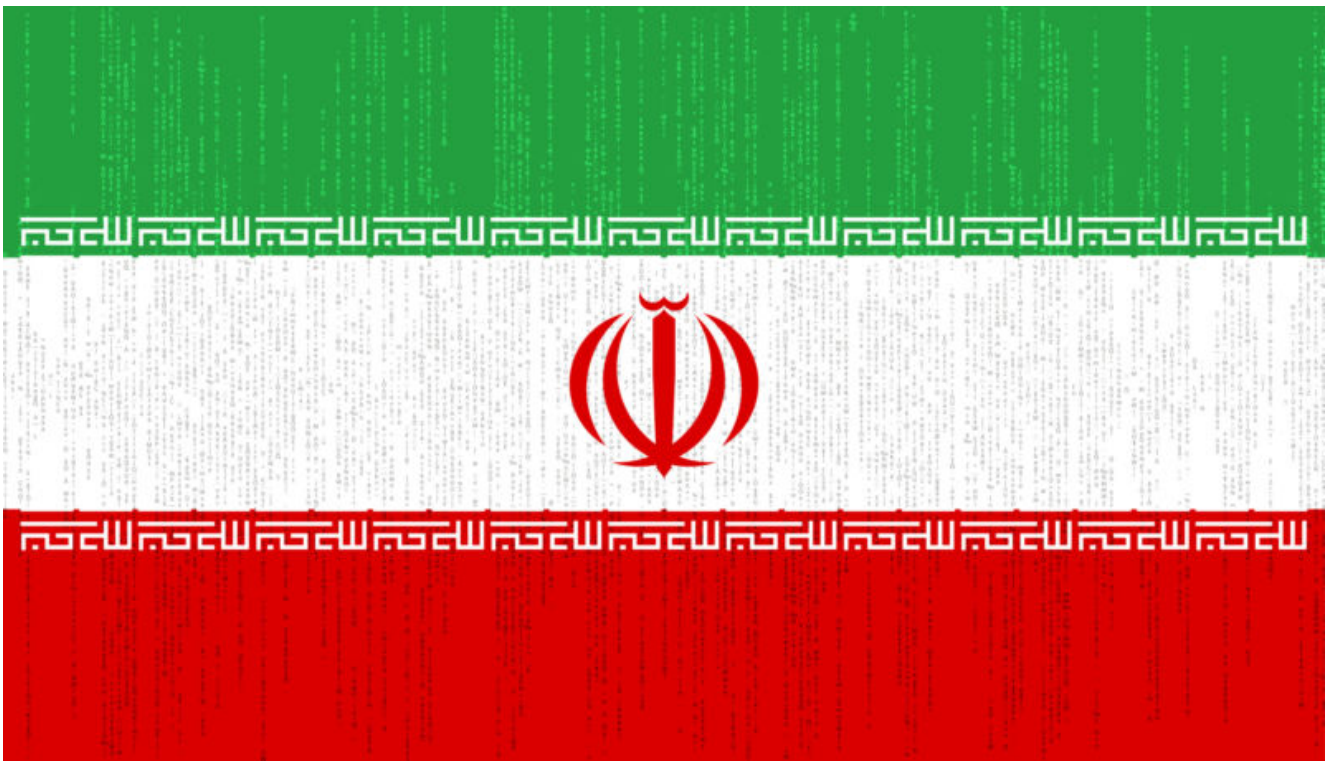
"We believe [the FBI's Cryptologic and Electronics Analysis Unit] should have checked with [Operational Technology Division's] trusted vendors for possible solutions before advising OTD management, FBI leadership, or the [US Attorney's Office] that there was no other technical alternative and that compelling Apple's assistance was necessary to search the Farook iPhone," the report stated.

In the three years since the standoff played out, both sides have further intensified their positions. Apple has strengthened the encryption in its phones, while Attorney General William Barr has renewed the push for backdoors and escalated complaints that encryption is hampering legitimate law enforcement investigations.

So far, the government has given no indication it plans to seek an order compelling Apple to defeat security protections in Alshamrani's device. But the request, and Apple's response, are both prerequisites before such an order could be obtained.

https://arstechnica.com/?p=1640633

Iran courted US security expert for years, seeking industrial hacking training



reader comments

23 with 20 posters participating

Share this story

Iran has over the past decade built up its own organic hacking and cyberwarfare capabilities. But the groups associated with orchestrating Iran's various cyberwarfare and cyber-espionage activities have also relied significantly on mining the work of others—and in at least one case, they have tried to bring in outside help for the ostensible purpose of training would-be hackers.

According to Chris Kubecka—a security researcher who played a prominent role in Saudi Aramco's response to the Iran-attributed Shamoon "wiper" malware—officials with the Telecommunication Company of Iran emailed and messaged her on behalf of the Iranian government, attempting "to recruit me to teach hacking in country against critical Infrastructure with focus on nuclear facilities," she told Ars.

These efforts, which Kubecka alluded to briefly in a

presentation at AppSec California in 2018, spanned over 2.5 years—during which Kubecka informed the FBI. “I was collecting evidence and communicating with them directly until last January when the FBI stepped in,” she said. “The last contact we had, the Iranians wanted my home address to send me ‘a gift’.”

The TCI contact offered Kubecka “up to $100,000 for one month” to come to Iran, Kubecka explained, to teach a Global Information Assurance Certification (GIAC) penetration tester advanced course for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. The trip included a scheduled “VVIP tour with pictures with their military,” Kubecka claimed. She showed some of the messages to Ars, including some of her communication with FBI.

Iran’s access to US information security tools and training is in theory blocked by sanctions against the country, though there have certainly been loopholes that could be exploited to get around those barriers. And when Iran approached Kubecka, UN sanctions had been partially lifted with the signing of the Joint Comprehensive Plan of Action (JCPA) in 2015—though US sanctions remained in place.

Though the Trump administration’s exit from the JCPA significantly impeded legitimate trade with Iran, the government can use proxies to gain technology that is restricted—including tools used by the TCI to censor Iran’s Internet and surveil Internet users. In the meantime, Iran has built its own organic capabilities atop off-the-shelf tools—some open source, some “cracked” commercial software—and lessons learned from its campaigns in Saudi Arabia and other Gulf states as well as against Western companies.

CISA has warned industry of Iran’s escalated activities, including new potential destructive attacks. And since then, there has been an uptick in the past few months in efforts to gain access and collect account information. In October and

November of 2019, the Iranian-attributed threat group APT33 targeted a total of about 4,000 organizations, mostly in the industrial controls space, with “password-spraying” attacks against hundreds of accounts at each organization.

In August and September of 2019, another Iranian threat group, APT35, was observed making thousands of attempts to breach the email accounts of the Trump presidential campaign organization. APT35 was also spotted trying to breach the email accounts of current and former US government officials and of journalists and Iranian expatriates.

https://arstechnica.com/?p=1640503

YouTube decides it’s easier to treat all watchers of kids’ content as kids



Enlarge / A young child watches a laptop computer.

reader comments

63 with 46 posters participating

Share this story

Congratulations, you’re a child again! Or at least you will be one as far as YouTube is concerned any time you happen to see a video designated as being “for kids.”

YouTube announced that change in a corporate blog post today, as the platform continues to try and thread a particularly tricky needle. YouTube (and the creators who use it) want to spread content as far and wide as possible, and they want to make as much money doing so as they can—but federal law limits what data companies can collect and use from the children who watch some of that content.

The changes stem from a $170 million settlement YouTube reached with the Federal Trade Commission last September over

alleged violations of the Children's Online Privacy Protection Act (COPPA).

Sin no more

COPPA governs the collection and use of personal data associated with children younger than age 13. Websites, apps, and other digital platforms that knowingly collect data from children are required to post a privacy policy and have parents consent to it. This is to give parents the option to opt out of having their children's information shared with third parties, to let parents review their children's data, and to make sites, apps, and platforms follow sound data storage and retention policies.

At the time, YouTube allegedly didn't discern between potentially underage visitors who might be visiting explicitly kid-friendly content and visitors ages 13 and up. Instead, the online video giant hoovered up all data equally. According to the FTC complaint, while Google said internally that it had no "child-directed" content and didn't need to worry about COPPA, it was at the same time telling companies such as Mattel and Hasbro that "YouTube was unanimously voted as the favorite website for kids 2-12" and "93 percent of tweens visit YouTube to watch videos."

The settlement wasn't just a fine; it also included an agreement that going forward, basically, YouTube would do better. Since last fall, the company has been making a series of changes that theoretically will help it handle kids' data more carefully.

All content creators who upload video to YouTube Studio for their video channels are now required to indicate whether the content is made for kids. If a video is indicated as "for kids," then data captured from *any* viewer of that content will be treated as coming from a child under 13.

Not as easy as it looks?

YouTube is also making its own algorithmic content determinations for videos that don't have specified a "for kids" / "not for kids" designation, using factors flagged by the FTC. "Creators know their content best and should set the designation themselves," the company said, adding that it will use machine learning to identify content featuring children's characters or themes, toys, or games, among other things.

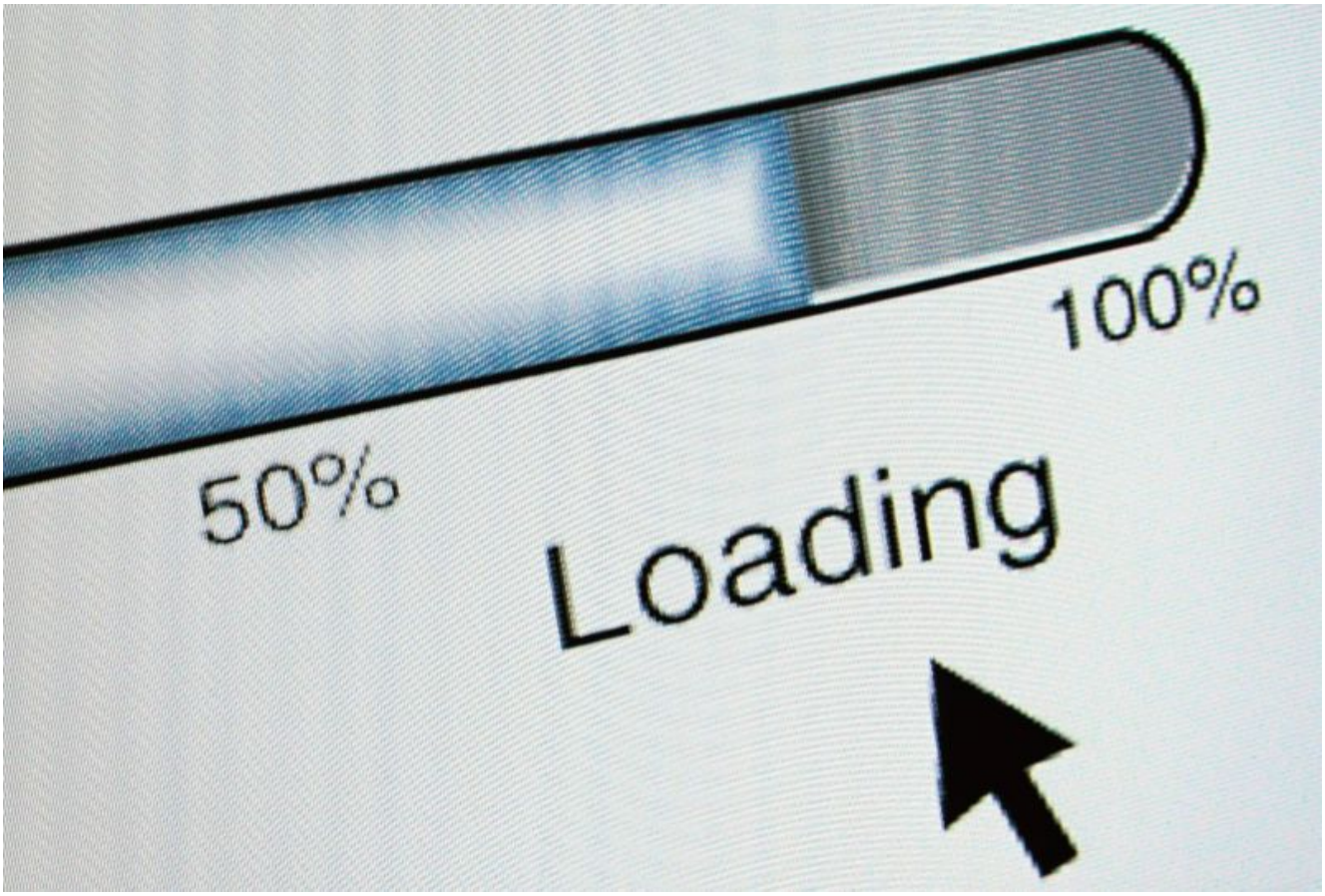
Content creators can "update a designation made by our systems if they believe it is incorrect," YouTube said. "We will only override a creator designation if abuse or error is detected."

YouTube content creators, who rely on the platform for their livelihoods, have for several weeks been raising the alarm about the new audience setting. Videos marked as "child directed" have comments, notifications, and personalized ads disabled, YouTube CEO Susan Wojcicki confirmed last year. Disabling those ways of engaging with a video could in turn lead YouTube's recommendation system to believe a video is simply not engaging and recommend it less to potential viewers.

Individual video creators themselves are also now personally on the hook for penalties of up to $42,350 if they fail to explicitly mark their videos as for children, the FTC said in November. This draws concern from creators who consider their content family-friendly but not necessarily child-directed.

https://arstechnica.com/?p=1639187

AT&T et al. fight against higher upload speeds in $20-billion FCC program



reader comments

79 with 55 posters participating

Share this story

AT&T, Frontier, Windstream, and their industry lobby group are fighting against higher Internet speeds in a US subsidy program for rural areas without good broadband access.

The Federal Communications Commission’s plan for the next version of its rural-broadband fund sets 25Mbps download and 3Mbps upload as the “baseline” tier. ISPs seem to be onboard with that baseline level for the planned Rural Digital

Opportunity Fund.

But the FCC also plans to distribute funding for two higher-speed tiers: namely an "above-baseline" level of 100Mbps down and 20Mbps up, and a "gigabit performance" tier of 1Gbps down and 500Mbps up. It's the above-baseline tier of 100Mbps/20Mbps that providers object to—they either want the FCC to lower that tier's upload speeds or create an additional tier that would be faster than baseline but slower than above-baseline.

FCC Chairman Ajit Pai has portrayed the $2 billion-per-year fund's goal as modernizing rural broadband by bringing up-to-gigabit speeds to remote corners of the nation. Companies pushing lower standards are trying to ensure that ISPs offering much slower speeds can get a large slice of that federal funding without making significant network upgrades.

The above-baseline tier's upload target should be 10Mbps instead of 20Mbps, according to an FCC filing on December 23 by Frontier, Windstream, and lobby group USTelecom (which represents those two providers as well as AT&T, Verizon, and others).

The providers and USTelecom claimed that 20Mbps upload speeds wouldn't benefit rural consumers much:

> *[W]hen considering network build-out using fixed wireless technologies, an upload target of 20Mbps likely drives significant additional deployment costs—up to two to three times as high—compared to a 10Mbps upload target. At the same time, a 20Mbps upload target provides little to no additional benefits to the end user customer as all key upload use cases, including HD streaming, video conferencing, and gaming can similarly be accomplished with 10Mbps. By adjusting the upload deployment target from 20Mbps to 10Mbps, the Commission can promote competition at the 100Mbps tier, incentivize additional broadband deployment, and make limited Rural Digital Opportunity Fund dollars reach further.*

The groups also gave the FCC a presentation making their case in more detail.

One problem with the providers' argument is that advertised broadband speeds in the US are basically the best-case scenario—consumers are offered "up to" a certain speed but often get less than that. If the providers succeed in getting significant funding for 10Mbps upload speeds, consumers could end up getting actual speeds in the single digits.

AT&T to FCC: "Reject… more costly tiers"

AT&T in October made its own filing that pushed for a slower tier of 50Mbps down and 6Mbps up "to encourage broadband deployment to as many locations as possible." The company also said the FCC "should reject proposals to over-emphasize more costly tiers." By that, AT&T means that the FCC should direct a larger share of the rural funding toward ISPs offering slower speeds.

On December 13, AT&T and other ISPs followed up with a proposal for a slightly slower tier than AT&T initially suggested, this time saying the new tier should be 50Mbps down and 5Mbps up (instead of the 6Mbps up that AT&T favored just two months previously). This December 13 filing was made by AT&T, Windstream, USTelecom, the Wireless Internet Service Providers Association (WISPA), and two small companies called Nextlink and Midco. The ISPs and trade groups urged the FCC to give more priority (or "weight") to ISPs offering their proposed 50/5Mbps tier than to ISPs promising 100/20Mbps.

Verizon filed comments in the FCC proceeding, too, but didn't suggest slower speeds. Verizon said the FCC should favor terrestrial broadband services and urged the commission to limit funding for high-latency satellite services to "exceptionally isolated or sparsely populated areas."

100/20Mbps already the norm in FCC fund

The Rural Digital Opportunity Fund would replace the similar Connect America Fund (CAF) that was created during the Obama administration. The CAF program is already mostly funding 100Mbps/20Mbps projects, so what AT&T and USTelecom propose would be a step back. As the FCC noted, the Connect America Fund Phase II auction in 2018 awarded $1.488 billion to ISPs that will serve 700,000 households and small businesses in 45 states, "with 99.75 percent of locations receiving at least 25/3Mbps service and more than half receiving at least 100/20Mbps service."

The proposed Rural Digital Opportunity Fund would provide $20.4 billion over 10 years and distribute the money in a reverse auction to ISPs that agree to provide service in rural areas at the required speeds to at least 4 million homes and small businesses. Like the existing Connect America Fund and all of the FCC's Universal Service programs, the new fund would be paid for by Americans through fees on their phone bills.

The FCC approved a Notice of Proposed Rulemaking to create the Rural Digital Opportunity Fund in August and then held a public-comment period. The FCC hasn't said when it will make a final decision on the fund's auction details.

Small ISPs support higher speeds

Two groups that represent smaller ISPs urged the FCC to reject calls for slower speeds. NTCA—The Rural Broadband Association and ACA Connects (formerly the American Cable Association) pointed out in a filing today that the Connect America Fund Phase II auction already included a 100Mbps/20Mbps tier.

"It would be remarkable 'backsliding' indeed from the CAF

Phase II auction to adopt lesser standards—such as lower upstream speeds or entirely new, lower speed tiers—for an auction that will be conducted at least two years later and will distribute funds into the early 2030s," NCTA and the ACA wrote. "Rather than closing the digital divide, USTelecom's proposal will only widen it."

Federal universal service law requires the FCC to promote deployment of telecom and information services to rural areas with quality and prices that are "reasonably comparable" to what's available in urban areas, and 10Mbps upload speeds are not up to that standard, the groups also told the FCC. The USTelecom proposal for slower upload speeds "runs counter to Chairman Pai's admonition that 'the Universal Service Fund must be forward-looking and support the networks of tomorrow,'" they wrote.

Another industry group that objects to the USTelecom proposal is the Fiber Broadband Association, which represents equipment vendors, ISPs, and others in the fiber industry. The group disputed USTelecom's claim that 20Mbps upload speeds provide "little to no additional benefits" over 10Mbps.

"[M]arket research data from RVA LLC show that average upload speeds in the US surpassed 10Mbps over two years ago, grew by 75 percent over the next year, and continues to increase significantly," the Fiber Broadband Association said. "Speed test data from Ookla show that average upload speeds are even higher—38.71Mbps as of December 2018 and increasing to 48.41Mbps as of November 2019." The group's filing included that data in an appendix.

Many Americans use Internet applications with significant upload requirements, such as social media, online gaming, video conferencing, uploading videos to YouTube, and offsite backup of files, the trade group said. The group's filing said:

> *Given the substantial and continuing growth in demand for upstream bandwidth, it is clear that the same virtuous cycle that has fed (and continues to feed) increased downstream consumer demand—higher performance infrastructure driving the development of more bandwidth hungry apps/content driving deployment of higher performance infrastructure—is now at work for upstream demand… Further, because funding for the Rural Digital Opportunity Fund program will flow at least through 2030, there is no support for adopting an already antiquated upstream speed of 10Mbps for the 100Mbps performance tier. In fact, the evidence supports just the opposite, adoption of an even higher upstream speed requirement.*

https://arstechnica.com/?p=1639471

Tired of hearing about Wi-Fi 6? Great, let's talk about Wi-Fi 6E



Enlarge / Expect to see an “e” tacked onto this logo somewhere in the near future, as an additional 1200MHz of spectrum becomes available to Wi-Fi 6 in the USA.

reader comments

93 with 41 posters participating, including story author

Share this story

On Friday, the Wi-Fi Alliance announced a new branding for the expansion of Wi-Fi into an additional 1200MHz of unlicensed spectrum.

Dubbed “Wi-Fi 6E,” the new spectrum should be made available for general Wi-Fi device use shortly; the US Federal Communications Commission proposed expansion of Wi-Fi into 6GHz spectrum in October 2018, and FCC chairman and novelty-coffee-mug aficionado Ajit Pai expressed a desire for the agency to “move quickly” (no concrete decision timeline was given) in opening up the spectrum to Wi-Fi at the Americas Spectrum Management Conference in September 2019.

What is Wi-Fi 6E?

Wi-Fi 6E is the Wi-Fi alliance’s branding for accessing the proposed new 6GHz spectrum using the existing Wi-Fi 6 protocol, otherwise known as 802.11ax. The new spectrum is right next door to the 5GHz unlicensed spectrum we’ve all been using since 802.11n (Wi-Fi 4). That means its RF characteristics are close enough to what we’re already accustomed to to require no further explanation: it’ll act just like 5GHz networking already does, for the most part.

What the new spectrum does is allow for much denser device-deployment strategies, by opening up the number of Wi-Fi “channels” which can be presented in one space without overlapping (and therefore congesting) with one another. The

additional 1200MHz can be divided into fourteen 80MHz-wide non-overlapping channels, or seven 160MHz-wide non-overlapping channels. Enterprise deployments could use the spectrum to allow much higher data-transfer rates to hundreds of devices all located near one another.

What would Wi-Fi 6E be good for?

The new spectrum would also be a potential large boon for consumer Wi-Fi mesh deployments—the great thing about Wi-Fi mesh is you don't have to run any wires; but the crappy thing about Wi-Fi mesh is that you didn't run any wires. When your mesh nodes have to talk to one another on the same channels that Wi-Fi devices already use to talk to them, latency goes up while speed and consistency go down.

The best Wi-Fi mesh kits already use three individual radios—one 2.4GHz for legacy devices: one 5GHz for modern design devices, and one 5GHz for backhaul. Unfortunately, this is generally enough for a single moderately-sized wireless LAN to effectively blanket the entire available Wi-Fi spectrum, all by itself. In very dense environments like apartment complexes, if any 5GHz neighbor networks are "audible," it may not be possible to set up a completely congestion-free network using only the existing, non-DFS allocated spectrum.

Without expanding either into the new 6GHz spectrum or into DFS (which doesn't work well in most urban areas), most users can realistically expect only two workable 5GHz, 80MHz, or 160MHz channels: one on the high band (above DFS frequencies), and one on the low band. In theory, the existing 5GHz spectrum can be divided into as many five non-overlapping, non-DFS 80MHz channels—but in practice, 160MHz deployments and the use of interstitial channels tend to make only one channel on each band viable, in spaces without tight RF controls.

If Wi-Fi gear is allowed to utilize another 1200MHz of contiguous spectrum, that suddenly makes it possible to have

extremely high-bandwidth (and therefore throughput) backhaul and fronthaul links available. Due to the rapid attenuation and blocking of 5GHz and 6GHz signals, the vast majority of physical spaces should then *realistically* have access to uncongested airtime in enough spectrum to come far, far closer to the kind of network quality one only expects in wired-backhaul commercial-style access points (such as Ubiquiti UAP, or TP-Link EAP) today.

Will you be able to use Wi-Fi 6E?

Decisions made by the US Federal Communications Commission are, obviously, only directly relevant to US users. But European users should see some additional spectrum opened for their use as well, though probably not the full 1200MHz proposed by the FCC.

It's unclear at this time whether existing Wi-Fi 6 hardware will be able to access the new spectrum once approved. In terms of physical design, existing hardware is more than likely OK—the antenna design to transmit and receive 5GHz should also work well at 6GHz. But there are serious questions about both how much is possible in firmware upgrades to existing Wi-Fi devices, and in how willing manufacturers will be to add this capability via free firmware upgrade rather than convincing consumers to buy a new gadget. We don't think vendors would be thrilled to give the capability away for free, so expect most to only implement it in new device designs.

With that said, we expect just having the new spectrum available to make an enormous difference in how well consumer Wi-Fi mesh networks can scale and provide high-quality Wi-Fi—even if the devices themselves don't support it. And very little guesswork or testing is needed in order to make this prediction—"more airtime, available over more spectrum" is much, much simpler to implement than radically new protocol

features like Wi-Fi 6’s OFDMA.

In *theory*, even Wi-Fi 5 (802.11ac) would work in the new spectrum—but in practice, don’t expect manufacturers to be interested in moving what’s rapidly becoming a legacy protocol into the new spectrum.

https://arstechnica.com/?p=1639355

Researchers unearth malicious Google Play apps linked to active exploit hackers



reader comments

44 with 30 posters participating

Share this story

Researchers have found more malicious Google Play apps, one of which exploits a serious Android rooting vulnerability so the app can take screenshots and collect other types of sensitive user information.

Camero exploits CVE-2019-2215, a potent vulnerability discovered in October by Google's Project Zero vulnerability research group, researchers from Trend Micro reported on Monday. The use-after-free flaw makes it easy for attackers to gain full root privileges on Pixel 1 and Pixel 2 phones and a host of other Android models. Google patched the vulnerability in October, a few days after Project Zero researcher Maddie Stone reported it was likely under active attack by either exploit developer NSO Group or one of its customers. All three apps are no longer available in Play.

Camero connected to a command and control server that has links to SideWinder, the code name for a malicious hacking group that has been targeting military entities since at least 2012. The app then downloaded attack code that exploits CVE-2019-2215 or a separate exploit in the MediaTek-SU driver that installs an espionage app called callCam. callCam collected a variety of sensitive user data including:

- Location
- Battery status
- Files on device
- Installed app list
- Device information
- Sensor information
- Camera information
- Screenshot
- Account
- Wi-Fi information
- Data of WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Gmail, and Chrome

To escape detection, callCam hid its icon after installation. It also used a complex cryptographic routine to encrypt stolen data before it was sent to attacker-controlled servers. callCam was also available as a standalone Google Play offering that advertised itself as a call and camera app. A third app, called FileCrypt Manager, meanwhile, installed callCam by abusing Android accessibility permissions to display screen overlays. Underneath, the app installed a series of apps that eventually ended with callCam.

While a certificate in one of the apps suggests the campaign has been active since March, Web search caches here and here show that Camero and callCam received only five and one install, respectively, from Google Play. The number of FileCrypt Manager installs wasn't immediately clear. Google removed the apps, so they are no longer available in the official Google Play store. It remains unclear if the apps are available elsewhere.

TrendMicro researchers Ecular Xu and Joseph C. Chen said the control servers to which the apps are connected are suspected of being part of the SideWinder infrastructure. A URL linking to one of the apps in Google Play is also found on one of the control servers. In 2018, researchers at Kaspersky Lab said SideWinder mainly targeted Pakistani military groups and had been active since at least 2012. Last month, a security researcher said on Twitter that SideWinder was likely behind attacks that exploited a now-patched vulnerability in the Equation Editor that's part of Microsoft Office.

People who want to check Android phones for infections can find indicators of compromise on the above-linked TrendMicro report. Google representatives had no comment for this post other than to confirm the apps have been removed from Play.

https://arstechnica.com/?p=1639397

Judge awards women $13 million in massive lawsuit against GirlsDoPorn



Anca Gabriela Rafan / EyeEm / Getty

reader comments

84 with 55 posters participating, including story author

Share this story

The operators of the popular GirlsDoPorn website owe nearly $13 million to 22 young women who were tricked and coerced

into shooting pornographic videos, a California judge ruled on Thursday. It took Judge Kevin Enright 187 pages to enumerate the many ways owner Michael Pratt and two co-conspirators mistreated the women.

“Plaintiffs have suffered and continue to suffer far-reaching and often tragic consequences,” the judge wrote. “Collectively, they have experienced severe harassment, emotional and psychological trauma, and reputational harm.” Damages include “lost jobs, academic and professional opportunities, and family and personal relationships.” Their lives were “derailed and uprooted,” with several plaintiffs contemplating suicide.

The group behind GirlsDoPorn recruited women by advertising clothed modeling gigs on Craigslist and elsewhere. When a woman responded to an ad, they were told that the job was actually shooting porn. However, the women were told that they could make $5,000—sometimes even more—in a single day of shooting. And these women were then assured that their videos would never appear on the Internet. Instead, footage would be burned to DVD and sold to private collectors in Australia and New Zealand. All of this turned out to be lies. Within weeks of shooting, the women’s videos appeared on GirlsDoPorn and various free pornographic “tube sites.”

The women were also promised that their confidentiality would be protected. Instead, their real-life identities quickly circulated online, causing them immense embarrassment with friends and family. Pratt himself owned PornWikiLeaks, a site dedicated to outing the women on sites like GirlsDoPorn, for several months. The judge found substantial circumstantial evidence that Pratt personally seeded the site with private information about GirlsDoPorn women.

The trial began last August and dragged on until November—largely because it took that long for the court to hear about the experiences of each of the 22 women. Lawyers

for the women say they've talked to many others who had similar experiences. However, the others were unwilling to face the risk of retaliation from the defendants or the humiliation of publicly re-living their experiences.

As the trial was getting under way, Pratt was getting out of town. He departed the United States in the early weeks of the trial and his exact location isn't known. He has also shifted assets overseas. The judge concluded that this was a calculated attempt to prevent the women from recovering damages in the case.

Coercive tactics

Lawyers for Pratt and the other defendants argued that the women weren't victims at all. They had voluntarily boarded airplanes knowing they were going to shoot porn, they said. Once they arrived, the defendants argued, they signed binding contracts and then voluntarily went through with the porn shots. Lawyers for the defense argued that this was simply a case of seller's remorse.

But Judge Enright decisively rejected that argument, pointing to numerous examples of fraud and coercion throughout the process of recruiting the models and shooting the videos.

Most obviously, the defendants were lying when they said that the videos wouldn't show up online. To bolster this lie, the defendants paid other women to pose as former models and reassure recruits that they would have a positive experience and that their videos would remain private. Pratt and his colleagues were careful to make these promises over the phone, not in writing. But the consistent stories of the 22 women—as well as corroboration from some junior figures in the GirlsDoPorn empire—confirmed that the girls were lied to repeatedly.

Once a woman arrived in San Diego, the GirlsDoPorn crew's

tactics shifted from fraud to intimidation. Women were picked up at the airport by a GirlsDoPorn staffer and chaperoned throughout their visit. During shooting, they were alone with two or more men they didn’t know. The men would become agitated if the women didn’t cooperate; some women testified that they feared for their safety. Women testified that men stacked equipment in front of the door to prevent them from leaving the room.

The men waited until minutes before the scheduled start of shooting to present women with lengthy contracts. They were then pressured to skim the documents quickly and sign them so that the shooting could get under way.

Most of the women had flown to San Diego from out of town, and many lacked funds to rent a hotel or book a flight home. They were also loath to call for help, since they’d have to admit why they’d traveled to San Diego in the first place. As a result, several women felt they had little choice but to complete the shoot.

Judge Enright ruled that all of these factors made the women’s nominal consent meaningless. The contracts were unenforceable because the women were induced to sign them by fraud and coercion. The shooting of the videos was not truly voluntary because most of the women did not feel free to leave.

Joint liability

The judge awarded each woman $300,000 to $550,000 in compensatory damages and an additional $150,000 in punitive damages. In total, the defendants collectively owe the women $12.8 million.

A big question now is how much the women will actually be able to collect. As mentioned above, ringleader Pratt has fled the country and may not be easy to track down. The other two men, Andre Garcia and Matthew Wolfe, have been arrested in a

related criminal case, however it’s not clear what assets they have. The judge awarded the damages jointly against all of the defendants, so the action has a good shot at bankrupting all three of them.

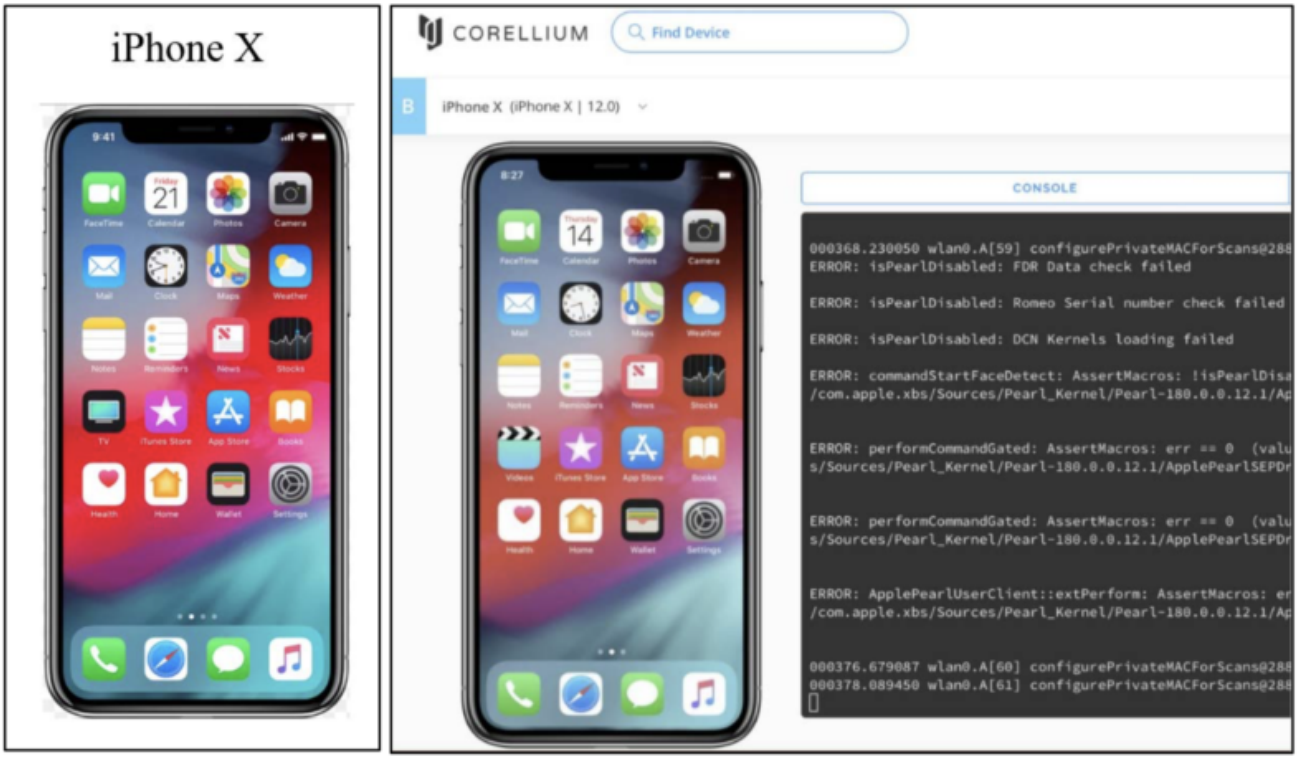
Remarkably, despite a high-profile lawsuit and a criminal prosecution, the GirlsDoPorn website is still online. At least one new woman’s video was posted online during last fall’s trial. The plaintiffs’ lawyers will have to figure out who currently owns the site—likely some kind of overseas shell company—and where they keep their funds.

If the defendants do try to continue operating GirlsDoPorn, the judge ordered them to stop lying about where the videos go. He ordered them to prominently disclose in contracts that women are shooting for GirlsDoPorn—and to send the contracts to prospective models before they set foot on an airplane. Of course, with the principals in jail or on the lam, it’s not clear how they’ll find time to try to recruit new models for the site.

Thanks for Courthouse News’s Bianca Bruno for posting a PDF of the ruling.

https://arstechnica.com/?p=1638693

Apple targets jailbreaking in lawsuit against iOS virtualization company



Enlarge / An image from Apple’s lawsuit shows a real iPhone X and Corellium’s service running a virtual iPhone X.

reader comments

48 with 33 posters participating

Share this story

Apple has expanded a lawsuit against an iOS virtualization company, claiming that its actions facilitate jailbreaking and violate the Digital Millennium Copyright Act (DMCA) prohibition on circumvention of copyright-protection systems.

Apple sued Corellium, a company that sells access to virtual machines that run copies of the operating system used in iPhones and iPads, in August 2019. We detailed the initial allegations in a previous article; Apple said that Corellium sells “perfect replicas” of iOS without a license from Apple and markets its software as “a research tool for those trying to discover security vulnerabilities and other flaws in Apple’s software.” But instead of aiding good-faith security research, Corellium “encourages its users to sell any

discovered information on the open market to the highest bidder," Apple alleged.

The first version of Apple's lawsuit accused Corellium of copyright infringement. A new version filed on December 27 alleges both copyright infringement and "unlawful trafficking of a product used to circumvent security measures in violation of 17 U.S.C. § 1201," a statute that's part of the DMCA. Apple argued that Corellium gives users the ability to jailbreak iOS for either benign or malicious purposes.

Apple "demonizes" jailbreaking, Corellium says

Corellium CEO Amanda Gorton responded to the newly expanded allegations in a blog post, writing that "Apple's latest filing against Corellium should give all security researchers, app developers, and jailbreakers reason to be concerned."

Corellium is "deeply disappointed by Apple's persistent demonization of jailbreaking," with Gorton writing that "developers and researchers rely on jailbreaks to test the security of both their own apps and third-party apps." Apple's filing, according to Corellium, essentially "assert[s] that anyone who provides a tool that allows other people to jailbreak, and anyone who assists in creating such a tool, is violating the DMCA."

Apple, Gorton wrote, "is using this case as a trial balloon in a new angle to crack down on jailbreaking" and "is seeking to set a precedent to eliminate public jailbreaks."

The case is in the US District Court for the Southern District of Florida.

Jailbreaking of smartphones and tablets such as iPhones and iPads is allowed in the US due to a DMCA exemption granted by the US Copyright Office (a division of the Library of

Congress).

The Copyright Office says the DMCA exemption for jailbreaking phones and tablets is intended "to allow the device to interoperate with or to remove software applications." There's also a DMCA exemption for security research on all types of devices. But to qualify for the security exemption, it must be "good-faith security research" that is "carried out in an environment designed to avoid any harm to individuals or the public."

The Electronic Frontier Foundation describes DMCA exemptions in general as "too narrow and too complex for most technology users."

Corellium bypasses encryption and hardware checks, Apple says

Apple argues that Corellium's alleged DMCA violations enable both violations of Apple's copyright and the spread of security vulnerabilities.

Apple's updated lawsuit notes that iOS uses "technological protection measures that control access to and protect Apple's exclusive rights in its software," such as "measures that prevent iOS and iTunes from being installed onto non-Apple-manufactured hardware." Apple said iOS also has "software restrictions that prevent unfettered access to the operating system," for example by "prevent[ing] a user from modifying the operating system."

Corellium violates Apple's rights by "enabl[ing] its users to circumvent the security protections that Apple has implemented to protect its copyrighted works and its exclusive rights in those works," Apple's updated lawsuit says.

Apple alleges that Corellium's sale of iOS replicas without Apple's authorization amounts to "trafficking in technologies,

products, or services" designed to bypass or remove technological measures that control access to Apple's copyrighted works, in violation of Section 1201. Those Apple technological measures "include encryption, hardware checks, and server checks that prevent iOS from being installed and executed on non-Apple-authorized hardware, and prevent unfettered access to the iOS operating system."

While Apple accused Corellium of facilitating jailbreaking, the alleged jailbreaking is of virtual iOS devices and not physical iPhones and iPads. Apple wrote:

> *The Apple Corellium Product also provides users with the ability to "jailbreak" virtual iOS devices. Jailbreaking refers to the act of modifying iOS to circumvent the software restrictions that prevent unfettered access to the operating system. Corellium openly markets the ability of its technology to "jailbreak… any version" of iOS. Corellium provides its jailbreaking technology to all its customers, regardless of their purpose.*

Apple also said that Corellium's product "makes modifications to iOS that allows it to be installed on, and run from, Corellium-developed or Corellium-operated hardware. Such modifications include disabling loadable firmware validation, disabling self-verification of the FIPS [Federal Information Processing Standard] module, adding Corellium software to the 'trust cache,' and instructing the restore tool not to contact Apple servers for kernel/device tree/firmware signing."

Apple: Corellium doesn't care about security

While Corellium argues that its software helps companies identify iOS bugs for the purpose of improving the product and protecting users, Apple claims that Corellium "makes no effort

whatsoever to confine use of its product to good-faith research and testing of iOS."

Apple cited a Motherboard article that describes Azimuth Security as Corellium's first customer. Apple wrote:

> *The Motherboard article reported that Azimuth sells a range of tools that exploit flaws in software. Azimuth's customers reportedly include foreign governments, including foreign intelligence agencies. And when a reporter recently asked Azimuth's founder Mark Dowd, whether Azimuth had ever reported a bug found using Corellium to Apple, he answered, "no." Contrary to its lofty rhetoric, Corellium in fact sells Apple's technology and the ability to circumvent the security measures embedded in that technology for its own profit, and makes no effort to ensure its customers are engaged solely in good-faith security research.*

iFixit founder Kyle Wiens, who has testified to the US Copyright Office in support of legalized jailbreaking for the purpose of fixing products, wrote yesterday that Apple's complaint is "a dangerous DMCA lawsuit." If Apple wins, "the damage will reverberate beyond the security community and into the world of repair and maintenance," Wiens wrote.

Corellium hasn't filed its response to Apple's expanded complaint in court yet, but the company vowed a strong fight. "We are prepared to strongly defend against this attack, and we look forward to sharing our formal response to this claim when we file it in court," Gorton wrote.

As for the more straightforward copyright allegation that Corellium sells replicas of iOS without a license from Apple, a Corellium response in October claimed that "Apple impliedly, directly, or indirectly, authorized, licensed, consented to, or acquiesced to Corellium's allegedly infringing use of Apple's works." Corellium wrote that Apple was "aware of Corellium's technology for several years" and "encouraged its

development.”

“During this time, Apple approved of Corellium participating in its invitation-only Security Bounty Program (‘bug bounty program’) with a promise to pay for software bugs identified by Corellium. While Apple gladly accepted and utilized bugs submitted by Corellium as part of this program, it broke its promise to pay for them,” Corellium wrote. Apple eventually “announced its own competing product and soon after sued Corellium,” the response said.

Corellium also claimed it “has made quintessential fair use of Apple’s technology.”

“Corellium’s technology is highly transformative because it does not merely replicate Apple’s products for the same purposes for which the products were developed. Instead, Corellium’s technology utilizes portions of Apple’s technology for entirely distinct purposes, which provide significant societal benefits,” Corellium wrote.

Rather than using or replicating iOS, Corellium claimed that it “uses its own proprietary software to facilitate executing iOS on different hardware.”

https://arstechnica.com/?p=1638563

Oracle copied Amazon’s API—was that copyright infringement?



Enlarge / An Oracle building in the San Francisco Bay Area.
Smith Collection/Gado/Getty Images

reader comments

177 with 63 posters participating

Share this story

Charles Duan is the Director of Technology and Innovation Policy at the R Street Institute, a nonprofit think tank based in Washington, DC . He has authored several amicus curiae briefs in the litigation between Oracle and Google, as well as the article Internet of Infringing Things: The Effect of Computer Interfaces on Technology Standards. The R Street Institute has received financial support from Google. The opinions expressed here do not necessarily represent those of Ars Technica.

Early this year, the Supreme Court will hear an important case that will determine the legal status of application programming interfaces under copyright law. If the high court sides with Oracle in its multibillion-dollar lawsuit against

Google’s Android platform, it could stifle competition and entrench dominant technology firms—possibly including Google itself.

Oracle has accused Google of infringing copyright law by copying the API of the Java programming language. An API is essentially a language for instructing a computer on what to do. It includes a vocabulary of named commands tied to grammatical structures for how those commands are to be used. To cause Java software to perform pre-defined tasks, such as calculating a sine function or encrypting a message, a programmer must use those named commands and grammatical structures with precision, much in the same way that a Waffle House diner invokes exact code words like “scattered, smothered, chunked, and diced” to get a hash brown order correct.

Google’s Android was designed to be compatible with the Java API so that programmers already familiar with Java could easily bring their software and knowledge over to the new mobile device platform. To do this, Android had to exactly copy the relevant Java API commands and grammatical structures. Oracle’s argument is that this “reimplementation” of the Java API is on par with writing an unauthorized “Harry Potter” novel and thus an infringement of Oracle’s copyrights in the command names and structures of the Java API.

But the Java API is not the only API, and Android is not the only reimplementation. APIs are found all over modern technology, and reimplementation is a key part of ensuring competition in the computer industry and preventing large-firm lock-in.

Did Oracle infringe copyright by

copying Amazon’s S3 API?



David Ryder/Getty Images

Consider Amazon’s popular data storage platform, S3. To allow programmers to store and retrieve files on S3, Amazon built a comprehensive, detailed API for interacting with the service. To get a list of stored files, for example, one sends the command name *GET* with the folder name as a grammatical object, along with cryptically tagged information such as *encoding-type*, *continuation-token*, and *x-amz-date*. Software must use these exact, cryptic terms and a bevy of others to work with Amazon S3.

Unsurprisingly, competitors have sprung up to Amazon’s market-leading cloud services. To convince programmers to switch away from Amazon’s offerings, those competitors reimplement S3’s API. In doing so, the competitors must mimic the command names, parameter tags, “*x-amz*” phrasing, grammatical structure, and overall organization of the S3 API—in other words, exactly the kind of thing Oracle argues is protected by copyright.

To be sure, a competitor may use a different programming language than Amazon did so the internal software code might not look like verbatim copying. But implementing an API in another computer language is simply an act of translation, and translating a copyrighted work into another language is specifically known to be a copyright infringement.

Among the companies offering a copy of Amazon's S3 API is Oracle itself. In order to be compatible with S3, Oracle's "Amazon S3 Compatibility API" copies numerous elements of Amazon's API, down to the *x-amz* tags.

Did Oracle infringe Amazon's copyright here? Ars Technica contacted Oracle to ask them if they had a license to copy Amazon's S3 API. An Oracle spokeswoman said that the S3 API was licensed under an Apache 2.0 license. She pointed us to the Amazon SDK for Java, which does indeed come with an Apache 2.0 license.

However, the Amazon SDK is code that uses the S3 API, not code that implements it—the difference between a customer who orders hash browns and the Waffle House cook who interprets the orders. Code that uses an API will be organized completely differently from code that implements one; it may not even contain the whole API. And Oracle has for years argued that using an API is unrelated to reimplementation and not an infringement of copyright (or else every app developer using Java would infringe). Oracle can't simultaneously argue that API-using code does not embody copyrighted material from an API, and yet API-using code embodies all copyrights in the API necessary to give Oracle the right to reimplement S3.

Even if the Apache license does apply, Oracle doesn't appear to comply with the terms of the license. Section 4 of the Apache license requires notices and attribution statements attached to derivative works. Yet I find no attribution to Amazon or relevant mention of an Apache license on Oracle's documentation or anywhere on the site.

API copyrights could create a legal minefield

Oracle is by no means alone in reimplementing an API like Amazon S3. A handful of cloud storage systems do the same. And there are abundant other APIs and reimplementations across the technology industry. Technical standards like Wi-Fi and Internet protocols—the glue that keeps the information economy connected—all involve APIs, and every computer and device that uses any modern communication technology necessarily reimplements them. Oracle's copyright theory could turn almost anything you do with a computer—from reading an online document to watching a video—into a legal minefield.

To avoid these far-reaching consequences, Oracle and the appeals court that endorsed Oracle's arguments have tried to limit copyright infringement to partial reimplementations of an API that are "incompatible" with the original. But partial reimplementations are commonplace and often expected. Even Oracle's S3 compatibility API notes its numerous "differences" and incompatibilities with Amazon's API.

The danger of Oracle's copyright lawsuit is that it could prevent smaller technology companies from building compatible versions of dominant software platforms. Without such compatibility, software programmers familiar with a dominant firm's API will effectively be locked into that firm's offerings. Sure, the competitors can ask for permission to use an API, but giving companies gatekeeper power over competition through copyright law cannot bode well for a robustly competitive software marketplace.

Update: Oracle sent Ars Technica the following statement.

> *The Apache license is a permissive open source license and any use-case-specific argument (e.g., "SDK vs. non-SDK") doesn't change the availability or nature of the license. It*

allows downstream users to copy and modify code, and use the code in their own projects, with few restrictions. That is why Apache-licensed code is widely used in commercial products. AWS understands this and obviously consciously chose to use a more permissive vs. more restrictive license (such as the GPLv.2).

https://arstechnica.com/?p=1635339