McCollough|Henry PC

dotLAW.biz
1250 South Capital of Texas Highway
Building 2, Suite 235
West Lake Hills, Texas 78746
Phone: 512.888.1112
Fax: 515.692.2522
wsmc@dotlaw.biz

November 8, 2014

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Written ***Ex Parte*** Filing

Open Internet Remand Proceeding, GN Docket No. 14-28; *Framework for Broadband Internet Service*, GN Docket No. 10-127; *Technology Transitions*, GN Docket No. 13-5; *A National Broadband Plan for Our Future*, GN Docket No. 09-51; *State of Wireless Competition*, WT Docket No. 13-135; *Broadband Industry Practices*, WC Docket No. 07-52

Dear Ms. Dortch:

Golden Frog, GmbH submitted Initial comments in the above docket on July 18, 2014. *See, e.g.*, http://apps.fcc.gov/ecfs/document/view?id=7521709960. Verizon submitted a letter responding to Golden Frog's comments on October 28, 2014. The letter is available at http://apps.fcc.gov/ecfs/document/view?id=60000976476.

Golden Frog addressed Verizon's letter in two "blog" postings. The first is "The FCC Must Prevent ISPs From Blocking Encryption." This was released on November 4. It is publicly available at http://www.goldenfrog.com/blog/fcc-must-prevent-isps-blocking-encryption, and a printed version is attached hereto. The blog hyperlinked to two press reports (https://www.techdirt.com/blog/netneutrality/articles/20141012/06344928801/revealed-isps and http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/mobile-isp-thwarted-customers-attempts-to-send-encrypted-e-mails-research-finds/, respectively) that are also reproduced and attached.

On November 6 Golden Frog blogged again. "Hey Verizon, We agree with you," posted on November 6, and available at http://www.goldenfrog.com/blog/hey-verizon-we-agree-with-you. The posting is also reproduced and attached. That posting also contained a hyperlink to the previously-mentioned and reproduced Washington Post article.

The blog posts more than adequately respond to Verizon's letter, so further elucidation by counsel is not necessary.

Sincerely,

W. Scott McCollough
Counsel for Golden Frog, GmbH

November 4, 2014

The FCC Must Prevent ISPs From Blocking Encryption

Last month, the popular online publication TechDirt published an article based on Golden Frog's filing with the FCC that urged the commission to truly restore an Open Internet. A key portion of the article focuses on how we noticed that ISPs and wireless broadband providers can block encryption technologies if they desire.

We discovered this by studying the service of a particular wireless broadband provider, and discovered it was able to interfere with the ability of one of our engineers to encrypt their email communication.

The article gathered a fair amount of attention and we received questions from the press (including the Washington Post), advocacy groups and our customers. We wanted to share the full story:

A Golden Frog engineer first noticed the issue in September 2013 when he was an AIO Wireless customer. (AIO was a prepaid wireless service provider and subsidiary of AT&T). Being a privacy-focused individual, he set his email client to require using an encrypted connection to his email server using STARTTLS. STARTTLS is an extension to SMTP (the standard email sending protocol) that allows an email server and client to use TLS (Transport Layer Security) to provide private, encrypted, and authenticated communication over insecure Internet connections.

In May 2014, AIO merged with Cricket Wireless so the Golden Frog engineer became a Cricket customer. In June 2014, he brought the issue to the attention of Golden Frog Co-CTO Michael Douglass while the two were working together at a coffee shop. While using his laptop tethered to his phone and connected via Cricket, he was unable to send email securely. He switched to the coffee shop's Wifi and was able to send encrypted email. They concluded that STARTTLS was being intercepted.

The two investigated further and started running tests. They determined Cricket was intercepting and blocking STARTTLS on port 25 – basically, the STARTTLS command was masked out in server responses, and a command failure response was returned. The engineer was connecting to a personal mail server NOT associated with the wireless provider. The test was repeated by connecting to multiple mail servers including Golden Frog's corporate mail servers. These were SMTP connections USING the Cricket/AIO network as a network provider to reach a remote, unaffiliated with AIO mail server.

Golden Frog Co-CTO Philip Molter presented the STARTTLS findings in a lightning talk at the Texas LinuxFest in Austin, TX a couple weeks later. We tested again in July 2014 when we filed our comments with the FCC, and found the same results. We included the screenshots of those test results, which are in our FCC filing.

After the TechDirt article came out, we anticipated we'd get some questions so we ran the same testing and found that STARTTLS is not currently being intercepted and blocked. We are unsure what changed.

We also tested on AT&T's network and found the encryption is not being blocked. Good.

However, this is a clear indication of what wireless ISPs can do under the claim of reasonable network management. Although it has apparently now reversed course, this particular ISP was putting its customers at serious risk by inhibiting their ability to protect online communications. We included it in our filing because as long as the FCC refuses to return to its prior “open access” policies and enable wide competition then it must establish effective rules to prevent both wireless and wireline ISPs from throttling and blocking users’ Internet traffic and preventing them from using encryption to protect their privacy. We also need more competition between ISPs so if an ISP blocks encryption citizens can “fire their ISP” and choose an ISP that doesn’t block encryption or intentionally slows down content providers such as Netflix.

We ask: Is it reasonable to invade privacy by deactivating encryption to block outgoing spam?

Neither the old or the new proposed Internet rules being debated by the FCC would stop wireless providers from blocking encryption technologies. That is very frustrating and one of the key points in our FCC filing. The FCC is a government organization and tasked with protecting national security when it comes to electronic communications. They are part of the same government that surveils its citizens. It’s not unreasonable to think they are getting pressure to curtail encryption.

Furthermore, ISPs have incentive to block privacy technologies like VPNs. They want to profit as much as possible from the way you use the Internet. Privacy services that are independent of their offerings don’t allow them to do that. If they aren’t selling the service to you, they aren’t making money and that frustrates them. However, when they are blocking privacy services, they are dangerously putting businesses’ confidential communications and individual customers’ privacy at risk.

We strongly believe that the same Open Access rules that should apply to wired Internet providers should also apply to mobile Internet providers, especially considering this specific encryption-related incident that affects online privacy.

0 Comments

Submit a Comment

Name (required)

Email (required)

Your Comment

Submit

Products | Blog | Dump Truck Web App | Control Panel

Share 0

November 6, 2014

Hey Verizon, We agree with you.

In July 2014, Golden Frog filed comments to the FCC in support of Open Access. We included some specific examples:

1. A VyprVPN customer told us he gets better Internet performance with VyprVPN than though his Internet Access Provider (in this case Verizon FIOS).
2. A wireless ISP was blocking a Golden Frog employee's ability to encrypt his communications with his third-party email server. We noted that neither the prior or proposed FCC rules prevent "wired" and "wireless" broadband Internet Access Providers from blocking encryption technologies if they desire.

The strong support our filing received from public advocacy groups and the press' interest in how our product can help alleviate Internet traffic congestion has caused Verizon to respond to our comments.

Surprisingly, we agree with much of what Verizon says.

We never accused Verizon of blocking encryption. As the Washington Post noted, Cricket is the wireless provider that was blocking encryption technologies. However, our point to the FCC is that Verizon (or any other Internet Access Provider) are free to block encryption technologies if they want, and Cricket did so for a while. Encryption inhibits the ISPs abilities to inspect and shape traffic, insert ads and sell additional services. Given their track record, we don't trust the Internet Access Providers and without clear rules at least some will be unable to resist the urge to block or interfere with technologies that inhibit their ability to make money, even if it hurts their customers' privacy.

Customers have noticed better Netflix performance by using our VyprVPN service. One reason is that Golden Frog manages its traffic so it goes to Internet Access Providers over uncongested links. This dramatically improves performance. Verizon agrees that is what is going on here. We won't speculate on how Netflix and others manage their deals with Verizon, but we have been able to provide excellent performance without having to pay Verizon like Netflix did. **We actively manage our network and take it as a compliment that Verizon validated what we do is working**. Congestion is a problem the FCC should fix, but until it does we are providing a workaround for ISPs' tactics.

Verizon's response spoke to "congestion" on the Internet-facing side, but it conspicuously failed to address several other points we made about Verizon's practices on the "user-facing" side. For example, Verizon did not deny that it inspects unencrypted traffic that comes from or goes to its users. Nowhere does Verizon deny that it looks at the content of its own users' Internet communications when it can. Verizon did not deny that it sometimes uses its knowledge of the content for its own advantage or discloses it to others, including the government. Nor did Verizon deny that it performs application identification and then unilaterally applies "special treatment" to some applications – either slowing or assigning priority using as-yet unknown criteria – on unencrypted traffic.

Golden Frog's mission is to provide tools that protect online privacy and provide a truly open Internet around the world. However, VyprVPN has another benefit – it defeats ISP throttling and congestion by application identification and "special treatment." VyprVPN, in effect, becomes the customer's virtual ISP and allows users to benefit from VyprVPN's encrypted connection by boosting their speeds. VyprVPN frustrates the Internet Access Providers' efforts on both the "Internet facing side" and "user-facing side," and simultaneously protects user privacy. **The FCC must act to protect users' continued ability to**

employ options like VyprVPN. If reasonable rules are not put in place Internet Access Providers will expand their monitoring, throttling and blocking and they soon may proceed to prevent users from defending their privacy using encryption tools like VyprVPN.

We strongly urge the FCC to put enforceable rules in place to prevent Internet Access Providers from being able to block VPNs, proxies and other encryption technologies. If the FCC imposes no effective rules against it and the ISPs get their way, poor Netflix performance may be the problem of today, but loss of tools to protect online privacy and security will become tomorrow's problem.

0 Comments

Submit a Comment

Name (required)

Email (required)

Your Comment

Submit

Insider Shop | Insight Community | Step2 | Search Techdirt | Search

NETNEUTRALITY

Techdirt Wireless News Innovation Case Studies Startups Net Neutrality Preferences Register Sign In

Main Submit a Story RSS

<< How Australia's New 'Anti-Terror' Censorship... NSA Finally Releases Keith Alexander's... >>
<< President Obama Makes Vague Meaningless... FCC Used Title II To Fine AT&T For SMS... >>

Revealed: ISPs Already Violating Net Neutrality To Block Encryption And Make Everyone Less Safe Online

from the *scary-news* dept

(Mis)Uses of Technology
by Mike Masnick
Mon, Oct 13th 2014
10:38am

0

Filed Under:
encryption, fcc, net neutrality, open internet, privacy, security, vpns, vypervpn
Companies:
golden frog

Permalink.

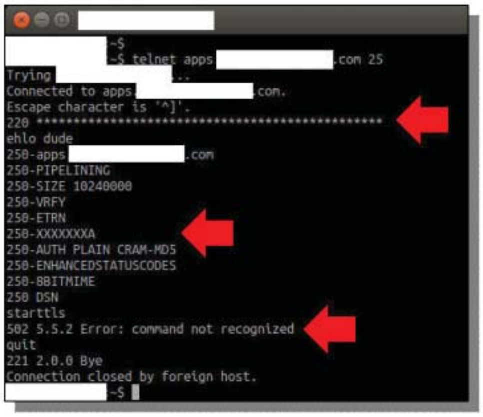
One of the most frequent refrains from the big broadband players and their friends who are fighting against net neutrality rules is that there's no evidence that ISPs have been abusing a lack of net neutrality rules in the past, so why would they start now? That does **ignore** multiple instances of violations in the past, but in combing through the comments submitted to the FCC concerning net neutrality, we came across one very interesting one that actually makes some rather stunning revelations about the ways in which ISPs are **currently** violating net neutrality/open internet principles in a way designed to **block encryption** and thus make everyone a lot less secure. The **filing comes from VPN company Golden Frog** and discusses "two recent examples that show that users are **not** receiving the open, neutral, and uninterrupted service to which the Commission says they are entitled."

The first example you may have actually heard about. It got some attention back in July, when entrepreneur Colin Nederkoorn **released a video** showing how Verizon was throttling his Netflix connection, which was made obvious when he logged into a VPN and suddenly his Netflix wasn't stuttering and the throughput was much higher. That video got a lot of attention (over half a million views) and highlighted the nature of the interconnection fight in which Verizon is **purposely allowing Netflix streams** coming via Level 3 to clog. As most people recognize, in a normal scenario, using a VPN should actually slow down your connection somewhat thanks to the additional encryption. However, the fact that it massively sped up the Netflix connection shows just how much is being throttled when Verizon knows it's Netflix traffic. Nederkoorn actually was using Golden Frog's VyprVPN in that video, so it actually makes Golden Frog look good -- but the company notes that it really shows one way in which "internet access providers are 'mismanaging' their networks to their own users' detriment."

But the second example Golden Frog provides is much scarier and much more pernicious, and it has received almost no attention.

> *In the second instance, Golden Frog shows that a wireless broadband Internet access provider is interfering with its users' ability to encrypt their SMTP email traffic. This broadband provider is overwriting the content of users' communications and actively blocking STARTTLS encryption. This is a man-in-the-middle attack that prevents customers from using the applications of their choosing and directly prevents users from protecting their privacy.*

They demonstrate this with the following graphic:



```
[redacted]
[redacted]-$
[redacted]-$ telnet apps[redacted].com 25
Trying [redacted]...
Connected to apps[redacted].com.
Escape character is '^]'.
220 ****************************************************
ehlo dude
250-apps[redacted].com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-XXXXXXXA
250-AUTH PLAIN CRAM-MD5
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
starttls
502 5.5.2 Error: command not recognized
quit
221 2.0.0 Bye
Connection closed by foreign host.
[redacted]-$
```

This is *scary*. If ISPs are actively trying to block the use of encryption, it shows how they might seek to block the use of VPNs and other important security protection measures, leaving all of us less safe. Golden Frog provides more details of what's happening in this case:

Follow Techdirt

Essential Reading

Hot Topics

- 5.7 Lena Dunham Once Again Threatens Lawsuit Over An Interpretation Of Her Book That She Doesn't Like
- 5.6 Former NSA Lawyer Says Reason Blackberry Failed Was 'Too Much Encryption' Warns Google/Apple Not To Make Same Mistake
- 5.6 Guy Accused Of Operating Silk Road 2.0 Arrested In SF... Just Like The Last One

New To Techdirt?

Explore some core concepts:

Advertising Is Content; Content Is Advertising

How Being More Open, Human And Awesome Can Save Anyone Worried About Making Money In Entertainment

Infinity Is Your Friend In Economics

read all »

Techdirt Insider Chat

> *Golden Frog performed tests using one mobile wireless company's data service, by manually typing the SMTP commands and requests, and monitoring the responses from the email server in issue. It appears that this particular mobile wireless provider is intercepting the server's banner message and modifying it in-transit from something like "220 [servername] ESMTP Postfix" to "200 ********************." The mobile wireless provider is further modifying the server's response to a client command that lists the extended features supported by the server. The mobile wireless provider modifies the server's "250-STARTTLS" response (which informs the client of the server's capacity to enable encryption). The Internet access provider changes it to "250-XXXXXXXA." Since the client does not receive the proper acknowledgement that STARTTLS is supported by the server, it does not attempt to turn on encryption. If the client nonetheless attempts to use the STARTTLS command, the mobile wireless provider intercepts the client's commands to the server and changes it too. When it detects the STARTTLS command being sent from the client to the server, the mobile wireless provider modifies the command to "XXXXXXXX." The server does not understand this command and therefore sends an error message to the client.*

As Golden Frog points out, this is "conceptually similar" to the way in which Comcast was throttling BitTorrent back in 2007 via packet reset headers, which kicked off much of the last round of net neutrality concerns. The differences here are that this isn't about blocking BitTorrent, but *encryption*, and it's a mobile internet access provider, rather than a wired one. This last point is important, since even the last net neutrality rules **did not apply** to wireless broadband, and the FCC is still debating if it should apply any new rules to wireless.

After reading the Golden Frog filing, the answer should be that it is *absolutely necessary* to apply the rules to wireless, because practices like these put us all at risk by *undermining the encryption that keeps us all safe*. As Golden Frog notes:

> *Absent enforceable Commission rules, broadband providers can (and at least one already does) block and discriminate against entirely acceptable Internet uses.* ***In this case, users are not just losing their right to use the applications and services of their choosing, but also their privacy****. It is not at clear that this type of encryption blocking would be forbidden for fixed broadband Internet access, under the proposed rules' exception for reasonable network management. This example involves mobile wireless broadband, however, and it is clear that the proposed rules would* not prohibit the activity. STARTLLS encryption does not constitute "a lawful website" or "an application[] that compete[s] with the provider's voice or video telephony services[.]"11 The proposed rules on their face do not prohibit mobile broadband Internet access providers from blocking user efforts to maintain privacy through encryption.

Furthermore, Golden Frog concludes:

> *The claim that rules banning blocking and unreasonable discrimination are solutions in search of a problem is flatly wrong. There have been problems in the past and there are problems now. The proposed rules do not resolve all of the problems identified in the NPRM. Further broadband Internet access providers are still interfering with beneficial and privacy-enhancing applications users want to employ.*

This is incredibly important -- just at a time when we need stronger encryption and privacy online, the FCC may undermine it with weak net neutrality rules that allow this type of behavior to continue.

A few months ago, I got into a conversation with a well-known internet entrepreneur/investor, who asked about possible "compromise" rules on net neutrality, suggesting that maybe it's okay to throttle Netflix traffic because there's *so much* of it. He argued that, perhaps there could be some threshold, and if your traffic was above that threshold it's okay to throttle it. After some back and forth, I asked the hypothetical about encryption: what if, at a time when more and more encryption is important, such a rule was in place, and overall encrypted traffic passed that threshold, then suddenly access providers could throttle all encrypted traffic, doing tremendous damage to security and privacy. What I didn't realize was that some access providers are effectively already attacking privacy and encryption in this manner.

To print the document, click the "Original Document" link to open the original PDF. At this time it is not possible to print the document with annotations.

Recent Stories

Thursday

10:41 Verizon Now Pleads For Bogus Net Neutrality Rules Under 706 Promising It Won't Sue This Time, Ignoring That Others Will Sue (5)

Friday

09:34 FCC Tests The Waters On A 'Hybrid' Net Neutrality Solution That Almost Everyone Hates (21)

Thursday

12:52 Verizon: 'Title II Is Not The Answer... Except When It Gives Us Massive Subsidies, Then It's Totally The Answer' (22)

10:28 Both Comcast And Verizon Agree To Pay Millions To Settle Overbilling Claims (29)

Wednesday

13:41 Cricket Revealed As Mobile ISP That Was Blocking Encrypted Emails (21)

10:33 Detailed Report Shows How ISPs Are Making 'Business Choice' To Make Your Internet Connection Terrible (31)

06:18 Verizon Launches Tech News Blog... That Bans Any Articles About Net Neutrality Or Government Surveillance (33)

Tuesday

13:38 FTC Sues AT&T For Selling 'Unlimited' Data Plans That Were Actually Throttled (18)

Monday

12:16 Payment Wars: How Merchants And Carriers Are Trying To Block Payment Systems They Can't Track (79)

Tuesday

13:45 FCC Used Title II To Fine AT&T For SMS Cramming And The World Didn't End: Why Would It For Broadband? (11)

More ➔

The Switch

Mobile ISP Cricket was thwarting encrypted emails, researchers find

By Nancy Scola and Ashkan Soltani October 28
Follow @nancyscola

(Courtesy Cricket Wireless)

Some customers of popular prepaid-mobile company Cricket were unable to send or receive encrypted e-mails for many months, according to security researchers, raising concerns that consumers may find that protecting their privacy is not always in their hands.

The inability to send some encrypted messages on Cricket's network was discovered by software engineers from the digital security and privacy firm Golden Frog. The company mentioned the issue in a July filing to the Federal Communications Commission, and the tech publication Techdirt published an article on it earlier this month. But neither Golden Frog's filing nor Techdirt named the mobile Internet service provider.

Golden Frog told The Washington Post that Cricket customers were unable to send encrypted messages and said its testing found that the problem ended shortly after the TechDirt article was published. It is unclear how long or how many customers were affected.

Cricket did not address repeated questions about the issue and did not alert customers, many of whom rely on Cricket as their sole Internet service, that they would not be able to protect their e-mails from prying eyes. AT&T, which absorbed Cricket when it acquired Leap Wireless last spring, did not respond to a request for comment.

Cricket said in a statement to The Post that it "is continuing to investigate the issue but does not intentionally prevent customers from sending encrypted emails."

Digital encryption allows computers — in this case, the mail servers that send and receive e-mails — to speak to each other in code. The service has been under a spotlight lately as consumers have become concerned about protecting the tremendous amount of information they send across digital networks. Encrypted e-mails were, for example, how NSA contractor Edward Snowden first communicated with journalists about the intelligence community's bulk data collection.

In simple terms, encrypting an e-mail typically works like this: User X's mail server asks User Y's mail server if it is willing to receive an encrypted, or coded, e-mail. If the server says, "yes," the encrypted version of the e-mail is sent. If the server says, "no," an unencrypted version is sent instead.

But Golden Frog says that in Cricket's case, when the sending e-mail server asked if it might transmit an encrypted e-mail, the network simply scrubbed the request before the receiving mail server had a chance to hear it.

"The server on the other end doesn't realize that it was asked to speak privately. So it doesn't speak privately," said Andrew Appel, chair of the computer science department at Princeton University.

Golden Frog, which sells privacy-focused software that includes an encrypted messaging service, said it discovered the problem because one of its software engineers living in rural Texas relied on Cricket's mobile Internet service. The engineer had configured his e-mail program to allow his e-mails to be sent only if encrypted.

When the company noticed that it was not receiving the employee's e-mails, it began looking into why. Golden Frog found that its engineer was trying to send e-mails through a virtual doorway known as Port 25. That portal has been used to send e-mails for years, but some Internet service providers recently began blocking it because they were concerned that it was dominated by spammers. Still, the system is popular among some tech experts, who use it to operate their own mail servers.

Cricket allowed customers to send and receive e-mails through Port 25 software, according to Golden Frog, but stripped the traffic of the encryption request, known as STARTTLS.

It is unclear whether the lack of encryption was limited to this system or how many Cricket customers were affected.

In its FCC filing, Golden Frog said it was concerned that Cricket's practices violated the spirit of net neutrality, or the idea that Internet service providers should allow Internet traffic to move freely across their networks.

"Any time an Internet service provider is interfering with a user's ability to protect their privacy it's very concerning to us, and to all Internet users," said Sunday Yokubaitis, Golden Frog's president. "If ISPs can force users' choices about encryption, where does that put us?"

Despite law enforcement complaints, consumers are relying more on digital encryption. Apple and Google recently moved to encrypt by default more of the services built into the iOS and Android operating systems. Those moves, the FBI has argued, will make it difficult, if not impossible, for law enforcement to do its job.

According to Google -- which has called unencrypted e-mail "as open to snoopers as a postcard in the mail" -- about half of the e-mails received through Gmail in October have been encrypted, up from about 30 percent in January.

Tom Lowenthal is the staff technologist at the Committee to Protect Journalists. "It is poor practice and obsolete to send and receive mail without using robust encryption," Lowenthal said. "Journalists who rely upon secure communications, and anyone else who doesn't want their personal messages to become public, should expect their e-mail providers to offer encrypted connections by default."

Cricket was founded in 1999, and its parent company Leap Wireless was acquired by AT&T earlier this year. (AT&T's network, according to Golden Frog, allowed the sending of encrypted e-mails.) The Golden Frog engineer first noticed the behavior in September 2013 on a network used by AT&T prepaid phone provider Aio. Cricket replaced Aio as

AT&T's pre-paid service after the acquisition was completed in March, and Golden Frog said the encryption practices continued for prepaid customers. Cricket's data plans start at $35 a month and do not require a contract.

John Levine is a senior technical adviser to the Messaging, Malware and Mobile Anti-Abuse Working Group, an organization with member companies including Apple, Google and Verizon. While it is unclear whether Cricket intentionally prevented its customers from encrypting e-mails, Levine said, "the result is exactly the same."

More and more people are taking steps to protect themselves from spying eyes, Levine said, "and if you're going to interfere with that, you need a really good reason."

Nancy Scola is a reporter who covers the intersections of technology and public policy, politics, and governance.