



TLP White

This week, Hacking Healthcare begins by providing a brief overview of how a major European law enforcement operation, made possible by cracked encryption, is likely to further fuel the long simmering encryption debate within the United States. We then wrap up by exploring the FCC's decision to formally name Chinese firms Huawei and ZTE as national security threats and how the trickle-down effects may impact healthcare. Welcome back to *Hacking Healthcare*.

1. **With Encryption Cracked, Law Enforcement Scoops Up Criminals.** A coalition of European law enforcement authorities claimed a major success last week when they arrested 746 individuals, and seized \$67 million in cash, as well as drugs and firearms.<sup>1</sup> They claim that the key to the operation was the successful cracking of encrypted messaging service EncroChat. Such a significant bust is likely to add more fuel to the contentious debate between law enforcement officials and privacy advocates over encryption and the need for purpose-built hardware and software backdoors.

According to the law enforcement authorities involved, the secure mobile phone messaging service EncroChat boasted around 60,000 users worldwide and has been a target for the U.K.'s National Crime Agency since at least 2016.<sup>2</sup> An apparent breakthrough in April allowed law enforcement authorities to install a surveillance tool to monitor communications on the platform and share them amongst each other.<sup>3</sup> Dutch authorities claimed that this allowed them read over 20 million messages and eventually coordinate the mass arrests across several countries.<sup>4</sup> No agency involved has specified exactly how they managed to crack or circumvent the platform's encryption.

#### ***Action & Analysis***

\*H-ISAC Membership Required\*

2. **FCC Declares Huawei and ZTE are National Security Threats.** On June 30<sup>th</sup>, the Federal Communications Commission ("FCC") released an announcement that formally declared Chinese technology companies Huawei and ZTE to be national security threats.<sup>5</sup> Ajit Pai, the FCC's Chairman, stressed that both companies' close relationship with the Chinese Communist Party and their obligation to laws requiring cooperation with Chinese intelligence authorities were major factors in the decision.

July 7th, 2020

Citing the need “to protect U.S. communications networks from security risks,” the announcement means that both companies and their parents, affiliates, and subsidiaries are now subject to the FCC’s ban on the use of universal service support to purchase equipment or services.<sup>6</sup> In effect, the announcement means that telecom companies cannot use money provided to them from the FCC’s \$8.3B Universal Service Fund on “equipment or services produced or provided by these suppliers.”<sup>7</sup>

Much of Huawei and ZTE’s appeal thus far has been the relative availability and affordability of their products. Cash strapped communications organizations with limited budgets for IT infrastructure may not have a suitable alternative at the ready. This issue is further compounded by the economic damage being inflicted by the COVID-19 pandemic.

Within the United States, the decision is a significant blow with terrible timing for smaller, often rural, Internet Service Providers (ISPs). The Rural Wireless Association (“RWA”), “a trade association representing rural wireless carriers who each serve fewer than 100,000 subscribers,” quickly released a statement that they were “stunned” by the decision.<sup>8,9</sup> In their statement, the RWA outlined how their members “will now lack the ability to support their critical networks that are serving hundreds of thousands of rural Americans and those traveling through rural America.”<sup>10</sup> Although waivers for this announcement are possible, there is some resentment at the lack of time given to submit them before the decision went into effect.

Congress has not been blind to the plight of smaller domestic ISPs that could be affected by such a decision. The Secure and Trusted Communications Networks Act of 2019 promised to “make reimbursements to providers of advanced communications service to replace covered communications equipment or services.”<sup>11</sup> However, FCC Commissioner Geoffrey Starks was keen to point out that as of June 30<sup>th</sup>, Congress “still has not appropriated funding for replacements.”<sup>12</sup>

### ***Action & Analysis***

\*H-ISAC Membership Required\*

## ***Congress –***

### Tuesday, July 7th:

- House – Committee on Appropriations - Subcommittee on the Departments of Labor, Health and Human Services, Education, and Related Agencies: Markup of FY 2021 Departments of Labor, Health and Human Services, Education, and Related Agencies Subcommittee Markup

### Wednesday, July 8th:

- House - Committee on Financial Services: Task Force on Artificial Intelligence: Exposure Notification and Contact Tracing: How AI Helps Localities Reopen Safely and Researchers Find a Cure

Thursday, July 9th: - No relevant hearings

July 7th, 2020

## ***International Hearings/Meetings –***

### ***EU –***

Tuesday, July 7th:

- European Parliament – Committee on Environment, Public Health, Food Safety: EU4Health Programme

## ***Conferences, Webinars, and Summits –***

--COVID-19 and its Cybersecurity Challenge – Webinar (7/9/2020)

<https://h-isac.org/hisacevents/covid-19-and-its-cybersecurity-challenge/>

-- H-ISAC Shared Solutions: Enabling Interoperable Identity Across Healthcare with SAFE Identity (TLP:GREEN) – Webinar (7/9/2020)

<https://h-isac.org/hisacevents/shared-solutions-interoperable-identity/>

--Healthcare Cybersecurity Forum - Mid-Atlantic – Virtual (7/16/2020)

[https://endeavor.swoogo.com/summer\\_virtual\\_healthcare\\_innovation\\_cybersecurity\\_forum/About](https://endeavor.swoogo.com/summer_virtual_healthcare_innovation_cybersecurity_forum/About)

--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)

[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/426499](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499)

-- H-ISAC Monthly Member Threat Briefing – Webinar (7/28/2020)

<https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-10/>

--H-ISAC Virtual Security Workshop – Virtual (7/29/2020)

<https://h-isac.org/hisacevents/nz-virtual-workshop/>

-- H-ISAC Monthly Member Threat Briefing – Webinar (8/25/2020)

<https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-11/>

--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)

[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/426517](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517)

--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020) - CANCELLED

<https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-village-co/>

--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)

[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/427126](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126)

--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)

<https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/>

--H-ISAC Security Workshop - Forchheim, Germany (9/23/2020)

<https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/>

--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)

<https://h-isac.org/hisacevents/summit-on-security-third-party-risk/>

--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)

[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/428840](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840)

--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)

<https://h-isac.org/hisacevents/cysec-2020-croatia/>

--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)

<https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/>

--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)

[https://endeavor.swoogo.com/2020\\_healthcare\\_innovation\\_cybersecurity\\_forums/428886](https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886)

--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)

<https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/>

July 7th, 2020

--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)

<https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/>

--H-ISAC Security Workshop - Paris, France (11/18/2020)

<https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/>

## ***Sundries –***

--Senators call for CMS to provide plan for telehealth changes

<https://www.healthcareitnews.com/news/senators-call-cms-provide-plan-telehealth-changes>

--CISA Stands to Gain Powers Under Both Versions of the Defense Authorization Bill

<https://www.nextgov.com/cybersecurity/2020/07/cisa-stands-gain-powers-under-both-versions-defense-authorization-bill/166630/>

--Artificial Intelligence Systems Will Need to Have Certification, CISA Official Says

<https://www.nextgov.com/cybersecurity/2020/07/artificial-intelligence-systems-will-need-have-certification-cisa-official-says/166600/>

**Contact us: follow @HealthISAC, and email at [contact@h-isac.org](mailto:contact@h-isac.org)**

---

<sup>1</sup> <https://www.cyberscoop.com/encrochat-encryption-drug-bust/>

<sup>2</sup> <https://www.zdnet.com/article/police-take-down-encrypted-criminal-chat-platform-encrochat/>

<sup>3</sup> [https://www.vice.com/en\\_us/article/3aza95/how-police-took-over-encrochat-hacked](https://www.vice.com/en_us/article/3aza95/how-police-took-over-encrochat-hacked)

<sup>4</sup> <https://www.cyberscoop.com/encrochat-encryption-drug-bust/>

<sup>5</sup> <https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf>

<sup>6</sup> <https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf>

<sup>7</sup> <https://twitter.com/AjitPaiFCC/status/1278003564162449417>

<sup>8</sup> <https://ruralwireless.org/about-rwa/>

<sup>9</sup> <https://ruralwireless.org/rwa-stunned-by-fccs-decision-to-immediately-bar-use-of-usf-funds-on-huawei-and-zte-equipment-and-services-during-a-time-when-it-is-critical-to-keep-rural-americans-connected/>

<sup>10</sup> <https://ruralwireless.org/rwa-stunned-by-fccs-decision-to-immediately-bar-use-of-usf-funds-on-huawei-and-zte-equipment-and-services-during-a-time-when-it-is-critical-to-keep-rural-americans-connected/>

<sup>11</sup> <https://www.congress.gov/bill/116th-congress/house-bill/4998/text>

<sup>12</sup> <https://docs.fcc.gov/public/attachments/DOC-365259A1.pdf>