Hot Clicks: Congressman Will Hurd's Idea of a Digital Border

Installing a fiber-optic network for surveillance technology can also help the digital divide, plus other news.

Amanda Ziadeh

Tue, 02/05/2019 - 10:37

Photo Credit: tiero/iStock

Republican Texas Rep. Will Hurd's district is along the southern border, and instead of a border wall to keep the border secure, he's interested in a digital wall — a system of cameras, sensors and drones that communicate through a fiber-optic network.

Hurd also believes this kind of solution can help with the digital divide — the inequality of access to network and technologies due to location, and in this case, rural location. The fiber-optic network, in particular, while being used to secure the

border, can also provide internet connectivity for the rural local communities along the Texas-Mexico border.

According to Hurd, in 13 out of the 29 counties he represents, less than 20 percent of people have access to broadband. Motherboard

FBI Using At-Home DNA Tests to Solve Crimes

The FBI is working with FamilyTreeDNA to solve violent crimes, and the laboratory that does the DNA tests for the company and others like it has been accepting samples from the DNA to identify suspects and human remains. The lab is helping to generate data profiles from evidence samples, so that FBI officials can upload the samples to databases and to FamilyTreeDNA and scan for matches. But in terms of what the FBI has access to, the owner of the lab, FamilyTreeDNA President Bennett Greenspan, said if law enforcement creates accounts with the same level of access as standard FamilyTreeDNA users, they're not violating user privacy. But to get any more information would require a legal order. Genetic databases and DNA testing has helped with high-profile cases like the Golden State Killer, but privacy concerns remain around DNA testing companies and law enforcement access. The Verge

Cyber Threats Didn't Rest During the Shutdown

The majority of NASA employees — nearly 95 percent of them — could not come to work during the 35-day shutdown, and according to a post-shutdown town hall Jan. 29, this threatened NASA's cybersecurity. But those working in NASA's Security Operations Center were still fighting cybersecurity threats, according to Renee Wynn, NASA's chief information officer. The SOC is housed in NASA Ames Research Center in California, and it operates every day and every hour of the year, so that NASA's networks and data are monitored and protected at all times. The SOC did research incidents during the shutdown and reported that, on average, the agency faced about one cybersecurity threat a day (this includes a NASA employee losing a phone). But because the SOC doesn't take a break, cybersecurity during the shutdown was, in the most part, in full swing. Space.com

Google’s Live Transcribe App Helps Deaf Community

Google’s Live Transcribe and Sound Amplifier apps, both released this week, provide great benefits to more than five percent of the world's population identified as deaf or hard of hearing. Live Transcribe uses Google’s speech-to-text intelligence feature to give written text representations of spoken words in near real time, as the conversation is happening. Sound Amplifier uses dynamic audio processing, an Android feature, to make sounds easier to hear. With this app, users can adjust volume, ambient noise, voice clarity and sound distribution from left to right ears. And with the transcribe app, users are able to read on their phone screens a transcription of the conversation they’re having. Some words aren’t always accurately transcribed depending on factors like accent, but it can pick up on certain words depending on context (chili versus chilly). Wired

Doorbell Cameras Spark Privacy Concerns

Home surveillance cameras are on the rise, with Ring video doorbells, Nest and other easily installed popular gadgets providing alerts and streaming capabilities right to a homeowner’s phone. But privacy, and the policy and rules around filming, are still in question. It is legal to film in public places and entryways, but there’s a debate about whether the cameras actually reduce crime. Law enforcement are also creating voluntary registries for private cameras in communities: Washington, D.C. pays up to $500 for cameras on private property, and Detroit’s mayor wants security cameras at businesses to provide a live feed to the police. Amazon is looking to add its Rekognition facial-identification software into its Ring doorbell cameras to automatically flag “suspicious” people, causing even more potential bias and privacy concerns. But all this tech can be hacked and the data re-routed, and it’s creating a “Big Doorbell” rendition of the “Big Brother” concept to worry about. The Washington Post

View printer friendly version
news roundup
Will Hurd
FBI
Amazon

Google
Federal Cybersecurity