



July 2026

## Summertime Roundup

*By Mark Costlow*

As we settle in to the high desert rhythm of punishingly hot days, often relieved by brief but intense downpours in the afternoon, we've been thinking about previous topics we have covered here. This month we'll give some updates on the Vera Rubin telescope, how most consumer routers are being made illegal, some new and tragic news about a self-driving car, and Internet of Things (IoT) abandonments.

### Vera Rubin Delivering on Promises

A year ago the [Vera Rubin telescope](#) in Chile completed construction and began taking pictures with the largest camera ever built. They have been running the telescope through its paces for the past year, leading up to starting the [Legacy Survey of Space and Time \(LSST\)](#).

For the next 10 years the Rubin will make a complete pass of the southern sky every 3 nights, recording a panoramic high-definition time-lapse of our universe. This will give scientists a recording of the changes in nearby and distant reaches of space over a long time period, complete with real-time alerts to call attention to changes as they happen.

The [LSST's goals](#) are to increase understanding of dark matter and dark energy, inventory the Solar System, and watch for objects that move or change brightness. Before starting the LSST, Rubin has already discovered [11,000 new asteroids](#) and the fastest-spinning asteroid ever found, and promises many more discoveries are to come.

At a smaller scale, a revolution in astrophotography has been quietly taking place in back yards and gardens around the world. New ["smart telescopes"](#) that cost well under \$1,000 are bringing deep space within reach of almost anyone interested. They are not optical telescopes in the traditional sense, but rather digital cameras with high magnification, paired with motors to automatically track the movement of the stars, and software to optimize image collection.

There are [debates](#) about whether smart telescopes are for "real astronomy". Most people agree that anything that helps us explore the natural world must qualify. Popular models like the [ZWO](#)

[SeeStar S30](#) and [Dwarflabs Dwarf 3](#) enable someone with no prior telescope experience to capture stunning images of the sun, moon, planets, stars, and galaxies within an hour of opening the box.

Smart telescopes use [image stacking](#) to get high-quality images that would otherwise require large and expensive equipment. They shoot dozens or hundreds of pictures of an object and combine them to produce a high-definition view that is impossible to get with a single snap. In many cases the stacking and post-processing can be done in the telescope itself, so there is less need for elaborate post-processing workflows on a computer (although you can still do that if you want).

### Consumer Router Bans

The US Government took further steps to ban networking equipment manufactured outside the US. In March, the [FCC banned new consumer internet routers](#), citing national security concerns.

As has become increasingly common, the ban came very quickly, without a lot of explanation, so details and adjustments have developed in the weeks that followed. [In the FCC fact sheet](#), they explain that "Foreign-made routers were also involved in the Volt, Flax, and [Salt Typhoon](#) cyberattacks targeting vital US infrastructure".

[Salt Typhoon](#) and others are widely [believed to be hacking initiatives backed by the Chinese government](#), with the aims of both spying and disrupting infrastructure (the power grid, water supply, transportation).

It is true that consumer routers are frequently compromised and used in large-scale botnets, and could be especially useful to create large-scale Internet disruptions. But these attackers primarily target enterprise routing hardware, like Cisco, Sophos, and Fortinet. It has infiltrated [at least 9 of the largest US telecom companies](#), including AT&T, Verizon, and Century Link (Lumen). AT&T and Verizon have variously reported to have expelled Salt Typhoon from their networks, but [refused to provide any reports to congress](#) to confirm it.

All that is to say, it's unclear how removing most of the consumer routers from Best Buy's shelves will protect the enterprise networks that are most at risk. It's also very hard to tell what devices are truly banned. After the initial rushed ban announcement, it has emerged that [manufacturers can apply for waivers](#) to escape the "covered list", so some foreign routers will be allowed and some not. The FCC says consumers who own existing routers (presumably the ones with security problems) don't need to do anything, they just can't buy new ones (which, ironically, might have fixed the security problems).

Our global economy and interlinked supply chains ensure that ALL routers are foreign-made at one level or another. Also, many of the Salt Ty-

phoon entry points have been traced back to using default passwords on routers deployed at the core of our public and private networks. The FCC action very much feels like we are floundering in the face of the extraordinary complexity of cyber-warfare, and this is the result of the extremely human urge to "DO SOMETHING", even if the something is not that useful.

## Self Driving Deathtrap

Just a few days after reporting here that robotaxis and other self-driving cars are poised to flood our streets, there was a news of [Waymo robotaxis causing gridlock in San Francisco](#), and a serious incident involving a self-driving Tesla in Texas.

On June 19th, a 44 year old driver in a residential neighborhood in Katy, TX, accelerated his Tesla Model 3 to 73 MPH in a cul-de-sac, [crashed into a brick house, and killed one of the residents](#). He was charged with manslaughter on July 1, and the charging document brings several interesting facts to light.

Since the Full Self Driving (FSD) function was engaged at the time of the crash, initial speculation around the case was that the Tesla had incorrectly accelerated out of control. However, telemetry from the car showed that the driver had overridden FSD by pressing the accelerator and never hit the brake. Many cases of "[Sudden Unattended Acceleration](#)" have been shown to be driver error, hitting the accelerator when they are trying to hit the brake in a panic, and it sounds like this may be what happened here.

The [driver has been charged with manslaughter](#), and the charging document further states that the driver recently Googled the search terms "FSD is not aggressive enough for city driving," and "Tesla fsd too timid." Immediately before the crash, the driver went through a stop sign and pressed the accelerator to override FSD's default behavior to come to a full stop. In that case, FSD allows the acceleration but keeps control of steering.

It seems that the human in the system created the problem in this case. But there are still questions about why FSD didn't take stronger action as the car approached a brick wall. But if we have decided the human is best equipped to make these decisions, those overrides will remain in place. It will be interesting to see how Tesla Robotaxis, which have no steering wheels or pedals with which to override, will fare.

## Platform Decay

[Cory Doctorow](#) wrote about the phenomenon of platform decay in 2022:

*Here is how platforms die: first, they are good to their users; then they abuse their users to make things better for their business customers; finally, they abuse those business customers*

*to claw back all the value for themselves. Then, they die. I call this [enshittification](#) [...]*

The examples that follow here involve platforms in some stage of decay. Internet of Things (IoT) devices are particularly vulnerable to this cycle because so many people are lured into a relationship with a platform they didn't approve or understand. In fact it may not have occurred to them that it even existed. They bought a product to serve a purpose, as they would a hammer, a dinner plate, or a DVD. Who would think that the hammer might start charging a monthly fee for use, or the plate might begin to display ads for meds or snacks, and the DVD could literally vanish into thin air, never to be seen again?

This list is presented without comment. In the PDF version of the newsletter, each item is a link to more information.

- [Samsung fridges with displays started showing ads](#) after a software update.
- Some [Jeeps are showing pop-up ads](#) for an extended warranty, *every time the vehicle stops*.
- The Hestan Cue bluetooth connected pan with app control [has lost its app](#), and is now a disconnected "dumb" pan.
- [Logitech has bricked its line of "Pop" smart buttons](#) and switches for controlling lights and appliances.
- [Bose SoundTouch home theater systems have lost their app](#) and all their smarts. The multi-room features (their reason to exist) no longer works.

We'll close things out with Jeep again. In October, a buggy software update on a Friday [bricked Jeep 4xe hybrids all over the country](#). They had to be towed to a dealer and fixed after Monday. Worse, the failure didn't happen immediately, but after the truck was driven a while. For some, that meant on the highway 50+ miles from home. Perhaps those owners would be interested in an extended warranty?

## This Month in Ideas & Coffee

- **July 21 6pm-7:30pm** - *WordPress Work Along* - Answers to your pressing WordPress questions. Bring your laptop!

Watch the [Ideas & Coffee](#) event calendar at <https://swcp.com/calendar> for future info.

---

**Southwest Cyberport - swcp.com**

New Mexico's Expert Internet Service Provider since 1994

**505-232-7992 | Support: [help@swcp.com](mailto:help@swcp.com)**

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

**Click on bold blue type in browser for links.**