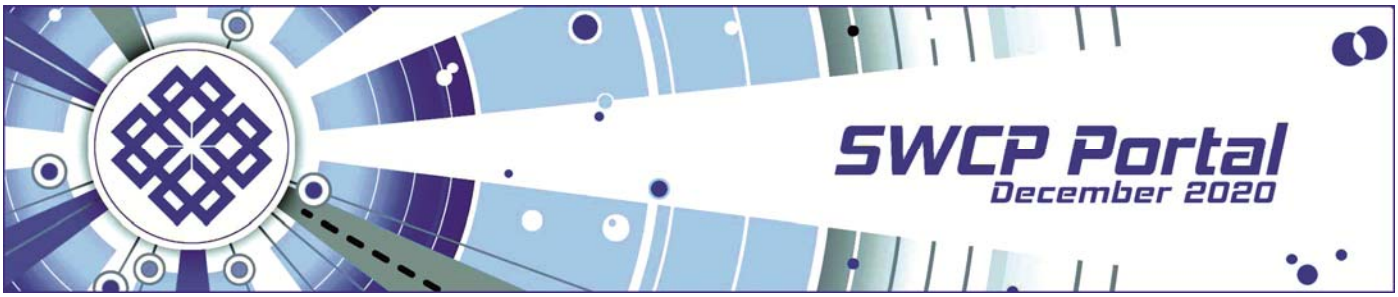

Winter is here, covid and craziness linger, but life goes on

Meanwhile…

While the pandemic, the presidential election, and Thanksgiving have monopolized everybody's attention recently, not much else seems to have been going on. Everything else on the planet appears to have been put on hold or set aside at least until the politics and the holiday were done.

But the world has certainly not stopped in the meantime. Developments in many areas have proceeded quietly behind the scenes. New and forgotten issues are rising to the forefront again. So this time, the *Portal* will look at some of the things many people might have overlooked.

Facebook, *nyet*

It appears that social media may finally get moderated due to **Russian interference** in 2016. But surprisingly, it's the *Russians* themselves who may block Facebook, Twitter, and YouTube.

Ironically, they object to their propaganda outlets such as RT being "discriminated" against by the platforms. Labeling state-affiliated profiles, the sites reduced Russian media's overall visibility by removing their content from the basic algorithms, angering the Kremlin (**zd.net/3qasWXy**).

Russia has already banned LinkedIn since 2015 for storing data about Russian citizens outside their country. Recently, Russia has also opened an administrative case against Google for failing to remove *30%* of banned content. This is the second time Google has been so penalized. Unlike the EU, which has fined them massive amounts for unfair competition and lack of data protection, this seems more like an attempt to pressure Western cooperation with Russian propaganda efforts.

It is all part of the ongoing fracturing of the worldwide internet into regional and national "**splinternets**". Competition for first-place is largely determined by the amount of cross-border traffic, and by that measure the US is already losing (**s.nikkei.com/3mjexpp**). Back in 2001, the US dominated the world in net traffic. Now, however, China has become the leading data superpower, siphoning off *23%* of international traffic while the United States has dropped to a mere *12%*.

Since **data** is the invaluable resource that fuels development and competitiveness, this may mean the US is losing its edge in AI and information technologies. Plus, such struggles to control data harms vital international cooperation to fight the coronavirus, global warming, and other problems.

Too many satellites

SpaceX and other companies have been busy shooting hundreds of tiny satellites into low Earth orbit to provide internet access here below but resistance is finally coming from more than just irate star-gazers. **NASA** has commented against a proposal to the FCC by AST & Science, a Texas telecommunications firm. It wants to put 240 large satellites into orbit for 5G connections on Earth, like 450-mile tall cell phone towers.

Not only are these satellites very big with huge antennas, they would be stationed near altitudes already occupied by constellations of critical Earth-monitoring probes (**bit.ly/2TUSuZC**).

Avoiding orbital crashes is a fast-growing headache. In October, a dead Soviet satellite and a Chinese booster barely missed each other. The nightmare possibility is of a "**Kessler syndrome**" event (**bit.ly/3oR1XiS**) where chains of crashes in overcrowded low Earth orbits could lead to so much dangerous debris being produced that space travel would become all but impossible.

Emailing Mars

Assuming outer space remains reachable, then future explorers will surely need internet access. Astronauts aboard the Space Station can email and surf the web, but there hasn't been a great need for a truly deep-space internet, though it has been talked about and tinkered with since 1998.

Returning to the Moon and then onto Mars will certainly change that. So it is a good thing that **Vint Cerf**, the man who helped invent email and

the net, is working on the interplanetary internet. The main difference is that this system will need a high tolerance for really, *really* long delays. This is done by a new set of net "bundling" protocols that replace good old TCP/IP (**bit.ly/3mYZZvj**) by including memory in the connection nodes.

It's being tested on the Space Station right now, remotely running a small rover in Germany. But the interplanetary net has been actually used since 2004, when JPL reprogrammed several Mars orbiters and rovers to intercommunicate much more rapidly, and now with cometary probes also.

Deepfakes come home

Security experts held their breath this election season for fear of disruptive **deepfake** videos (**bit.ly/3eod7Ha**). These are AI-generated hoaxes based on real footage where a person's voice and facial features have been replaced. A security industry has quickly grown up looking for ways to instantly and accurately detect and defeat them.

Fortunately, deepfakes were not used this time around, possibly because there was enough chaos already. Instead, they have been busy **removing clothes** from real, ordinary women online.

Celebrities were the first targets, not just because of fame but for the huge number of available images previously needed for deepfakes. But recently an app (since removed) was found on the encrypted messaging platform Telegram, used to create nude or explicit images of **thousands** of unsuspecting women (**bit.ly/3eqUx12**).

Worse, this app needed just a single picture to create the hoax. It might be even easier to do on platforms like Instagram or TikTok, which are video-based – and have many underage posters.

Eventually, these novel kinds of abuses may be classified as a new type of crime, "**digital rape**". Until then, the law has a lot of catching up to do.

Dangers of IoT sex toys

Recently, a serious security flaw was revealed in the **Cellmate Chastity Cage**, a kinky device to ensure male sexual continence (**bit.ly/3exLbk7**). Apparently, hackers can easily remotely take over and could lock users in permanently, as there is no physical key or override. The only options involve cutting, grinding, or applying an electric shock.

This isn't the only adult toy with such flaws, some even more disturbing. With the holidays coming up, users are warned once again of the many dangers of poorly-secured Internet of Things gizmos. The holidays have never been so weird.

Amazon: Christmas elf or Grinch?

The online superstore has become essential during the pandemic and it expects to sell over *$100 billion* worth of goods during the last quarter of 2020. As Santa's warehouse and delivery system, this year Jeff Bezos is giving *$500 million* in bonuses to his hard-working staff with full-time workers getting *$300* and part-timers *$150*, but that's less than Amazon makes in a *single day*.

A **worldwide boycott** of Amazon over Black Friday was planned to protest the company's unchecked growth. Unsafe practices and low living wages for its workers, spying on their efforts to organize labor, unfair business practices targeting stores selling through the site, tax avoidance, and huge environmental impacts have all come under strong international criticism (**bit.ly/33zSRhG**).

Yet despite recent regulatory disapproval of its tracking customers' purchasing data to put third-party vendors at a disadvantage, the everything store just launched a "**Shopper Panel**" program where they will pay users *$10 a month* in credit to upload receipts from certain outside retailers.

Even **creepier initiatives** have to do with its voice assistants and home security devices. Long suspected of secretly spying on customers, soon, under its new "**Sidewalk**" program, Amazon Ring doorbells, lights and Echo gizmos will all be able to connect to the net by means of an ad hoc mesh system that will use whatever Wifi is handy – your own or your neighbors' (**bit.ly/33EbH77**).

Users will get to choose when setting up the devices. While touted as a means of finding lost pets and porch pirates, Amazon has a history of pressuring homeowners into turning their Ring devices into surveillance tools for the police.

Stay safe with the internet

2020 has been a tough, strange year, but covid remains. Distance, mask up, and use the net where possible. You can do many things for yourself, including paying your SWCP bill through our **Members Portal** on our website. Email or call us if you need help with the net. Happy Holidays!