BCAP NewsClips

September 5, 2019

Philadelphia Inquirer
'I felt nauseous,' Bucks County woman says of plan for 48-foot 5G cell tower in her front yard

Washington Post
YouTube settlement raises questions about Washington's ability to rein in Silicon Valley

Remember the days before robocalls? When your landline and cell phone were free from scam artists selling something, threatening you with arrest, wheedling to extract a credit-card number?

Nah, we can't either. The number of unwanted calls in the U.S. is measured in the tens of billions each year. The Federal Communications Commission, citing private analyses, says American consumers were hit with almost 4 billion robocalls a month in 2018. Still, there is cause for skeptical optimism on this front, even though the odds seemed perpetually stacked in favor of scammers who've perfected the art of the auto-dial.

In July the U.S. House of Representatives adopted the Stop Bad Robocalls Act, which would require telecom companies to step up enforcement and give consumers more ways to insulate themselves. The bill, sponsored by Rep. Frank Pallone, D-N.J., coasted through on a 429-3 vote. It's now before the Senate.

A week ago a group of state attorneys general — including Josh Shapiro of Pennsylvania and Gurbir Grewal of New Jersey — announced an agreement they'd reached with the 12 largest phone service providers. The

TV Answerman
DirecTV to Show Notre Dame Football In 4K HDR

Fierce Video
Verizon taps Altice USA for local news after shutting down Fios News

Bloomberg
NFL Kicks Off With Preview of Verizon 5G Service in 13 Stadiums

New York Times
No, Netflix Is Not Abandoning Its Binge Format

Philadelphia Inquirer
Fired top FBI official Andrew McCabe to headline Pa. Democrats' fund-raiser

Philadelphia Inquirer
The legal team in the Pa. gerrymandering case set their sights on N.C. They just won again.

companies, including Verizon, Comcast, T-Mobile and AT&T, signed on to offer free call-blocking services to customers. They agreed to keep a closer watch on robocalls and help authorities identify and track phone scammers.

The Federal Trade Commission is stepping up enforcement. Working with federal, state and local investigators, the FTC recently announced charges against three firms and one individual believed to be responsible for more than 1 billion illegal spam calls. While this qualifies as a start, there's more to be done. Not all robocalls and phone solicitations are illegal, but the system has been gamed by those who have mastered easy-to-use technology, often operating from safe havens overseas.

The best hope rests with the industry — with government oversight to check on compliance. Several companies have taken steps to install an anti-"spoofing" technology called STIR/SHAKEN, which allows consumers with caller ID to know if an incoming calls is bona fide or a spammer using a local or familiar number. And there are call-blocking apps that can be downloaded, some for free.

State and federal "Do Not Call" registries are still accepting numbers and trying to help, but we know from experience they don't provide anything close to a firewall. People can still report robocalls to the feds at **ftc.gov/calls**.

We need a unified effort — government, industry and individual — to make a dent in the extortion-by-phone business. No one is expecting total peace and quiet, but we should be able to "weaponize" the consumer, to help neutralize the criminal on the other end of the line. Seeing some of the worst offenders talking to themselves in prison would be rewarding, too. – ***Easton Express-Times* editorial**

The phrase was opaque but vaguely appealing. Why would anyone want to repeal something called "net neutrality"? Neutral is inoffensive, right? So when the Federal Communications Commission debated whether to ditch the policy, many Americans joined in the energetic protests.

Recall how **the U.S. Senate Democratic caucus warned** that "If we don't save net neutrality, you'll get the internet one word at a time." **Sen. Elizabeth Warren said** that "The repeal of these protections has corporate greed and corruption written all over it." **Sen. Chuck Schumer predicted** that without net neutrality, watching baseball on a smartphone would mean missing every other pitch. Hotter heads even used the internet itself to threaten the murder of FCC Chairman Ajit Pai's family. One sign memorably warned his children: **"They will come to know the truth — Dad murdered democracy in cold blood."**

Net neutrality, a policy imposed by the Obama administration's FCC in 2015, essentially said internet providers should make all content available at the same speed. Many liberal advocacy groups and Democratic officials warned that if the Trump administration's FCC repealed net neutrality, cable companies and wireless carriers would speed up and improve the transmission quality of the websites they control, while slowing down rival data streams. What's more, the providers surely would charge more to guarantee high speeds to affluent users, while slowing down data streams to those who couldn't afford fast service.

In other words, defenders of net neutrality said repealing the policy would imperil America's disadvantaged and anti-establishment voices. They

argued that the piping of the internet should be viewed as akin to a regulated water or electric utility, and maintained as a neutral carrier. We wrote in December 2017 that **that argument would make sense if technology had reached maximum progress** and the main concern, as with an electric company, is keeping the lights on. In truth, though, digital technology is a new, evolving industry, more like robotics or bitcoins than water service. It thrives on market competition, consumer choice and, above all, unfettered innovation.

We argued that the policy emphasis should be on encouraging scientific and commercial discoveries, while incorporating safeguards against exploitation of consumers. Our hunch was that rather than enticing internet providers to extort their customers, this deregulation would give private-sector companies incentives to improve speeds and services: Increased competition would be a greater spur to innovation than government fiat had been.

The FCC **did vote to nix** net neutrality, effective June 2018. A year-plus later, broadband download and upload speeds have quickened rather than slowed. Internet providers haven't bifurcated service into different speeds for rich and poor households. Mobile networks, too, move data more swiftly than before. Broadband investment in better technology again has accelerated. And if baseball fan Chuck Schumer has missed a pitch, blame his bat speed, not his data speed. Who knows, maybe the internet providers are lying in wait to pounce on their customers.

More likely, they've learned a lesson from one failure of the post-net-neutrality era. During the California wildfires, Verizon throttled service to the Santa Clara Fire Department, the better to nudge the firefighters into a more expensive data plan. That looked like an outrageous attempt at exploitation. The rest of the story: Verizon copped to a humiliating customer service failure. The company representative engaging with the Fire Department either didn't know about, or flouted, Verizon's standing policy in such situations of suspending any data speed restrictions to emergency responders.

It was a bad mistake, but a mistake. And all the other notorious cases that suggest a need to reinstate net neutrality? That is, where's the internet Cybergeddon the naysayers predicted, and predicted, and predicted? That silence you hear in response to those two questions is the sound of free-market incentives improving internet services at a steady pace. Companies are competing to increase rather than decrease data speeds. And, thus far, internet providers haven't adopted exploitative service and pricing policies that would drive angry customers to rival providers in a heartbeat. And if companies do take unfair advantage of life after net neutrality, the federal deregulation can be modified, or reversed by regulators, or overridden by Congress.

America's web users, then, are back to where they were before net neutrality, when the internet operated without much government interference — and without adverse effects. Government regulation does have its place. But on the internet as in so many other realms, consumers' demands and decisions are the most powerful regulators. Americans are the living, breathing free market forces that drive companies to make their internet services better — and increasingly faster — than ... one ... word ... at ... a ... time. – ***Chicago Tribune* editorial**

Small businesses can take steps to make their computers and websites less vulnerable to cybercriminals, but owners also need to be vigilant about protecting their data. Cybersecurity has some basic components, such as using anti-virus and anti-malware programs on all devices, and making sure that updates and patches that hardware and software makers periodically send out are installed, says James Goepel, CEO of Fathom Cyber, a cybersecurity consulting firm.

Another aspect of cybersecurity is education for everyone, including the owner, about the dangers of clicking on links and attachments in emails. That's a common way for phishing scams to occur; these attacks use realistic-looking emails to trick computer users into downloading harmful software onto computers, phones and other devices. There are plenty of resources online to help owners understand what they need to do. The website for the Federal Communications Commission lists the basics, and also has links to organizations and technology companies that supply more details. Visit **www.fcc.gov/general/cybersecurity-small-business**. Goepel recommends owners visit the website for the Center for Internet Security, which has a comprehensive description of cybersecurity practices. It can be found at **www.cisecurity.org**.

But protecting a company against cyberattacks must be a thorough and ongoing process to be effective. An owner trying to stay on top of patches, updates and changes while also dealing with all the aspects of running a business is likely to need help. Unless there is a dedicated technology staffer in the company, the best strategy is to hire professionals whose work is to monitor companies' systems and be sure their protection is up to date. Similarly, websites need to be monitored to be sure they're not hacked — and if they are, to deal with the invasion immediately. One issue small companies face is that owners may not know how many devices, programs and apps are in their systems — any of them could be vulnerable. "You can't patch everything if you don't know what you have on your network," Goepel says.

Small firms are increasingly targets for attackers, according to insurer Hiscox, which commissioned a survey of 5,400 companies and organizations of all sizes about cybersecurity in late 2018. Forty-seven percent of small businesses, those with under 50 employees, reported at least one or more cyberattacks, up from 33% in a survey a year earlier. Among mid-sized companies, those with between 50 and 249 staffers, 63% reported they'd been hit by a cyberattack, up from 36%. Many small businesses have taken steps to make their data more secure, according to a survey of 1,504 owners Bank of America released during the spring. But when asked about the steps owners took, many hadn't taken care of some key fundamentals. Of the 80% of small businesses that had made adopted cybersecurity measures, only 47% installed security patches and updates and 44% secured their customers' information. That meant a lot of systems weren't protected. "The bad guys know the small guys aren't spending money on it," Goepel says. – ***Associated Press***

BCAP
Broadband
Cable Association
of Pennsylvania
127 State Street Harrisburg, PA 17101
717-214-2000 (f) 717-214-2020
bcapa.com
First in Broadband.
The Future of Broadband.®