Photos by Tony Wittkowski / HP staff

Mike Strudas, owner of Nine to Five Computers in Stevensville, discusses the measure Congress recently passed concerning internet privacy in his business Friday.

Greed in the wires

The battle between privacy and commerce

By RALPH HEIBUTZKI
HP Correspondent

When you're facing a digital world that's getting more efficient at learning your life's most intimate details, it makes sense to try to draw some boundaries.

MELTON

Lake Michigan College's chief information officer, Randall Melton, and his wife followed that logic when they left Facebook, one of the world's most popular social media outlets.

"Everybody that we almost connected to in the past showed up, and we didn't want that. That was too much information. It was a boundary: 'We have a new life now,'" he said.

But those boundaries appeared to blur considerably last month after Congress blocked rules designed to stop internet service providers from selling or tracking consumers' online activity without their permission.

The Federal Communications Commission proposed the rules in October 2016, as President Obama's administration was winding down.

The measure passed the U.S. House of Representatives and U.S. Senate by votes of 215-205, and 50-48, respectively. President Trump signed it into law on April 3.

In the House, Fred Upton, R-St. Joseph, voted to block the rules from taking effect, while Democratic Senators Gary Peters and Debbie Stabenow voted to leave them intact.

Deepening the ISP grasp?

The vote drew sharp criticism from advocacy groups like the Electronic Frontier Foundation, which blasted it as "a crushing loss for online privacy" in its official statement.

"They (ISPs) shouldn't be able to profit off of the information about what you search for, read about, purchase, and more without your consent," the EFF stated.

The outcry, in Melton's eyes, reflects a debate over how to best protect privacy – one that's far from settled.

"When they start releasing your name, and different things like that, that's when it gets a little squirrelly," he said.

Mike Strudas, owner of Nine to Five Computing in Stevensville, said the legislation will only deepen the power that companies like Google enjoy now – in which "you're targeted with the same ads, for the same things you're searching for," he said.

Strudas would like some limits on that power.

"They've (Google) got to make money, too," Strudas said. "I totally

See PRIVACY, page A6

Alex Ott, who runs FixIT Computing in Bridgman, works on a laptop Friday.

Much ado about nothing?

By HP STAFF

Online privacy advocates were aghast when Congress in late March canceled regulations barring internet service providers from trading in personal browsing histories.

But the move by Congress has its supporters, who argue the practical effect on internet users will be nill.

The Federal Communications Commission last year adopted rules barring ISPs from selling such histories without users' permission. The FCC in 2015 gained such authority in its efforts to enforce net neutrality, the idea that ISPs shouldn't play favorites with internet communications.

Until then, the Federal Trade Commission regulated internet privacy.

FCC Chairman Ajit Pai and acting FTC chairwoman Maureen Ohlhausen argued in an April 4 Washington Post column that the FTC can do a better job of protecting privacy than can the FCC.

"Put simply, the Chicken Little-like reaction (to the congressional vote) doesn't make any sense, particularly when compared with the virtual silence when the FCC stripped away existing privacy protections in 2015," the two wrote.

President Donald Trump, who appointed Pai and Ohlhausen to their current positions, signed the repeal.

Pai and Ohlhuausen argue the ISPs have no interest in trading in browsing histories.

"That's simply not how online advertising works," they wrote. "And do so would violate ISPs' privacy promises. ... Congess's decision ... didn't remove existing privacy provisions. It simply cleared the way for us to work together to reinstate a rational and effective system for protecting consumer privacy."

PRIVACY

From page A1

get that. But I don't pay Google anything. I do pay my ISP. They shouldn't make additional profits off me based on that."

Alex Ott, owner of Fix-IT Computing in Bridgman, agrees – citing the policy imposed on users of Microsoft's Edge Web browser.

"You search enough of the same topic, they keep a record, unless you go in, and delete the cookies out of the temporary internet folder. So they're already doing that," she said.

Ott said she didn't recall feeling concerned about the votes in Congress until those scenarios began crossing her mind.

"The more I thought about that, I thought, 'Well, that's a little ridiculous,'" she said.

Getting around the issues

The new legislation "takes away some of the responsibility they (ISPs) had (to consumers)," said Mike Elsner, lead technician for PC Services in Stevensville.

Companies could still offer an opt-out feature to customers trying to protect their digital privacy, but wouldn't legally have to do it.

However, those policies aren't as ironclad as customers think, as Elsner found out when he provided information for a bank loan.

"Every month, or six months, they send a warning: 'We won't use your data,'" Elsner said. "But that doesn't apply to companies owned by the bank. They share that data and send you ads. The next day, I got 20 emails. Their response was, 'We're not selling your information, we're just letting our affiliates use it.'"

The votes in Congress leave large ISPs best positioned to capitalize on users' data because their smaller competitors lack the capability, Elsner said.

Big companies maximize their reach through tactics like "ad injection" or covertly inserting ads into Web pages without a site owner's permission, he said.

"The best defense against the ads are ad blockers. But a lot of sites now say, 'You can't use our site because we've detected an ad blocker,' or, 'You're going to lose functionality if you're going to block our ads,'" Elsner said.

Follow the money

Analysts are calling Congress's actions a major victory for companies like AT&T, Comcast and Verizon, which lobbied to overturn the proposed FCC rules.

That effort involved contributions to representatives and senators voting to overturn the rules, asserts the Verge, an independent reporting website that published a list showing the amounts that Republican supporters received.

In the House, Energy and Commerce Committee, Chairman Greg Walden emerged as the top telecommunication dollar recipient ($155,100) – followed by Steve Scalise ($121,750), and Upton ($108,250), the Verge's list states.

On the Senate side, Majority Leader Mitch McConnell (R-Ky.) led the list, with $251,110, followed by John Thune ($215,000), and then, Roy Blunt ($185,550).

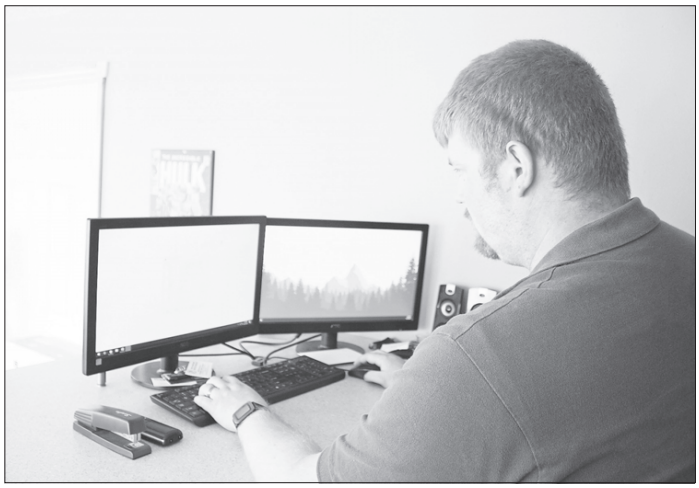
By contrast, Sen. Todd Young, R-Ind., who voted to block the rules, ranked near the bottom, with $28,670.

"Trump needs to use that executive pen and put term limits in place (for congressional representatives). If it has to come to that, it needs to be done, because obviously, people don't vote these guys out," Ott said. "I just don't understand it."

Melton agrees the concerns are real, but doesn't think the battle is over.

He sees nothing to stop states from acting on their own – as Minnesota's state Senate did recently, in passing a bill that bars ISPs from selling data without a user's written consent.

After reading follow-up comments from FCC Chairman Ajit Pai, "I think they're trying to move some of the (privacy) rules back to the FTC (Federal Trade Commission)," Melton said.



Tony Wittkowski / HP staff

Mike Strudas, owner of Nine to Five Computers in Stevensville, focuses on his work Friday.

How to protect yourself

By RALPH HEIBUTZKI
HP Correspondent

So how do consumers protect themselves in this digital jungle?

The No. 1 rule still applies, said Randall Melton, Lake Michigan College's chief information officer.

"We should ask ourselves, 'If this activity were made public, how would this affect me?' We have to be conscious that the private matters we do can be publicly known."

For those reasons, he recommends encrypting sensitive documents, like tax returns – and not posting them on sites like Google Docs, where anyone can retrieve them.

Another option is a virtual private network, or VPN, whose popularity has grown in recent years, said Mike Strudas, owner of Nine to Five Computing in Stevensville.

VPN access fees range anywhere from $6 a month, to $30 to $60 per year.

"All of your Internet traffic – rather than going straight to your ISP – is encrypted, and then sent to a third party, who doesn't collect information, and it goes out to their ISP," Strudas said. "You're part of 100,000 people or more, who are all going out the same pipe."

On the downside, signing with a VPN means "you're subject to the terms and conditions, whatever those may be," Strudas said. "Generally, they're honest and open, but nobody reads those things."

Alex Ott, owner of Fix-IT Computing in Bridgman, is skeptical of VPNs "because you still have to log in with your account," she said.

Aside from being cautious, Ott recommends taking smaller steps – such as erasing your temporary internet folder's contents after a day of searching.

"If you're going to do searches, understand that they're keeping track of it," she said.

Getting savvy about tech

Consumers who don't want to take such radical steps can follow other common sense precautions, which also means getting a lot savvier on how technology affects them, Melton said.

"Always make sure your routers at home – your gateway devices – are secure, that you're not using the default password. Some routers are known to be easily exploitable (to data breaches)," he said.

The same rule goes for other digital devices, such as cameras, that can be accessed remotely, Melton said.

"You need to catalog all your devices, and it's only going to get more challenging, as Whirlpool and other players start creating Wi Fi-connected appliances," he said.

Make sure phones or devices have adequate passwords – preferably 12 digits and longer – so "if you leave it accidentally, you won't have somebody compromising your photos, and things of that nature," he said.

The nature of your job and type of data you handle will help determine what precautions to take, Melton said.

"You need to ask, 'Am I a target?' Not everyone is, but some people can become a target because of what they share on social media, so just be aware of that," he said.