Cooper	Keating	Perlmutter
Correa	Kelly (IL)	Peters
Costa	Kennedy	Peterson
Courtney	Khanna	Pingree
Crist	Kihuen	Pocan
Crowley	Kildee	Polis
Cuellar	Kilmer	Quigley
Cummings	Kind	Raskin
Davis (CA)	Krishnamoorthi	Rice (NY)
Davis, Danny	Kuster (NH)	Richmond
DeFazio	Langevin	Rosen
DeGette	Larsen (WA)	Roybal-Allard
Delaney	Larson (CT)	Ruiz
DeLauro	Lawrence	Ruppersberger
DelBene	Lawson (FL)	Ryan (OH)
Demings	Lee	Sánchez
DeSaulnier	Levin	Sarbanes
Deutch	Lewis (GA)	Schakowsky
Dingell	Lieu, Ted	Schiff
Doggett	Lipinski	Schneider
Doyle, Michael F.	Loebsack	Schrader
	Lofgren	Scott (VA)
Ellison	Lowenthal	Serrano
Engel	Lowey	Sewell (AL)
Eshoo	Lujan Grisham, M.	Shea-Porter
Espaillat		Sherman
Esty	Luján, Ben Ray	Sinema
Evans	Lynch	Sires
Foster	Maloney, Carolyn B.	Smith (WA)
Frankel (FL)		Soto
Fudge	Maloney, Sean	Speier
Gabbard	Matsui	Suozzi
Gallego	McCollum	Swalwell (CA)
Garamendi	McEachin	Takano
Gonzalez (TX)	McGovern	Thompson (CA)
Gottheimer	McNerney	Thompson (MS)
Green, Al	Meeks	Titus
Green, Gene	Meng	Tonko
Grijalva	Moore	Torres
Gutiérrez	Moulton	Tsongas
Hanabusa	Murphy (FL)	Vargas
Hastings	Nadler	Veasey
Heck	Napolitano	Vela
Higgins (NY)	Neal	Velázquez
Himes	Nolan	Visclosky
Hoyer	Norcross	Walz
Huffman	O'Halleran	Wasserman Schultz
Jackson Lee	O'Rourke	
Jayapal	Pallone	Waters, Maxine
Jeffries	Panetta	Watson Coleman
Johnson (GA)	Pascrell	Welch
Johnson, E. B.	Payne	Wilson (FL)
Kaptur	Pelosi	Yarmuth

NOT VOTING—9

Marino	Rooney, Thomas J.	Scott, David
Pittenger		Simpson
Price (NC)	Ros-Lehtinen	Slaughter
	Rush	

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (during the vote). There are 2 minutes remaining.

□ 1547

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

PROVIDING FOR CONGRESSIONAL DISAPPROVAL OF A RULE SUBMITTED BY THE FEDERAL COMMUNICATIONS COMMISSION

Mrs. BLACKBURN. Mr. Speaker, pursuant to House Resolution 230, I call up the joint resolution (S.J. Res. 34) providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to ''Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'', and ask for its immediate consideration in the House.

The Clerk read the title of the joint resolution.

The SPEAKER pro tempore. Pursuant to House Resolution 230, the joint resolution is considered read.

The text of the joint resolution is as follows:

S.J. RES. 34

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled, That Congress disapproves the rule submitted by the Federal Communications Commission relating to ''Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have no force or effect.

The SPEAKER pro tempore. The joint resolution shall be debatable for 1 hour equally divided and controlled by the chair and ranking minority member of the Committee on Energy and Commerce.

The gentlewoman from Tennessee (Mrs. BLACKBURN) and the gentleman from Pennsylvania (Mr. MICHAEL F. DOYLE) each will control 30 minutes.

GENERAL LEAVE

Mrs. BLACKBURN. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on S.J. Res. 34.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Tennessee?

There was no objection.

Mrs. BLACKBURN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I do rise today in support of S.J. Res. 34, which disapproves of the rule submitted by the Federal Communications Commission relating to protecting the privacy of customers of broadband and other telecommunication services.

I applaud Senator FLAKE's work on this issue, as S.J. Res. 34 was passed by the Senate last week. I also filed a companion resolution in the House.

The FCC finalized its broadband privacy rules on October 27, 2016. At that time, they assured us that the rules would provide broadband customers meaningful choice, greater transparency, and stronger security protections for their personal information collected by internet service providers, but the reality is much different.

There are three specific problems with which the FCC has gone about these rules. First, the FCC unilaterally swiped jurisdiction from the Federal Trade Commission. The FTC has served as our Nation's sole online privacy regulator for over 20 years.

Second, having two privacy cops on the beat will create confusion within the internet ecosystem and will end up harming consumers.

Third, the FCC already has authority to enforce privacy obligations of broadband service providers on a case-by-case basis. These broadband privacy rules are unnecessary and are just another example of Big Government overreach. The Competitive Enterprise Institute estimates that Federal regulations cost our economy $1.9 trillion in 2015.

Since President Trump took office, Republicans have been working diligently to loosen the regulatory environment that is suffocating hardworking taxpayers.

Here is what multiple House Democrats said in a letter to the FCC last May regarding the FCC's privacy rules:

> The rulemaking intends to go well beyond the traditional framework that has guarded consumers from data practices of internet service providers and ill-served consumers who seek and expect consistency in how their personal data is protected.

Further, FTC Commissioner Joshua Wright testified before Congress that the FTC has unique experience in enforcing broadband service providers' obligations to protect the privacy and security of consumer data. He added that the rules will actually do less to protect consumers by depriving the FTC of its longstanding jurisdiction in the area. Once again, these rules hurt consumers.

Incredibly, former FCC Chairman Tom Wheeler referred to the internet as the most powerful and pervasive network in the history of the planet before these rules were even created. I found this really odd because it implied that the FTC regulation had indeed been successful and ought to continue, ultimately undermining his own rationale for additional FCC privacy regulation.

Now, there are a couple of myths that are going around that I want to take the time to dispel. Our friends claim there will be a gap for ISPs in the FCC privacy rules when they are overturned. This simply is false, and let me tell you why. The FCC already has the authority to enforce the privacy obligations of broadband service providers on a case-by-case basis.

Pursuant to section 201 of the Communications Act, they can police practices of the ISPs that are unjust or unreasonable. Sections 202 and 222 also protect consumers. It is already in statute. So I encourage my friends to read title II of the Communications Act. Also, the State attorneys general have the ability to go after companies for unfair and deceptive practices.

Third, litigation is another avenue consumers can pursue against ISPs for mishandling personal data. Service providers have privacy policies. If they violate the policy, guess what? They can be sued. I know Democrats will certainly understand that, as they have many trial lawyer friends, and I urge them to speak to the trial bar.

Fourth, the free market is another great equalizer. Can you imagine the embarrassment for an ISP that is caught unlawfully selling data? We have all seen the economic fallout from something such as a data breach. Companies have a financial incentive to handle your personal data properly because to do otherwise would significantly impair their financial standing.

To my Democrat friends across the aisle, the bottom line is this: the only gap that exists is in these arguments that you have made.

Consumer privacy is something we all want to protect, and consumer privacy will continue to be protected and will actually be enhanced by removing the uncertainty and confusion these rules will create, as the Democrats Rush, Schrader, and Green indicated in a letter to the FCC last May.

I also want to speak, for just a moment, on the edge providers because there has been some question about who has visibility into your data. Clinton administration veteran privacy expert Peter Swire offered a report in February 2016 titled ''Online Privacy in ISPs.''

ISP's access to consumer data is limited and often less than access to others. Swire found that ISPs have less visibility into consumer behavior online than search, social media, advertising, and big tech companies.

Swire's study found that, as a result of advancing technologies, the rise of encryption, and the various ways and locations individuals access the internet, ISPs now have increasingly limited insight into our activities and information online.

By contrast, however, so-called edge providers, like search engines, social media, advertising, shopping, and other services online, often have greater visibility into personal consumer data.

Mr. Speaker, I reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in strong opposition to S.J. Res. 34.

Today, colleagues, we are waist deep in the swamp. The American people did not ask for this resolution.

In fact, no company will even put its name behind this effort. Instead, this resolution is the result of an explicit written request from Washington lobbyists. These lobbyists make the bogus claim that having actual protections will confuse consumers and the only way to help clear up this information is to have no rules at all.

No consumer has come forward to support this position. No consumer has said this argument even makes sense.

I challenge every Member of this body at your next townhall meeting to have a show of hands of how many people think it is a good idea to allow your internet service provider to sell their personal information without their permission.

□ 1600

Then after you get that show of hands, ask them how many of them would vote for you if you support allowing corporations to do that.

This resolution is of the swamp and for the swamp and no one else. The rules of this resolution would overturn rules that are simple and make common sense. They don't require much, only three things:

One, internet service providers should ask permission before selling your private internet browsing history, app usage, or other sensitive information;

Two, once they have your information, internet service providers should take reasonable measures to protect it; and

Finally, if the information gets stolen, the company should quickly let you know.

That is it. That is all that is being asked of them.

These modest rules don't stop internet service providers from using data for advertising and profiling or whatever else so long as they ask first.

ISPs have an obligation under these rules not to dive into the personal lives of Americans unless that is what those Americans want. They just need to ask first.

This is particularly true because broadband providers see literally everything you do online, every website you visit, every app, every device, every time. By analyzing your internet usage and browsing history, these companies will know more about you than members of your own family, more than you tell your doctor, more than you know about yourself. Without these rules, these companies don't have to ask before selling all of that information, and they don't have to take reasonable measures to protect that information when they collect it.

Make no mistake about this, colleagues: Anyone who votes for this bill is telling your constituents that they no longer have the freedom to decide how to control their own information. You have given that freedom away to big corporations. More importantly, there aren't rules to fall back on if Congress scraps these.

Critics of the rules argue that the Federal Trade Commission should oversee the privacy protection for broadband providers, but, under current law, they have no authority to do so, and the CRA won't do a thing to fix that. Under a Federal court of appeals case, the FTC has no authority over mobile broadband providers at all.

And to those that say the FCC can evaluate complaints on a case-by-case basis using its statutory authority, the current Chairman—your current Chairman—stated that section 222 cannot be used to protect personal information and that rules are necessary to enforce this statute.

Mr. Speaker, I include for the RECORD a statement by the FCC Commissioner.

DISSENTING STATEMENT OF COMMISSIONER AJIT PAI

Re TerraCom, Inc. and YourTel America, Inc., Apparent Liability for Forfeiture, File No. EB–TCD–13–00009175.

A core principle of the American legal system is due process. The government cannot sanction you for violating the law unless it has told you what the law is.

In the regulatory context, due process is protected, in part, through the fair warning rule. Specifically, the D.C. Circuit has stated that ''[i]n the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property.'' Thus, an agency cannot at once invent and enforce a legal obligation.

Yet this is precisely what has happened here. In this case, there is no pre-existing legal obligation to protect personally identifiable information (also known as PII) or notify customers of a PII data breach to enforce. The Commission has never interpreted the Communications Act to impose an enforceable duty on carriers to ''employ reasonable data security practices to protect'' PII. The Commission has never expounded a duty that carriers notify all consumers of a data breach of PII. The Commission has never adopted rules regarding the misappropriation, breach, or unlawful disclosure of PII. The Commission never identifies in the entire Notice of Apparent Liability a single rule that has been violated.

Nevertheless, the Commission asserts that these companies violated novel legal interpretations and never-adopted rules. And it seeks to impose a substantial financial penalty. In so doing, the Commission runs afoul of the fair warning rule. I cannot support such ''sentence first, verdict afterward'' decision-making.

To the extent that the circumstances giving rise to today's item merited the Commission's attention, there was a better (and lawful) path forward. We could have opened a notice-and-comment rulemaking. This process would have given the public an opportunity to speak. And in turn, the agency would have had a chance to formulate clear, well-considered rules—rules we then could have enforced against anyone who violated them. Instead, the Commission proposes a forfeiture today that, if actually imposed, has little chance of surviving judicial review.

One more thing. The Commission asserts that the base forfeiture for these violations is nine billion dollars—that's $9,000,000,000—which is by far the biggest in our history. It strains credulity to think that Congress intended such massive potential liability for ''telecommunications carriers'' but not retailers or banks or insurance companies or tech companies or cable operators or any of the myriad other businesses that possess consumers' PII. Nor can I understand how such liability can be squared with the Enforcement Bureau's recent consent decrees with these companies. Under those consent decrees, the companies paid the Treasury $440,000 and $160,000 for flouting our actual rules and draining the Universal Service Fund by seeking Lifeline support multiple times for the same customer.

Consumer protection is a critical component of the agency's charge to promote the public interest. But any enforcement action we take in that regard must comport with the law. For the reasons stated above, I dissent.

Mr. MICHAEL F. DOYLE of Pennsylvania. Without these protections, there will be no clear rules of the road. At a time when foreign actors like the Russians, the Chinese, and everyone else under the sun are constantly trying to steal our data and compromise our security, it would be irresponsible to roll back the only Federal safeguards we have. I want my colleagues to think long and hard before you give corporations the ability to sell your information without their permission.

Mr. Speaker, I include several articles in the RECORD by Free Press and the Open Technology Institute opposing the CRA, an op-ed from a current

FTC Commissioner opposing this CRA, and a memorandum from engineers at EFF opposing this CRA.

[From Free Press, May 10, 2016]

PAY-FOR-PRIVACY SCHEMES PUT THE MOST VULNERABLE AMERICANS AT RISK

(By Sandra Fulton)

The FCC has opened a proceeding on the rules and policies surrounding privacy rights for broadband service. One industry practice called into question in that proceeding could have a devastating impact on our most vulnerable populations.

Internet service providers charge broadband customers a ton for Internet access. ISPs are increasingly finding new revenue streams too, by taking part in the multibillion-dollar market that's evolved out of selling users' personal information to online marketers. As the debate around privacy has heated up, ISPs have tried to placate the public's growing interest in privacy protections while maintaining revenues they can get when they auction off their customers' valuable personal information.

One proposed solution that AT&T has largely ''pioneered''? Have customers pay to preserve their privacy.

The potential harms and discriminatory implications of this practice are obvious. It could mean that only people with the necessary financial means could protect their privacy and prevent their ISPs from sharing their personal information with predatory online marketers. The FCC rulemaking proceeding seeks comments on whether to allow such ''financial inducements'' for the surrender of private information. If the agency decides not to ban such practices outright, it wants to know how it should regulate them.

As our lives have moved online, ISPs have gained access to our most sensitive personal information. Advanced technologies allow companies to track us invisibly, collecting and selling data on nearly every detail of what we do online.

But ISPs don't just stop at knowing what we're doing. The location tracking that's needed to provide mobile service to our phones lets the ISPs know when and where we do it too. And they can figure out the people and organizations we associate with by looking at who we talk to and which websites we visit.

As ISPs track their customers, they create comprehensive dossiers containing sensitive information on each person's finances, health, age, race, religion and ethnicity. Their reach is so pervasive that information like a visit to a website discussing mental health, a search on how to collect unemployment benefits, or a visit to a church or Planned Parenthood office could be swept up into their databases.

How do you feel about your ISP selling such a personal glimpse into your life to online advertisers? Under a pay-for-privacy scheme, you wouldn't need to worry about it so long as you could afford to shell out the hush money. But those who aren't so fortunate would have to relinquish any control over how their personal data is spread across the Web.

The FCC raised concerns about this dynamic when it launched its rulemaking proceeding, noting that such pay-for-privacy practices might disadvantage low-income people and members of other vulnerable communities. But it didn't make any specific recommendations or issue any proposals on how to regulate in this space.

Long before the FCC launched this inquiry at the end of March 2016, and even before the agency had clarified its authority to protect broadband users in the February 2015 Open Internet Order, AT&T's GigaPower broadband service had become one of the first pay-for-privacy plans on the market. The AT&T deal allows customers to opt out of some information sharing if they pay an extra $29 a month or more.

For a struggling family, that could mean choosing between paying for privacy and paying for groceries or the public transportation needed to get to work. And while AT&T might be the first to launch this kind of service, an article in Fortune notes that other companies are eager to roll out similar plans.

Under pay-for-privacy models, consumers who are unable to pay the higher broadband cost will likely see their ISPs share their data with shadowy online data brokers who use this information to tailor marketing messages. While unregulated and unaccountable data brokers are a threat to everyone's privacy, they're notorious for targeting low-income communities, people of color and other vulnerable demographics.

One particularly damning report from the Senate Commerce Committee offered this glimpse into how these brokers categorize and label these target audiences:

The Senate committee's report notes, for example, that the ''Hard Times'' category includes people who are ''Older, down-scale and ethnically diverse singles typically concentrated in inner-city apartments.''

It continues: ''This is the bottom of the socioeconomic ladder, the poorest lifestyle segment in the nation. Hard Times are older singles in poor city neighborhoods. Nearly three-quarters of the adults are between the ages of 50 and 75; this is an underclass of the working poor and destitute seniors without family support . . .''

These classifications can influence not just what kinds of ads people see, but the interest rates they're offered or the insurance premiums they pay. These targeted communities are precisely the ones who can't pay extra to shield their personal information from these dangerous companies.

There may be some argument that if big companies are going to profit from our data anyway, it's actually good if their customers get a share of that. The FCC's rulemaking proposal notes that brickand-mortar stores and websites alike offer all sorts of ''free'' services, discounts and perks in exchange for the data they mine from their customers and users.

But the nature of the broadband market—where users have no real options when it comes to choosing their providers, and no way to opt out short of staying offline—makes the tradeoffs here especially worthy of attention. If users could get fair value for their data, and if they got a real discount on broadband and not just a privacy penalty, and if they were providing truly informed consent with full knowledge of all the pernicious uses data brokers have for their information, then maybe we could have a conversation about the fairness of such schemes. But those are some very big ifs.

We need better transparency rules for marketers and easy-to-use disclosures and opt-in mechanisms before we get there. We also need strong baseline privacy protections guaranteed for all, including rules that prohibit ISPs from using discriminatory schemes that jeopardize the rights of their most vulnerable customers.

We applaud the FCC for taking this crucial first step to protect privacy from broadband ISPs' overreach and abuse. As gatekeepers to the Internet, ISPs hold a wealth of information about their customers, and the Communications Act commands the FCC to establish strong safeguards for that private info. But the FCC also must also remember that our rights are not for sale—and that privacy is not a luxury for the wealthy.

ISPS KNOW ALL

YOU DESERVE MORE PRIVACY FROM YOUR BROADBAND PROVIDER

(By Eric Null)

As you read this post, your internet service provider is collecting information about you: what you're reading right now on Slate, what URL you go to next, what time of day it is, and whether you're on your home computer or your mobile device, among many other data points. Your ISP has similar data about apps you've used, how much data you consume at any given time of day, and your other daily internet habits and rhythms. Of course, your ISP has other up-to-date personal information as well—things like your name, address, telephone number, credit card number, and likely your Social Security number. In this way, ISPs have access to a uniquely detailed, comprehensive, and accurate view of you and every other subscriber. All of this at a time when consumer concern over privacy is increasing and has actually caused people to refrain from engaging in e-commerce and other activities online.

To make matters worse, you are essentially powerless to limit the data your ISP collects about you. While you may, in some instances, defend yourself against tracking by websites and apps by disallowing cookies or turning on ''Do Not Track'' in your browser settings, in many cases there is no way to protect against ISP tracking except by avoiding the internet altogether.

While there are some tools that can help consumers protect themselves, they are not prevalent. For example, ISPs cannot see full website addresses when that site uses encryption—denoted by a small lock icon in your browser bar. However, the website—not you—decides whether it will use encryption. And while Netflix traffic is encrypted (so your ISP only knows you're watching videos, not specifically which ones you're watching), WebMD traffic is not (so your ISP likely knows every page you've visited on WebMD), even though medical symptoms are clearly much more personal than your favorite TV program.

Another example of ways consumers can purportedly protect themselves is through virtual private networks, or VPNs, which route web traffic through another network and therefore effectively ''hide'' the traffic from the person's ISP. But VPNs are difficult to use and configure. They often cost extra money, slow down your browsing, and simply send your data through some other access provider that may be collecting data about you, too. These options are not practical defenses for most consumers.

Currently, there are no rules to prevent your ISP from using these data for almost any purpose, including categorizing you and serving you advertisements based on those categories. Targeted ads may even be based on whether you have (or the ISP has inferred you have) a certain disease or what your income level is. Recently, Cable One was found to be using predictive analytics to determine which of its customers were ''hollow'' (that is, had low credit scores) and then offering them low-quality customer service. Cable One technicians, the company's CEO stated, aren't going to ''spend 15 minutes setting up an iPhone app'' for someone with a low credit score. Of course, making decisions based on credit scores is going to disproportionately affect communities of color and other vulnerable populations. Additionally, the data ISPs collect, often compiled into a ''profile,'' might be sold to third parties (like advertisers or data brokers) and used and reused for purposes for which they were not initially collected—in ways that often annoy people, such as when personal information is used to send a ''barrage of unwanted

emails.'' And as the number of entities who hold your data increases, so too does the chance those data will be compromised by a leak or hack.

So you may find yourself between a rock and a hard place: Use the internet and give up your privacy, or forego internet access entirely—something that's not exactly reasonable. But there is good news. The Federal Communications Commission is trying to make sure that you and all other ISP customers don't have to confront this choice. In 2015, as part of decision to uphold net neutrality, the FCC ruled that ISPs are ''common carriers.'' (The U.S. Court of Appeals for the District of Columbia Circuit recently upheld that ruling.) Since then, the FCC has had a statutory obligation to protect the data ISPs collect about their customers. To accomplish that, the FCC recently proposed a new rule that would require ISPs, in most cases, to seek opt-in consent from customers before using data collected for purposes other than to provide service, such as to deliver certain kinds of ads or to sell to data brokers. That means that if the rule passes, your ISP would have to notify you of any new intended use of the data and give you the opportunity to say ''yes, that is OK with me'' or ''no, that is not OK with me.'' Of key importance in this rule is that if you said ''no,'' your ISP couldn't just refuse to serve you—it would have to respect your wishes and still provide you with service.

The FCC's proposal should be enacted, because you should not have to trade your privacy to access the internet. (New America's Open Technology Institute, where I work, has been actively engaged on this issue and has submitted comments in the record. New America is a partner with Slate and Arizona State University in Future Tense.) It should go without saying, but it's important enough that I will say it anyway: Internet access is imperative for personal and professional success in today's digital world. Yet to gain access to the most important tool of the 21st century, you have to allow your ISP access to incredibly rich and private information about what you do online. You should get to control what it does with that data. Consumers deserve real choice when it comes to protecting their data, and the opt-in regime proposed by the FCC is a huge step in the right direction.

Yet—perhaps unsurprisingly—ISPs and several House committees have responded to the FCC's proposal as if the sky is falling. They have mounted an all-out assault on the idea that you should have the right to choose how ISPs use your data. Their arguments range from the highly dubious (the proposal exceeds the FCC's authority) to the downright silly (consumers will be confused by having different privacy rules for ISPs as compared with other companies, like search engines and social networks). Chances are your ISP is telling the FCC that you don't need protections against exploitation of your data. (If you're interested, you can see exactly what your ISP is saying—here are the responses from AT&T, Comcast, CenturyLink, T-Mobile, Verizon, and Sprint; unnamed ISPs may be represented by various trade associations like the National Cable and Telecommunications Association and CTIA for wireless.) However, as with the net neutrality debate that led to this proposal, consumers may feel differently.

The FCC has proposed a very strong rule that will help protect ISP customers from exploitative uses of their data. This battle for consumer choice will be ongoing for many months, but soon, you may finally be able to choose both having internet access and protecting your privacy.

ELECTRONIC FRONTIER FOUNDATION,
San Francisco, CA.

FIVE WAYS AMERICANS' CYBERSECURITY WILL SUFFER IF CONGRESS REPEALS THE FCC PRIVACY RULES

If the House votes to repeal the FCC's recent privacy rules, Americans' cybersecurity will be put at risk. That's because privacy and security are two sides of the same coin: privacy is about controlling who has access to information about you, and security is how you maintain that control. You usually can't break one without breaking the other, and that's especially true in this context. To show how, here are five ways repealing the FCC's privacy rules will weaken Americans' cybersecurity.

1. Internet providers will record our browsing history, and the systems they use to record that information (not to mention the information itself) will become very tempting targets for hackers. (Just imagine what would happen if a foreign hacker thought she could blackmail a politician or a celebrity based on their browsing history.)

2. In order to record encrypted browsing history (i.e. https websites), Internet providers will start deploying systems that remove the encryption so they can inspect the data. Although US-CERT (part of DHS) just put out an alert saying that this is extremely dangerous for Americans' cybersecurity, FCC Chairman Pai just decided not to enforce rules that keep Internet providers from doing this.

3. Internet providers will insert ads into our browsing, but that could break the existing code on webpages. That means security features might be broken, which could expose Americans to a greater risk of attack.

4. Internet providers will insert tracking tags into our browsing—and that means every website will be able to track you, not just your Internet provider, and there's nothing you can do to stop them.

5. Internet providers will pre-install software to record information directly from our mobile phones (after all, it's just one more source of information they can monetize). But if the software that does that recording has bugs or vulnerabilities, hackers could break into that software, and then access everything the Internet provider could see. Do you trust your Internet provider, which can't even keep an appointment to fix your cable, to write completely bug-free software?

The net result is simple: repealing the FCC's privacy rules won't just be a disaster for Americans' privacy. It will be a disaster for America's cybersecurity, too.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I reserve the balance of my time.

The SPEAKER pro tempore (Mr. ROGERS of Kentucky). The gentleman is reminded to address his remarks to the Chair.

Mrs. BLACKBURN. Mr. Speaker, I will remind my colleagues across the aisle that, again, section 222 of the Communications Act covers the authority that the FCC needs. Traditionally, online privacy has been handled by the FTC. That is an authority that we have designated to them.

Mr. Speaker, I yield 5 minutes to the gentleman from Oregon (Mr. WALDEN), chairman of the Energy and Commerce Committee.

Mr. WALDEN. Mr. Speaker, I thank my colleagues for their good work on this legislation.

As we increasingly rely on technology in nearly every area of our lives, one of Congress' most important responsibilities is to strike the right balance between protecting consumers' privacy while also allowing for private sector innovation and the new jobs and economic growth that accompany it.

The resolution before us today reverses overreaching, shortsighted, and misguided rules adopted by unelected bureaucrats at the Federal Communications Commission. These rules do little to enhance privacy, but clearly add a new layer of Federal red tape on innovators and job creators. This is exactly the type of government overreach that the Congressional Review Act was meant to stop.

The Federal Communications Commission, frankly, overstepped its bounds on many issues during the Obama administration, including privacy regulations. After stripping the Federal Trade Commission of its authority over the privacy practices of internet service providers, ISPs, the FCC adopted shortsighted rules that only apply to one part of the internet. Despite the FTC's proven case-by-case approach to privacy enforcement that, frankly, has protected consumers, while simultaneously allowing ISPs to innovate, the FCC opted to abandon this model in favor of an approach that assumes the Federal Government knows best what consumers want.

Simply put, the rules that the FCC applied to ISPs are illogical. The regulations would require companies to apply the same privacy protections to consumer data, regardless of its importance or sensitivity. It hardly makes sense to treat a local weather update and personal financial information the same way.

In addition, the FCC's approach only protects consumer data as far as the internet service provider is involved. An entirely separate set of rules applies to providers of edge services. That means the giant search corporations, one of which controls up to 65 percent of your searches on the internet, don't live by the same set of privacy rules as your small town ISP.

What America needs is one standard, across-the-internet ecosystem, and the Federal Trade Commission is the best place for that standard.

The impact of these rigid regulations has the potential to stifle one of the most innovative sectors of our Nation's economy, and it is consumers who will suffer. These rules, which Congress will repeal, only lead to higher costs, less competition, and fewer service offerings. This approach is particularly burdensome for small businesses, which do not have hallways full of lawyers to navigate these tedious and unnecessary rules.

The benefits of the FCC's privacy regulations are questionable, but the harms are certain, which is why I urge my colleagues to support this resolution. And once these rules are reversed, the FCC can turn back to working together with the FTC to ensure that our privacy framework allows the internet

to flourish while truly protecting consumers.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I would remind my friends that, under current law, the FTC has no authority to regulate ISPs and that it was your Commissioner, your current FCC Commissioner, that said that they can't do it under section 222 also, which I have submitted for the record.

Mr. Speaker, I yield 4 minutes to the gentlewoman from California (Ms. ESHOO).

Ms. ESHOO. Mr. Speaker, I thank my friend, Mr. DOYLE, for both his leadership and for yielding time to me.

America, listen up today. There may not be that many people on the floor of the House, but this is a big one. This is really a big one. Congress is poised today to betray the American people on one of the issues they care the most about: their privacy—their privacy. Every single one of us cares about it, and so do the American people. I often say that every American has it in their DNA: Keep your mitts off my privacy, what I consider to be private.

Now, the consequences of passing this resolution are clear. Broadband providers like AT&T, Comcast, and others will be able to sell your personal information to the highest bidder without your permission, and no one will be able to protect you, not even the Federal Trade Commission that our friends on the other side of the aisle keep talking about. It is like open the door and there is no one there. That is what this thing creates.

The Republicans are blowing a gaping hole in Federal privacy protections by barring the FCC from ever adopting similar protections in the future. So, if it is gone today, it is gone, period.

The FCC rules are simple. They require broadband providers to get the permission of their customers—including all of us—before they can sell their web browsing history, their location information, and other sensitive data to third parties.

The majority claims that we need to repeal these protections because they treat broadband providers differently than other online service providers, edge providers. Broadband providers are in the unique position of seeing everything we do on the internet. This is the reason, and it is reason enough, to put privacy protections in place; but it is also important to keep in mind that consumers, all of us, pay a high monthly fee to broadband providers, and they face serious barriers if they want to switch. If I want to switch, if you want to switch, you have to, many times, pay early termination fees.

This is completely different from other online services that collect consumer data. Consumers don't pay to use search engines or social media applications like Google and Facebook. If they don't like Google's privacy policy, they can switch over to Bing without paying any fees. But consumers can't do this with broadband providers, and therein lies the difference.

Last week, we heard the Republicans bemoan the lack of choice in the healthcare market. They should take a closer look at the state of the broadband market, particularly in rural America, where only 13 percent of consumers have access to more than one high-speed broadband provider.

So the majority is telling Americans today, particularly those in rural areas, that they need to choose between their privacy and their access to the internet. If this resolution passes, people across the country will certainly not have both.

This resolution is—excuse the phrase—repeal without replace. The Republicans have not put forward any privacy proposal at all to replace the FCC's rules, despite knowing that repealing these rules will leave a gap in the Federal protections.

So the message to the American people is clear: Your privacy doesn't matter, and your web browsing history should be available to anyone who will pay the highest price for it.

For all these reasons, I urge my colleagues to stand up for privacy rights and oppose this joint resolution.

Mrs. BLACKBURN. Mr. Speaker, I yield the balance of my time to the gentleman from Texas (Mr. FLORES), and I ask unanimous consent that he may control that time.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Tennessee?

There was no objection.

Mr. FLORES. Mr. Speaker, I yield myself such time as I may consume, and I thank the gentlewoman for yielding the balance of her time to me.

Mr. Speaker, as an original cosponsor of the House companion to S.J. Res. 34, I rise to strongly urge my colleagues to support the resolution before us today. Like all of my colleagues in the House, I care deeply about protecting the privacy of our constituents, but I cannot support the Federal Communications Commission's counterproductive rules that will actually harm consumers and stifle innovation.

For 20 years, the Federal Trade Commission—or the FTC, as we call it, frequently—oversaw consumer privacy for the entire internet ecosystem: content providers, advertisers, and internet service providers, or ISPs. The FTC's privacy program focused on preserving sensitive consumer data and took the context of a consumer's relationship with businesses into consideration. The FTC's experience in implementing a wide range of rules and regulations has resulted in over 500 cases protecting consumer information, ensuring their privacy online.

In a flawed political move, absent any finding, complaints, or investigations to determine whether broadband providers have violated consumers' privacy or that the FTC had failed at doing its job, the FCC proceeded with a partisan vote to target ISPs and to expand its regulatory footprint.

After stripping the FTC of its authority over the privacy practices of internet service providers, the FCC subsequently adopted rules that would harm consumers and split the internet, creating an uneven playing field between service providers and content providers. Congress must fix this overreach so the new administration can create a comprehensive, consistent set of privacy protections.

□ 1615

Consumers expect their privacy to be protected the same way no matter what type of entity holds their data. Having two sets of requirements creates confusion for consumers and may jeopardize their confidence in the internet.

Our internet economy has thrived under the privacy regime created by the FTC. Yet the FCC, under its previous Chairman, Tom Wheeler, wanted to undermine that success by bifurcating privacy protections to serve outside political interests, not the American consumer.

By contrast, the FCC's approach did not base its requirements on consumers' preferences about sensitive information and to set opt-in and opt-out defaults. Accordingly, its overall approach was top-down, heavyhanded regulation in stark contrast to the FTC's greater reliance on markets and consumer preferences.

The FCC's rule has a number of problematic issues:

The first is that the opt-in/opt-out regime reduces consumer choice and would be detrimental to the survival of many businesses in this country.

The second is that the FCC would have prohibited unforeseeable future uses of collected data regardless of what consumers actually preferred and businesses may need.

Third, the FCC would also have unjustly applied its heavyhanded approach to broadband providers, treating them more harshly than other players in the internet ecosystem.

In sum, the FCC's broadband privacy protection approach would have rejected free markets and ignored sound economics.

Alternatively, the FTC private enforcement is market oriented and flexible and adaptable to changes in consumer preferences and markets. It also treats companies and players neutrally, fostering an environment of competition and innovation.

This resolution rescinds the FCC's rule, but it does provide the FCC the opportunity to provide oversight more in line with the FTC, which has been successfully regulating online privacy for nearly two decades.

This joint resolution does not lessen or impede privacy and data security standards that have already been established. We are simply restoring a more stable regulatory playing field to ensure that consistent, uniform privacy security standards are maintained to protect consumers and future innovation.

Once Congress rejects these rules, the FCC can turn back to cooperating with

the FTC to ensure that both consumer privacy across all aspects of the internet is provided through vigorous enforcement and also that innovation is allowed to flourish.

I urge my colleagues to support this resolution.

Mr. Speaker, I reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I would just remind my colleague, once again, that the FTC has no authority to regulate ISPs once this bill is implemented; and consumers will not be protected, and their current FCC Commissioner has stated that.

Mr. Speaker, I yield 1½ minutes to the gentlewoman from Colorado (Ms. DEGETTE).

Ms. DEGETTE. Mr. Speaker, I oppose this resolution because it would remove consumers' right to control their online privacy and put it in the hands of corporations.

Every time people go online, they create trails of data that have tremendous commercial value. This creates incentive for the ISPs to sell web history to a third party, be it an advocacy group, a for-profit company, or even a foreign government.

Late last year, the FCC put Americans in charge of how ISPs use and share their consumer data. The FCC's rule also required that the ISPs engage in reasonable data security practices.

Even if people believe that the FCC's rule went too far and should be modified, it is unclear how the FCC could move forward with such a plan given the constraints of the Congressional Review Act. Furthermore, as several people have mentioned, the FCC, which is charged with protecting consumers' privacy, does not even have the authority to oversee ISP practices.

Given the number of data breaches in recent years at companies such as Yahoo, we should, frankly, be strengthening data retention requirements, not weakening them. At its core, S.J. Res. 34 weakens consumer protections today and makes them harder to implement in the future, which is why I urge my colleagues to oppose it.

Mr. FLORES. Mr. Speaker, I yield 2 minutes to the gentleman from Ohio (Mr. JOHNSON).

Mr. JOHNSON of Ohio. Mr. Speaker, when the FCC reclassified the internet as a common carrier, utility-style service and adopted their rules regulating the use of consumer data by internet service providers, it represented a monumental shift in the way we view privacy.

Instead of a uniform, technology-neutral standard that balanced data protection with consumer choice, internet users were stuck with a two-sided approach that causes confusion and dampens competition. There is one set of rules for service providers, and one set for the rest of the internet ecosystem. But how often do consumers really recognize the difference between where their data is accessed and where it is stored?

Ultimately, consumers are actually harmed by the artificial sense of protection created by these rules. It is essential that we take steps to restore the time-tested framework embraced by the Federal Trade Commission.

We have talked a lot about protecting consumer privacy and data, but I haven't heard a lot about allowing the consumer to decide how their information is used. Consumers deserve to have the autonomy to control their information and their internet experience.

As Acting Chairman of the FTC Maureen Ohlhausen pointed out:

> The FTC approach reflects the fact that consumer privacy preferences differ greatly depending on the type of data and its use.

There is widespread agreement that sensitive data, like financial or health information, should be strongly protected and opt-in appropriate. But what about other types of nonsensitive data? Let's not forget the ways that consumers benefit from allowing ISPs access to that kind of information.

Consumers should retain the ability to make the decisions that make sense for them when it comes to how their nonsensitive data is used and obtain the discounts or lower prices that can result. This vote isn't about reducing the level of privacy protection for consumers; it is about an FCC decision that ignored the preferences of consumers in favor of a regulatory power grab.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. FLORES. Mr. Speaker, I yield an additional 15 seconds to the gentleman.

Mr. JOHNSON of Ohio. The FCC's privacy rules are an overreaching regulatory mess that create confusion and inconsistency for consumers, harm competition, and upend internet privacy as we know it.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, might I inquire as to how much time remains on both sides?

The SPEAKER pro tempore. The gentleman from Pennsylvania has 19 minutes remaining. The gentleman from Texas has 11¾ minutes remaining.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I would remind my colleagues that, whether it is nonsensitive information or sensitive information, the ISP should ask for your permission to use it.

Mr. Speaker, I yield 5 minutes to the gentleman from New Jersey (Mr. PALLONE), the ranking member of the Energy and Commerce Committee.

Mr. PALLONE. Mr. Speaker, nearly every day now, we hear about new ways our enemies are trying to steal Americans' information. Just a couple weeks ago, two Russian hackers were indicted for stealing personal information from millions of us.

American consumers visit billions of internet destinations through a multitude of devices. Broadband providers potentially have access to every bit of data that flows from a consumer. The American people are rightfully concerned about companies selling their personal information, including sensitive information like their location, financial and health information, Social Security numbers, and information about their children.

Late last year, the FCC took steps to protect every American citizen's data and privacy, and the rules were simple: first, broadband providers had to ask their customers before selling any data; second, the companies had to take reasonable measures to protect that data; and third, the companies had to let people know if their data was stolen.

That was a good first step, Mr. Speaker. But Congress also has a role in protecting our data, and we should be working in a bipartisan fashion to discuss ways we can better protect the American people's data. Instead, the Republicans have decided to spend this time wiping out the few privacy safeguards that we already have.

The FCC's cybersecurity rules are, in my opinion, not burdensome. They simply tell the network providers to be reasonable when protecting the data. That is all. The FCC left it to the companies, themselves, to use their best judgment about how to get the job done. They just needed to be reasonable.

It seems being reasonable is still too much for the Republicans—first in the Senate, and now here in the House. This resolution tells the companies charged with running the country's broadband networks that they no longer have to be reasonable when it comes to their customers' data.

So I say, Mr. Speaker, make no mistake: This resolution is a gift to countries like Russia who want to take our citizens' personal information. And if the House passes this resolution, it will go straight to the President's desk, a President who will be more than happy to sign his name to this gift to the Russians.

This resolution also gives large corporations free rein to take customers' data without anyone's permission. This debate is about whether Americans have the freedom to decide on our privacy.

We hear all kinds of complicated arguments about jurisdiction, implementation dates, and who knows what else, but these arguments just muddy the water.

Republicans will say that the FCC's rules are confusing to consumers, people won't know what to do if they are asked first before broadband companies sell their sensitive information. If that were the case, we would have heard from people who oppose the rules, but we simply have not heard any of those concerns. The facts speak for themselves. Consumers want more privacy protection, not less.

Seventy-four percent of Americans say it is very important that they be in control of information, and 91 percent of people feel they have lost control

over their own information. There are real consequences to these feelings. Nearly half of Americans say they limit their online activity because they are worried about their privacy and security. That is why they overwhelmingly support stronger protections.

The FCC listened to the American people and adopted reasonable rules. Despite Republican claims to the contrary, the rules were not hard to follow. The rules still allow broadband companies to offer services based on their customers' data, and they can still customize ads or send reminders.

The FCC's rules simply required companies to ask people first before selling their sensitive information. That is it. In fact, I had hoped the FCC would have gone even further, but the agency chose this more moderate approach.

So as this debate proceeds, we should be asking one simple question: Should the American people have the freedom to choose how their information is used or should the government give that freedom away?

I think the answer is clear. I stand with the American people, and, therefore, I strongly oppose this legislation.

Mr. FLORES. Mr. Speaker, I yield 3 minutes to the gentleman from Ohio (Mr. LATTA).

Mr. LATTA. Mr. Speaker, I thank the gentleman for yielding.

Mr. Speaker, I rise today in support of the resolution and want to address an issue created by the Federal Communication Commission's misguided privacy rule in a recent Ninth Circuit case.

For decades, the Federal Trade Commission has been the privacy cop on the beat for most industries, including the technology sector, protecting consumers from unfair or deceptive acts or practices. The Federal Trade Commission has brought over 500 privacy and data security cases to protect consumers. These include cases against internet service providers and some of the largest edge providers.

The Federal Communications Commission is a regulatory body focused on regulating interstate and international communications by radio, television, wire, satellite, and cable.

The Federal Trade Commission's work in privacy and data security has long been held up as a model by both parties, praising the agency for strong enforcement without overly burdensome regulations. During negotiations with the European Union to finalize the U.S.-European privacy shield, the Obama administration held up the Federal Trade Commission as the premier privacy enforcement agency.

Unfortunately, in a midnight action, the Federal Communications Commission jammed through its own privacy rule that is very different from the framework that the Federal Trade Commission has been enforcing for decades.

While we can reverse the poorly constructed FCC rule today, we must still address a recent court ruling. The Ninth Circuit recently ruled that the common carrier exemption in the Federal Trade Commission Act exempts an entity in its entirety from the Federal Trade Commission's jurisdiction if it engages in any common carrier activities, even if the company also engages in non-common carrier activity.

I have introduced legislation to address the court's ruling with the gentleman from Texas (Mr. OLSON). It is my hope that our colleagues will join us.

S.J. Res. 34 makes clear that the Federal Trade Commission has authority over common carriers when they are acting outside the scope of the common carrier.

The repeal of the Federal Communications Commission's misguided privacy rule in the Ninth Circuit's opinion creates a gap and an irrational approach to privacy for consumers and would leave portions of the internet ecosystem completely outside the Federal Trade Commission's jurisdiction. This bill makes clear that the common carrier exemption is important to ensure that no duplication regulation occurs. At the same time, there are no loopholes left for certain companies to be outside the jurisdiction of the Federal Trade Commission.

□ 1630

We need to be consistent in our approach to privacy and focus on consumer-oriented enforcement. This approach has been the foundation not just of Silicon Valley, but innovators across the country; and the S.J. Res. 34 sets right the decades of innovation that has spurred job growth in the United States and greater online services for consumers.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I remind my friend, since he acknowledges the court decision does not allow FTC jurisdiction and that he wants to introduce a bill, perhaps the Republicans should have done that first, before scrapping the rules that leave ISPs with no rules.

Mr. Speaker, I yield 2 minutes to the gentlewoman from California (Ms. MATSUI).

Ms. MATSUI. Mr. Speaker, I rise in strong opposition to S.J. Res. 34. This is just the latest attempt from our Republican colleagues to use the Congressional Review Act to gut critical protections for American consumers.

The internet is increasingly intertwined with our daily lives, and nearly every American family uses the internet to access and share personal and sensitive information. The business we conduct online includes financial information, details about our medical history, and even information on our kids.

If this resolution of disapproval passes today, there will be no rules on the books to stop internet service providers from selling that browsing history without your permission. Because our Republican colleagues are using the Congressional Review Act to overturn these critical consumer protections, the FCC can't go back and write new rules in the future.

Despite what my colleagues on the other side of the aisle have said, the Federal Trade Commission cannot bring cases against broadband providers. That is why the FTC supported these rules when the FCC adopted them last year.

Even if you think the FCC did not get these rules right, this resolution effectively eliminates the FCC from ever acting to protect consumer privacy in the future. We should be working together to address any real shortcomings if these rules need to be fixed. That is not what the resolution before us will do.

Mr. Speaker, I urge my colleagues to vote against this damaging resolution.

Mr. FLORES. Mr. Speaker, I yield 2 minutes to the gentleman from New Jersey (Mr. LANCE).

Mr. LANCE. Mr. Speaker, I rise to support S.J. Res. 34, which seeks to halt agency overreach of the Federal Communications Commission concerning the way broadband internet service providers handle their customers' personal information.

The FCC's broadband privacy rule, a midnight regulation adopted by executive order in the waning days of the Obama administration, unnecessarily targets internet service providers and does very little to protect consumer privacy.

The rule adds costly and unnecessary innovation-stifling regulations to the internet and is another example of the Federal Government's picking winners and losers.

When passed, the FCC claimed that the rule would provide broadband customers meaningful choice, greater transparency, and strong security protections for their personal information collected by internet service providers.

In reality, the FCC's rules arbitrarily treat ISPs differently from the rest of the internet, creating a false sense of privacy.

Consumer data privacy is of significant concern to every American. The proper parties should address the issue. In this area, the Federal Trade Commission has historically held authority on the establishment and enforcement of general online privacy rules.

Repealing the FCC's privacy action is a critical step toward restoring a single, uniform set of privacy rules for the internet. This legislation puts all segments of the internet on equal footing and provides American consumers with a consistent set of privacy rules to permit the FCC and the FTC to continue to work to ensure consumer privacy through enforcement.

The FTC, the premier agency in this regard, has the experience to protect the privacy of the American people regarding the internet—at least 20 years of experience. Bifurcation between the FTC and the FCC is not productive. A good question to ask the FTC: Why did it wait until the last minute of the

Obama administration to promulgate its regulation?

Mr. Speaker, I believe it is important that we pass S.J. Res. 34, and I rise to ask all of my colleagues to support it.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I have heard about this last-minute dropping and late at night. Just for the other side's information, after a 7-month rulemaking process, this rule was adopted midday on October 26. So let's get the record straight.

Mr. Speaker, I yield 3 minutes to the gentleman from California (Mr. MCNERNEY).

Mr. MCNERNEY. Mr. Speaker, first, I thank Mr. DOYLE for his opposition to S.J. Res. 34. I rise in opposition as well.

The FCC's broadband privacy rules are commonsense rules. These rules give consumers the ability to choose how their information is used and shared by their internet service providers.

According to the Pew Research Center, a large majority of Americans say it is very important that they control who has access to their information. Despite a loud cry from the American people that they want to be able to choose how their information is used, S.J. Res. 34 strips consumers of the power to choose how their ISPs use and share their information.

This resolution also leaves consumers more vulnerable to attacks because their ISP will no longer be required to make reasonable steps to secure their personal information.

In recent years, we have seen numerous data breach incidents that have jeopardized consumers' personal information. Some examples are Yahoo, Target, Home Depot, LinkedIn, and Anthem. The list goes on.

Given the growing cyber threats that our Nation faces, it is critical that we do more, not less, to secure consumers' data. Strong data security practices are critical for protecting our consumers' confidentiality.

This resolution would make consumers' data more susceptible to being stolen and used for identity theft and other harmful unauthorized purposes.

Consumers want to be heard. They want more privacy. They want their information to be secure. We have an obligation to respond to their requests.

I am appalled that one of the Republicans' first acts in this Congress after trying to take health coverage away from 24 million people is to attack consumer protections and weaken data security. Americans are just now hearing about this legislation, and my phones are ringing off the hook in opposition.

I have to rhetorically ask the other side: Why are you pushing this?

Americans don't want it. Your voters are beginning to pay attention. This is just after your humiliating defeat with the ACA repeal. I ask that you withdraw this bill and start listening to your constituents.

Mr. Speaker, I urge my colleagues to reject S.J. Res. 34.

Mr. FLORES. Mr. Speaker, I yield 2 minutes to the gentleman from Louisiana (Mr. SCALISE), the GOP whip.

Mr. SCALISE. Mr. Speaker, I thank the gentleman from Texas for bringing forward this legislation.

The FTC's light touch in case-by-case enforcement had fostered an internet economy that has become the envy of the world, much to the benefit of all American families and consumers across this country.

But rather than following the FTC's proven framework of privacy protection, the FCC came in and overreached and missed the mark with these rules, injecting more regulation into the internet ecosystem. With all due respect, the internet was not broken and did not need the Federal Government to come in and try to fix it.

The bottom line is that families expect and deserve to be protected online with a set of robust and uniform privacy protections. These rules simply do not live up to that standard.

Rather than regulating based on the sensitivity of our data, these rules are applied unevenly, based on what type of company you are or what kind of technology you use.

Consumers should feel assured online that there is a cop on the beat with a track record of success, not an agency with a history of regulatory overreach. These midnight rules are harmful, inconsistent, and should be repealed.

Mr. Speaker, I urge my colleagues to adopt this important resolution.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, may I inquire how much time is remaining on both sides?

The SPEAKER pro tempore. The gentleman from Pennsylvania has 10¾ minutes remaining. The gentleman from Texas has 5 minutes remaining.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I remind the gentleman that these heavy-handed regulations that he speaks of are simply: ask permission, protect people's data, and tell them if it gets stolen.

That doesn't sound too heavy-handed to me.

Mr. Speaker, I yield 2 minutes to the gentleman from New York (Mr. TONKO).

Mr. TONKO. Mr. Speaker, I rise today in opposition to S.J. Res. 34, a bill that would strike most of the internet privacy guarantees protecting the American people today.

I have grave concerns with this effort. Our agenda here should be working on behalf of our constituents to protect their privacy and give them, not their service providers, data security. Instead, this effort would eviscerate any real online privacy protections and would limit data security.

Some of my colleagues have claimed that this commonsense rule has created challenges for consumers. I have found just the opposite. My office has been inundated with calls demanding that Congress protect their privacy and data security by opposing S.J. Res. 34. To everyone who has called, I hear you and I stand with you in opposing this harmful and misguided effort.

Back at home in New York's capital region, I have been hearing from many people who are frightened by the thought that S.J. Res. 34 will become law and the last shred of their online privacy will be lost forever.

They know how much information their internet service provider has mined from their search and browsing history, including financial, medical, and other very personal and sensitive details. They rightly believe that they should have a say in when that information can be bought and when it can be sold.

They understand that gutting these privacy protections would mean that internet service providers could sell their private information without their permission. It means their private internet browsing and search history, the text of their emails, and their mobile app usage can all be sold without their permission.

They have a right to control what they search for, their financial information, their health insurance, and information about their children. They have a right to protect their Social Security numbers and the contents of their emails. These rights are enshrined in our Constitution.

Privacy rules also require providers to use reasonable measures to protect consumers' personal information, a clear and commonsense standard that all who do business online should be required to uphold.

Finally, internet service providers must notify customers if hackers breach the system and may have access to their private data. With hackers from Russia and elsewhere running rampant across the net, this is a critical provision for our American families.

This is not too much to ask. The American people deserve to know that their data will be protected and that they will be notified if their data is compromised.

Mr. FLORES. Mr. Speaker, I yield 1½ minutes to the gentleman from Texas (Mr. OLSON).

Mr. OLSON. Mr. Speaker, I rise today in support of S.J. Res. 34, which will protect consumers and the future of internet innovation.

The internet is changing the way we communicate, shop, learn, and entertain. It is changing how we control our homes, our cars, and many other parts of our lives, including my two teenage kids. These changes give us certain expectations of privacy on the internet.

Until last year, the Federal Trade Commission provided a robust, consistent privacy framework for all companies in the internet services market. Their holistic and consistent approach struck the right balance. Consumers' use of internet services continues to increase and their privacy has been protected.

The resolution we are voting on today puts all segments of the internet on equal footing. It provides consumers with a consistent set of privacy rules.

Mr. Speaker, I urge my colleagues to vote for S.J. Res. 34.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I remind my friends once again that this does not put us on equal footing. The FTC has no power to regulate ISPs under current law.

Mr. Speaker, I yield 3 minutes to the gentleman from Massachusetts (Mr. CAPUANO).

□ 1645

Mr. CAPUANO. Mr. Speaker, we all know that our cell phones are tracking every move we make and keeping a record of it. Many people don't know, but your automobile is also doing the same thing. They keep a record of where you go. They keep a record of whether you wore your seatbelt. They keep a record of whether you applied the brakes or turned the turn signal on. Okay. That is your automobile. You don't have to drive.

Just recently, in the last couple months, we have learned that our televisions and children's dolls are doing the same thing. Last month, it was revealed that Vizio had spied on 11 million consumers by listening to them while their TV was off because they can do it.

Also, last month, a child's doll called My Friend Cayla for little girls or boys was banned in Germany—banned in Germany—because that doll listens and responds. It goes into the internet, and the doll's owner keeps and sells that information.

This month—this month—a teddy bear manufactured by a company called CloudPets was exposed for collecting more than 2 million voice recordings of children talking to their teddy bear.

Now, maybe we accept that. I know that those are not the items that this resolution would address, but the problem is you are taking an item for ISPs and reducing it down to this level. You say your privacy is protected. I just gave you three examples in the last 2 months where your privacy is not protected. Neither is your children's. Neither is your family's.

In 2012, a giant international company—international ISP company, by the way—filed for a U.S. patent for a cable box that would sit in your house. It would watch you. It would record you. It contained an infrared sensor and even take your body temperature with a thermographic—and that is a quote—thermographic camera. It would do all this without telling you and would work whether the cable box was on or not. If you don't believe me, if you still have the courage to go on the internet, go find patent application number—now, write this one down—2012/0304206. That is the patent application number. It is still online.

I want to read you one small segment from that 25-page patent application. This is a direct quote. I am not making up a single word. The device ''may detect . . . that two users are cuddling on a couch during the presentation of the television program and prior to an advertisement break. Based on the detected . . . action . . . the device would select a commercial associated with cuddling.''

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I yield an additional 30 seconds to the gentleman from Massachusetts.

Mr. CAPUANO. For example: ''a commercial for a romantic getaway vacation, a commercial for a contraceptive, a commercial for flowers . . . et cetera.''

I didn't make up a single word of what I just read, and every one of you is sitting there with your mouth open that this might happen in your world. That is what this resolution will allow, and you can't turn it off. You can't say: Don't watch my children. Don't watch my wife.

This is a terrible resolution. As I asked earlier today, what are you thinking?

Mr. FLORES. Mr. Speaker, we are thinking that the gentleman's comments do not pertain to this resolution, that this resolution in no way is going to allow any of the activities that were described, whether it is cuddling or anything that is going to get in the way of any of that or allowed to be sold.

Mr. Speaker, I yield 2 minutes to the gentleman from New York (Mr. COLLINS).

Mr. COLLINS of New York. Mr. Speaker, I would like to thank the people who worked to make this legislation a reality. As we become increasingly concerned with cyber threats, online privacy is a critical concern for every American.

Unfortunately, in October of last year, the FCC issued regulations titled, ''Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,'' also known as broadband privacy rules. These titles do not actually accurately reflect the impact these regulations are having on constituents' electronic privacy.

These broadband privacy rules took internet service providers, ISPs, which you subscribe to for TV and internet access, and edge providers that deliver online applications, services, and website content, and separated them into two different groups. This has caused confusion among businesses trying to adhere to this change.

While writing this regulation, the FCC had the opportunity to employ FTC precedent in drafting the broadband privacy rules, but instead chose to ignore existing precedent and create additional and onerous regulations. The FCC believed that these new rules would give consumers more choice and heightened transparency; however, this has not been the case.

This legislation does not remove privacy protections for consumers, and it does not expose consumer information. Both the FCC and the FTC will retain authority over consumer privacy on a case-by-case basis. ISPs will continue to be subject to the Communications Act of 1934, which protects all consumer proprietary network information. This is in addition to the many other existing Federal and State privacy rules that ISPs must continue to follow.

This proposed system, separating edge providers from ISPs, creates confusion for both consumers and business operations. This legislation works to reduce the confusion that has been created from this unnecessary regulation that has stifled competition and impeded innovation. I am happy to support this legislation which will provide much-needed clarity to the ongoing debate.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, may I inquire how much time remains on both sides?

The SPEAKER pro tempore. The gentleman from Pennsylvania has 5¼ minutes remaining. The gentleman from Texas has 2 minutes remaining.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I just remind my friend, you can say it as many times as you want, but the fact of the matter is that, under current law, the FTC has no authority to regulate the FCC, and the FCC Commissioner has said that you cannot do this without a rule in section 222.

I yield 1 minute to the gentlewoman from California (Ms. PELOSI), our House Democratic leader, the magic minute.

Ms. PELOSI. Mr. Speaker, on behalf of my five children and my nine grandchildren and everyone I know, as a matter of fact, I thank the gentleman for being a champion for privacy for the American people. I thank the gentleman from Pennsylvania (Mr. MICHAEL F. DOYLE) for his leadership. I thank the gentleman from New Jersey (Mr. PALLONE) for his leadership. The gentlewoman from California (Ms. ESHOO) has been a champion on this issue as well.

Mr. Speaker, Americans turn to the internet for so many things these days: buying books, filing taxes, learning about why they are feeling sick. The Republicans want this information to be sold without your permission: the websites you visit, the apps you use, your search history, the content of your emails, your health and financial data. Overwhelmingly, the American people do not agree with the Republicans that this information should be sold, and it certainly should not be sold without your permission.

Our broadband providers know deeply personal information about us and our families: where we are, what we want, what we are looking for, what information we want to know, every site we visit, and more. Our broadband providers can even track us when we are surfing in private, browsing in a private browsing mode.

Americans' private browser history should not be up for sale. Yet Republicans are bringing S.J. Res. 34 to the floor to allow internet service providers to profit—to profit; this is about profit—from America's most intimate personal information without our knowledge or our consent. Republicans' use of the Congressional Review Act will do permanent damage to the FCC's ability to keep Americans' personal information safe.

As FCC Commissioner Clyburn and FTC Commissioner McSweeny warned: ''This legislation will frustrate the FCC's''—the Federal Communications Commission's—''future efforts to protect the privacy of voice and broadband customers.''

It is important for our constituents to know that, if the Republicans had a problem with this particular policy, they might tweak it and say we don't like it this way or that in regular legislation so that we could have a debate on it. It could go back to the Federal Communications Commission. They could revise it and send it back if it were a legitimate presentation of concerns. But it is not about a legitimate presentation of concerns. It is about increasing profits at the expense of the privacy of the American people.

So, as I say, the Republicans' use of the Congressional Review Act does permanent damage and also damages the FCC's ability to keep America's personal information safe. With this measure, Republicans would destroy Americans' right to privacy on the internet—we made that clear—and forbid any effort to keep your personal information safe. Republicans are bending over backwards.

Think of it. Think of the context of all of this.

Since Gerald Ford was President, every candidate for President, every nominee of a major party, every candidate for President of the United States, Democrat and Republican, has released their income tax returns out of respect for the American people—out of respect for the American people. Week in and week out—in fact, sometimes day in and day out—in committee as well as on the floor, the Republicans have kept the President's income tax returns private when the public has a right to know that, that the public has always known that about every President since Gerald Ford—in fact, since Richard Nixon; although, in his case, it wasn't voluntary.

So while they are hiding President Trump's tax returns, some discrete piece of information that the public has a right to know, they are selling your most personal, selling your most personal and sensitive information—again, your browsing history, your children's location, everything—to anyone with the money to buy it.

Incognito tabs or private browsing modes will not protect you from the internet service providers watching and selling, as Mr. CAPUANO pointed out, watching and selling. Republicans have picked the week after Russian spies were caught hacking into half a billion American email accounts to open the floodgates, overturning the requirement that internet service providers keep their sensitive data secured from cybercriminals.

The American people deserve to be able to insist that intimate details and information about their browser history be kept private and secure.

So how is this?

We have this magnificent technology that science has made available to people to facilitate commerce, to learn about different subjects, to privately pursue, in a way that they may not even want their families to know, what symptoms they have and what illness that might tell them about.

Most Americans have no or limited choices for broadband providers and no recourse against these invasions of their privacy because, with this measure, Republicans turn their back on the overwhelming number of Americans who want more control over their internet privacy.

Americans can choose who represents them in Congress. Americans are paying close attention. They want to know who is taking a stand with them in opposing efforts to sell the private information of the American people.

This is staggering. This is almost a surrender. If the Republicans are allowed to do this, we have surrendered all thoughts of privacy for the American people.

Privacy is a value that the American people treasure. It is about their dignity. It is about their dignity. We cannot allow the Republicans to sell the dignity of the American people. I hope that everyone will vote ''no'' on this most unfortunate assault on the dignity of the American people.

□ 1700

Mr. FLORES. Mr. Speaker, I reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I yield 1 minute to the gentlewoman from Illinois (Ms. SCHAKOWSKY).

Ms. SCHAKOWSKY. Mr. Speaker, I thank the gentleman for yielding.

Last week, Republicans tried to take away your health care; and, today, they are trying to take away your privacy.

Republicans have said broadband providers and other internet companies should be under the same privacy rules. But oddly enough, when the committee considered an amendment to give the FTC, the Federal Trade Commission, rulemaking authority like the FCC, a change that would allow the agencies to adopt the same privacy protection, every single Republican voted no. In fact, Republicans proposed making it harder for the FTC to pursue privacy and data security cases.

The protections that the FCC adopted last year were very simple: consumers should know what data is being collected, opt in to sharing of sensitive data, have their data reasonably protected, and receive notice when their data is compromised. But this dangerous resolution puts America's privacy and data security at risk.

Mr. Speaker, I urge all of my colleagues to stand up for consumers and vote ''no.''

Mr. FLORES. Mr. Speaker, I continue to reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I yield 1 minute to the gentleman from Rhode Island (Mr. LANGEVIN).

Mr. LANGEVIN. Mr. Speaker, I thank the gentleman for yielding.

Mr. Speaker, I rise in strong opposition to this resolution of disapproval, which would repeal broadband privacy rules being implemented by the FCC.

As co-chair of the Congressional Cybersecurity Caucus, I hope I can offer some additional perspective on this debate. Studying the many threats our country faces in cyberspace, I have become deeply aware of how ingrained the internet is in every aspect of our lives and our economy. And that has also helped me understand the unique role of broadband service providers to grant access to the great potential of the Information Age.

By necessity, ISPs see every bit of traffic that leaves your network for the broader internet. Even when you use encryption, ISPs can still capture data about whom you are talking to or what sites you are visiting. These data are sensitive, and consumers have a right to decide whether or not they can be shared or monetized. Unfortunately, the resolution of disapproval under consideration would strip consumers of that right and presumptively allow sharing and selling without your permission.

Mr. Speaker, the resolution before us today that the Republicans have proposed is downright creepy. It is going to allow potentially unprecedented abuse of personal or private information be shared without your permission. This cannot stand. I urge my colleagues to oppose it.

Mr. FLORES. Mr. Speaker, I continue to reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, may I inquire how much time I have remaining?

The SPEAKER pro tempore. The gentleman from Pennsylvania has 2 minutes remaining. The gentleman from Texas has 2 minutes remaining.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I yield 1 minute to the gentlewoman from Florida (Mrs. DEMINGS).

Mrs. DEMINGS. Mr. Speaker, please stop me if you have heard this one before and know how it ends. My colleagues on the other side are once again trying to sell the American people a broken alternative to something that is working pretty much as it was intended to.

The FCC privacy rule just says that customers must opt in before internet

companies can sell their web browsing history, and that those companies must make reasonable efforts to protect customers' sensitive information. These are not unreasonable requirements.

The internet is our gateway to the world. Whether we connect through our mobile phone or our home computer, we pay companies for access. If those companies want to sell information about what we do on the internet, they should have to get our permission first. It is the right thing to do.

Mr. Speaker, I urge my colleagues on the other side to simply do the right thing.

Mr. FLORES. Mr. Speaker, I continue to reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I include in the RECORD letters from a coalition of small ISPs, a coalition of civil rights organizations, the Consumers Union, and an article by Terrell McSweeny all opposing this CRA.

ELECTRONIC FRONTIER FOUNDATION,
San Francisco, CA.

Re Oppose S.J. Res 34—Repeal of FCC Privacy Rules.

DEAR U.S. REPRESENTATIVES: We, the undersigned founders, executives, and employees of ISPs and networking companies, spend our working lives ensuring that Americans have high-quality, fast, reliable, and locally provided choices available when they need to connect to the Internet. One of the cornerstones of our businesses is respecting the privacy of our customers, and it is for that primary reason that we are writing to you today.

We urge Congress to preserve the FCC's Broadband Privacy Rules and vote down plans to abolish them. If the rules are repealed, large ISPs across America would resume spying on their customers, selling their data, and denying them a practical and informed choice in the matter.

Perhaps if there were a healthy, free, transparent, and competitive market for Internet services in this country, consumers could choose not to use those companies' products. But small ISPs like ours face many structural obstacles, and many Americans have very limited choices: a monopoly or duopoly on the wireline side, and a highly consolidated cellular market dominated by the same wireline firms.

Under those circumstances, the FCC's Broadband Privacy Rules are the only way that most Americans will retain the free market choice to browse the Web without being surveilled by the company they pay for an Internet connection.

Signed,

Sonic, MonkeyBrains, Cruzio Internet, Etheric Networks, Aeneas Communications, Digital Service Consultants Inc., Hoyos Consulting LLC, Om Networks, Motherlode Internet, Goldrush Internet, Credo Mobile, Andrew Buker (Director of Infrastructure Services & Research computing, University of Nebraska at Omaha), Tim Pozar (co-founder, TwoP LLC), Andrew Gallo (Senior Network Architect for a regional research and education network), Jim Deleskie (co-founder, Mimir networks), Randy Carpenter (VP, First Network Group), Kraig Beahn (CTO, Enguity Technology Corp).

JANUARY 27, 2017.

Hon. PAUL D. RYAN,
Speaker of the House, House of Representatives, Washington, DC.
Hon. MITCH MCCONNELL,
Senate Majority Leader, U.S. Senate, Washington, DC.
Hon. NANCY PELOSI,
Minority Leader, House of Representatives, Washington, DC.
Hon. CHARLES SCHUMER,
Minority Leader, U.S. Senate,
Washington, DC.

DEAR SPEAKER RYAN, SENATOR MCCONNELL, REPRESENTATIVE PELOSI, AND SENATOR SCHUMER: The undersigned media justice, consumer protection, civil liberties, and privacy groups strongly urge you to oppose the use of the Congressional Review Act (CRA) to adopt a Resolution of Disapproval overturning the FCC's broadband privacy order. That order implements the mandates in Section 222 of the 1996 Telecommunications Act, which an overwhelming, bipartisan majority of Congress enacted to protect telecommunications users' privacy. The cable, telecom, wireless, and advertising lobbies request for CRA intervention is just another industry attempt to overturn rules that empower users and give them a say in how their private information may be used.

Not satisfied with trying to appeal the rules of the agency, industry lobbyists have asked Congress to punish internet users by way of restraining the FCC, when all the agency did was implement Congress' own directive in the 1996 Act. This irresponsible, scorched-earth tactic is as harmful as it is hypocritical. If Congress were to take the industry up on its request, a Resolution of Disapproval could exempt intemet service providers (ISPs) from any and all privacy rules at the FCC. As you know, a successful CRA on the privacy rules could preclude the FCC from promulgating any ''substantially similar'' regulations in the future—in direct conflict with Congress' clear intention in Section 222 that telecommunications carriers protect their customers' privacy. It could also preclude the FCC from addressing any of the other issues in the privacy order like requiring data breach notification and from revisiting these issues as technology continues to evolve in the future. The true consequences of this revoked authority are apparent when considering the ISPs' other efforts to undermine the rules. Without these rules, ISPs could use and disclose customer information at will. The result could be extensive harm caused by breaches or misuse of data.

Broadband ISPs, by virtue of their position as gatekeepers to everything on the intemet, have a largely unencumbered view into their customers' online communications. That includes the websites they visit, the videos they watch, and the messages they send. Even when that traffic is encrypted, ISPs can gather vast troves of valuable information on their users' habits; but researchers have shown that much of the most sensitive information remains unencrypted.

The FCC's order simply restores people's control over their personal information and lets them choose the terms on which ISPs can use it, share it, or sell it. Americans are increasingly concerned about their privacy, and in some cases have begun to censor their online activity for fear their personal information may be compromised. Consumers have repeatedly expressed their desire for more privacy protections and their belief that the government helps ensure those protections are met. The FCC's rules give broadband customers confidence that their privacy and choices will be honored, but it does not in any way ban ISPs' ability to market to users who opt-in to receive any such targeted offers.

The ISPs' overreaction to the FCC's broadband privacy rules has been remarkable. Their supposed concerns about the rule are significantly overblown. Some broadband providers and trade associations inaccurately suggest that this rule is a full ban on data use and disclosure by ISPs, and from there complain that it will hamstring ISPs' ability to compete with other large advertising companies and platforms like Google and Facebook. To the contrary, ISPs can and likely will continue to be able to benefit from use and sharing of their customers' data, so long as those customers consent to such uses. The rules merely require the ISPs to obtain that informed consent.

The ISPs and their trade associations already have several petitions for reconsideration of the privacy rules before the FCC. Their petitions argue that the FCC should either adopt a ''Federal Trade Commission style'' approach to broadband privacy, or that it should retreat from the field and its statutory duty in favor of the Federal Trade Commission itself All of these suggestions are fatally flawed. Not only is the FCC well positioned to continue in its statutorily mandated role as the privacy watchdog for broadband telecom customers, it is the only agency able to do so. As the 9th Circuit recently decided in a case brought by AT&T, common carriers are entirely exempt from FTC jurisdiction, meaning that presently there is no privacy replacement for broadband customers waiting at the FTC if Congress disapproves the FCC's rules here.

This lays bare the true intent of these industry groups, who also went to the FCC asking for fine-tuning and reconsideration of the rules before they sent their CRA request. These groups now ask Congress to create a vacuum and to give ISPs carte blanche, with no privacy rules or enforcement in place. Without clear rules of the road under Section 222, broadband users will have no certainty about how their private information can be used and no protection against its abuse. ISPs could and would use and disclose consumer information at will, leading to extensive harm caused by breaches and by misuse of data properly belonging to consumers.

Congress told the FCC in 1996 to ensure that telecommunications carriers protect the information they collect about their customers. Industry groups now ask Congress to ignore the mandates in the Communications Act, enacted with strong bipartisan support, and overturn the FCC's attempts to implement Congress's word. The CRA is a blunt instrument and it is inappropriate in this instance, where rules clearly benefit internet users notwithstanding ISPs' disagreement with them.

We strongly urge you to oppose any resolution of disapproval that would overturn the FCC's broadband privacy rule.

Sincerely,

Access Now, American Civil Liberties Union, Broadband Alliance of Mendocino County, Center for Democracy and Technology, Center for Digital Democracy, Center for Media Justice, Color of Change, Consumer Action, Consumer Federation of America, Consumer Federation of California, Consumer Watchdog, Consumer's Union, Free Press Action Fund, May First/People Link, National Hispanic Media Coalition, New America's Open Technology Institute, Online Trust Alliance, Privacy Rights Clearing House, Public Knowledge.

CONSUMERSUNION®, POLICY & ACTION FROM CONSUMER REPORTS,
March 27, 2017.

HOUSE OF REPRESENTATIVES,
Washington, DC.

DEAR REPRESENTATIVE: Consumers Union, the policy and mobilization arm of Consumer

Reports, writes regarding House consideration of S.J. Res. 34, approved by a 50–48 party line vote in the Senate last week.

This resolution, if passed by the House and signed into law by President, would use the Congressional Review Act (CRA) to nullify the Federal Communication Commission's (FCC) newly-enacted broadband privacy rules that give consumers better control over their data. Many Senators cited ''consumer confusion'' as a reason to do away with the FCC's privacy rules, but we have seen no evidence proving this assertion and fail to understand how taking away increased privacy protections eliminates confusion. Therefore, we strongly oppose passage of this resolution—it would strip consumers of their privacy rights and, as we explain below, leave them with no protections at all. We urge you to vote no on S.J. Res. 34.

The FCC made history last October when it adopted consumer-friendly privacy rules that give consumers more control over how their information is collected by internet service providers (ISPs). Said another way, these rules permit consumers to decide when an ISP can collect a treasure trove of consumer information, whether it is a web browsing history or the apps a consumer may have on a smartphone. We believe the rules are simple, reasonable, and straightforward.

ISPs, by virtue of their position as gatekeepers to everything on the internet, enjoy a unique window into consumers' online activities. Data including websites consumers visit, videos viewed, and messages sent is very valuable. Small wonder, then, that ISPs are working so hard to have the FCC's new privacy rules thrown out through use of the Congressional Review Act. But we should make no mistake: abandoning the FCC's new privacy rules is about what benefits big cable companies and not about what is best for consumers.

Many argue the FCC should have the same privacy rules as those of the Federal Trade Commission (FTC). FCC Chairman Ajit Pai went so far as to say ''jurisdiction over broadband providers' privacy and data security practices should be returned to the FTC, the nation's expert agency with respect to these important subjects,'' even though the FTC currently possesses no jurisdiction over the vast majority of ISPs thanks to the common carrier exemption—an exemption made stricter by the Ninth Circuit Court of Appeals in last year's AT&T Mobility case. We have heard this flawed logic time and time again as one of the principal arguments for getting rid of the FCC's strong privacy rules. Unfortunately, this is such a poor solution that it amounts to no solution at all.

For the FTC to regain jurisdiction over the privacy practices of ISPs, the FCC would first have to scrap Title II reclassification—not an easy task which would be both time-consuming and subject to judicial review, and jeopardize the legal grounding of the 2015 Open Internet Order. Congress, in turn, would have to pass legislation to remove the common carrier exemption, thus granting the FTC jurisdiction over those ISPs who are common carriers. We are skeptical Congress would take such an action. Finally, the FTC does not enjoy the same robust rulemaking authority that the FCC does. As a result, consumers would have to wait for something bad to happen before the FTC would step in to remedy a violation of privacy rights. Any fondness for the FTC's approach to privacy is merely support for dramatically weaker privacy protections favored by most corporations.

There is no question that consumers favor the FCC's current broadband privacy rules. Consumers Union launched an online petition drive last month in support of the Commission's strong rules. To date, close to 50,000 consumers have signed the petition and the number is growing. Last week, more than 24,000 consumers contacted their Senators urging them to oppose the CRA resolution in the 24 hours leading up to the vote. Consumers care about privacy and want the strong privacy protections afforded to the them by the FCC. Any removal or watering down of those rules would represent the destruction of simple privacy protections for consumers.

Even worse, if this resolution is passed, using the Congressional Review Act here will prevent the FCC from adopting privacy rules—even weaker ones—to protect consumers in the future. Under the CRA, once a ride is erased, an agency cannot move forward with any ''substantially similar'' rule unless Congress enacts new legislation specifically authorizing it. Among other impacts, this means a bare majority in the Senate can void a rule, but then restoration of that rule is subject to full legislative process, including a filibuster. The CRA is a blunt instrument—and if used in this context, blatantly anti-consumer.

We are more than willing to work with you and your fellow Representatives to craft privacy legislation that affords consumer effective and easy-to-understand protections. The FCC made a step in that direction when it adopted the broadband privacy rules last year, and getting rid of them via the Congressional Review Act is a step back, not forward. Therefore, we encourage you to vote no on S.J. Res. 34.

Respectfully,

LAURA MACCLEERY,
Vice President, Consumer Policy & Mobilization, Consumer Reports.
KATIE MCINNIS,
Policy Counsel, Consumers Union.
JONATHAN SCHWANTES,
Senior Policy Counsel, Consumers Union.

[From wired.com, Mar. 22, 2017]

CONGRESS IS ABOUT TO GIVE AWAY YOUR ONLINE PRIVACY

(By Terrell McSweeney and Chris Hoofnagle)

The resolution that could come to a Congressional vote this week aims to tackle differences in how the FCC rule treats ISPs compared with other internet companies. Your broadband provider has to offer you a choice about what information it shares about you, but ecommerce sites and search engines do not.

Advocates for repealing the current protections—the resolution is sponsored by Senator Jeff Flake (R–AZ)—argue that Congress should void the FCC's rule using the Congressional Review Act. They contend that in order to properly govern privacy and avoid confusing consumers, the FCC should maintain consistent rules across the internet ecosystem. But inconsistent standards pervade privacy and consumer law. Furthermore, consistent standards militate in favor of increasing protections for privacy, rather than unraveling them as the current proposal would do.

An alphabet soup of state and federal laws set the privacy requirements for everything from our financial information to data about our children. That's largely because privacy is both essential to and sometimes in conflict with our most deeply held value, liberty. So, legislators have never been able to craft omnibus privacy protections. Instead, they've developed frameworks informed by prevailing norms, incentives, political economy, and ways the information might be used.

As we connect more devices in our home and on our bodies, the array of technologies that raise data privacy and security concerns is expanding. The privacy landscape will likely continue to be shaped as technologies evolve.

Different consumer technologies may justify different approaches. For example, the safety issues inherent in cars and medical devices may warrant particularly strong privacy and security protections. In the future, privacy rules could come from the FCC as well as the Department of Commerce, National Highway Traffic Safety Administration, Food and Drug Administration, and other agencies.

Consider that your bank can—and probably does—sell your contact and financial information unless you opt out. Yet if you rent a movie, online or off, the rental service can't sell information about your media consumption without your consent, and it must delete your rental history after it's no longer needed. Congress enacted those protections to shield intellectual freedom, so that one can enjoy controversial movies without fear of one's curiosity resulting in extortion or embarrassment.

This brings us to our second point: If consistency and reducing consumer confusion is the goal, consumers should demand stronger internet privacy norms. Given the animating purpose of protecting movie rental information, why not require consumers to consent to the sharing any information about their online behavior? After all, our web activity is the ultimate manifestation of our intellectual curiosity, representing second-by-second decisions about consuming news and entertainment.

In addition to existing federal laws, legislators could, as professor Helen Nissenbaum has suggested, look to offline contexts, such as the strong privacy norms governing searching for a book in a library, to guide the privacy rules we ought to enjoy when using a search engine. The government also could take a page from the confidentiality standards patients enjoy when conversing with physicians and apply those same norms to medical information websites. Policymakers could look to the last two centuries of privacy in the postal mail to guide rules for commercial scanning of email. Yet in all these contexts, web business models drive design decisions that have turned social and personal behaviors into marketplace transactions.

Left standing, the FCC rule offers an opportunity for a meaningful debate about how to better translate our analog privacy norms into the digital world. Broadband ISPs are essentially utilities, like postal mail and the telephone. Subscribers have little or no competitive choice as to which provider to use. ISPs know our identities, and their position gives them the technical capacity to surveil users in ways that others cannot. It makes sense to ensure consumers can choose whether to share data related to their Internet usage.

The majority of consumers—91 percent in a recent survey—feel they've lost control of their personal information. Yet, paradoxically, the late, great privacy researcher and historian Alan Westin consistently found that Americans expect companies to handle personal data in a ''confidential'' way. In reality, the modern internet is like a one-way mirror, where users are often unaware that they are being silently watched by third parties. The FCC rule exposes this one-way mirror and allows people to decide whether to draw a curtain on it.

Maintaining the current rules would make ISP practices more consistent with consumers' expectations of confidentiality. Congress should spend time examining the

strengths and weaknesses of our current approach, instead of using consistency arguments to eviscerate the FCC's rule.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I yield 1 minute to the gentlewoman from California (Ms. LOFGREN), my colleague from the class of '94.

Ms. LOFGREN. Mr. Speaker, a ''yes'' vote exempts all broadband service providers from all rules on user privacy and all limitations on how they use your data. They are in a unique position to see every place you go, every website you visit, they can do deep packet inspection and see what is in your emails.

What protects your privacy?

This rule that is about to be repealed.

If you have problems with the privacy policies of your email provider or social network, you have got competition to go to. But most Americans have just one or, at most, just two choices for their broadband provider. And, interestingly enough, all of those providers are supporting the repeal of this privacy rule.

Why?

They are going to make money selling your information.

The idea that we could have an FTC solution is an interesting one, but there is no way to do it. In the Ninth Circuit's 2016 ruling of AT&T v. FTC, they ruled that the FTC is barred from imposing data breach rules. So vote ''no'' and protect your constituents' privacy.

Mr. FLORES. Mr. Speaker, I continue to reserve the balance of my time.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, I ask my colleagues to vote against this horrible resolution, and I yield back the balance of my time.

Mr. FLORES. Mr. Speaker, I yield myself the balance of my time.

We have heard a lot of interesting claims today in the discussion about this fairly simple resolution to roll back overreaching regulation from the FCC that were passed late in the Obama administration's time.

I would remind everybody, Mr. Speaker, that this CRA has nothing to do with the President's tax return, it has nothing to do with Russian hacking, and there have been some gross mischaracterizations of what this resolution does.

Why do we need this resolution?

The three reasons are, as Chairwoman BLACKBURN opened up at the beginning:

First of all, the FCC swiped jurisdiction from the FTC.

Second, two cops on the beat create confusion among consumers and among the ISP providers.

Third, the FTC already has jurisdiction over this space.

Let me close with this: this resolution of disapproval only rescinds the FCC's rule, but it still provides the FCC the opportunity to provide more oversight more in line with the Federal Trade Commission, which has successfully been regulating online privacy for nearly 2 decades.

This resolution does not lessen or impede the privacy and data security standards that we already have established. We are simply restoring a more stable regulatory playing field to ensure that consistent uniform privacy standards are maintained to protect consumers and future innovation.

Once Congress rejects these rules, the FCC can turn back to cooperating with the FTC to ensure both the consumer privacy across all aspects of the internet is protected through vigorous enforcement and that innovation is allowed to flourish.

I urge all of my colleagues to support this commonsense resolution.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. All time for debate has expired.

Pursuant to the rule, the previous question is ordered on the joint resolution.

The question is on the third reading of the joint resolution.

The joint resolution was ordered to be read a third time, and was read the third time.

The SPEAKER pro tempore. The question is on the passage of the joint resolution.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. MICHAEL F. DOYLE of Pennsylvania. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this question will be postponed.

RAISING A QUESTION OF THE PRIVILEGES OF THE HOUSE

Ms. LOFGREN. Mr. Speaker, I rise to a question of the privileges of the House, and offer the resolution that was previously noticed.

The SPEAKER pro tempore. The Clerk will report the resolution.

The Clerk read as follows:

Expressing the sense of the House of Representatives that the President shall immediately disclose his tax return information to Congress and the American people.

Whereas, the Emoluments Clause was included in the U.S. Constitution for the express purpose of preventing federal officials from accepting any ''present, Emolument, Office, or Title . . . from any King, Prince, or foreign State'';

Whereas, in Federalist No. 22 (Alexander Hamilton) it is said, ''One of the weak sides of republics, among their numerous advantages, is that they afford too easy an inlet to foreign corruption,'' and;

Whereas, the delegates to the Constitutional Convention specifically designed the Emoluments Clause as an antidote to potentially corrupting foreign practices of a kind that the Framers had observed during the period of the Confederation, and;

Whereas, Article 1, section 9, clause 8 of the Constitution states: ''no person holding any office of profit or trust . . . shall, without the consent of the Congress, accept of any present, Emolument, Office, or Title of any kind whatever, from any King, Prince, or foreign State'', and;

Whereas, in 2009, the Office of Legal Counsel clarified that corporations owned or controlled by foreign governments presumptively qualify as foreign States under the foreign Emoluments Clause, and;

Whereas, the word ''emoluments'' means profit, salary, fees, or compensation which would include direct payment, as well as other benefits, including extension of credit, forgiveness of debt, or the granting of rights of pecuniary value, and;

Whereas, according to The New Yorker, in 2012, The Trump Organization entered into a deal with Ziya Mammadov to build the Trump Tower Baku in the notoriously corrupt country Azerbaijan in possible violation of the Foreign Corrupt Practices Act and, by profiting from business with the Mammadov family, due to their financial entanglements with the Iran Revolutionary Guard may have also violated the Emoluments Clause if income from this project continues to flow to The Trump Organization, and;

Whereas, The Trump Organization has deals in Turkey, admitted by the President himself during a 2015 Brietbart interview, and when the President announced his travel ban, Turkey's President called for President Trump's name to be removed from Trump Towers Istanbul, according to The Wall Street Journal, and President Trump's company is currently involved in major licensing deals for that property which may implicate the Emoluments Clause, and;

Whereas, shortly after election, the President met with the former U.K. Independence Party leader, Nigel Farage, to get help to stop obstructions of the view from one of his golf resorts in Scotland, and according to The New York Times, both of the resorts he owns there are promoted by Scotland's official tourism agency, a benefit that may violate the Emoluments Clause, and;

Whereas, at Trump Tower in New York, the Industrial and Commercial Bank of China is a large tenant, according to Bloomberg; the United Arab Emirates leases space, according to the Abu Dhabi Tourism & Culture Authority; and the Saudi Mission to the U.N. makes annual payments, according to the New York Daily News, and money from these foreign countries goes to the President, and;

Whereas, according to NPR, in February China gave provisional approval for 38 new trademarks for The Trump Organization, which have been sought for a decade to no avail, until President Trump won the election. This is a benefit the Chinese Government gave to the President's businesses in possible violation of the Emoluments Clause, and;

Whereas, the President is part owner of a New York building carrying a $950 million loan, partially held by the Bank of China, according to The New York Times, when owing the Government of China by the extension of loans and credits by a foreign State to an officer of the United States would violate the Emoluments Clause, and;

Whereas, NPR reported that the Embassy of Kuwait held its 600 guest National Day celebration at Trump Hotel in Washington, D.C., last month, proceeds to Trump, and;

Whereas, according to The Washington Post, the Trump International Hotel in Washington, D.C., has hired a ''director of diplomatic sales'' to generate high-priced business among foreign leaders and diplomatic delegations, and;

Whereas, according to his 2016 candidate filing with the Federal Election Commission, the President has 564 financial positions in