I thank the majority for advancing this bill, and I look forward to working with them to advance similar legislation.

I reserve the balance of my time.

Mr. LAMBORN. Mr. Speaker, I yield such time as he may consume to the gentleman from Georgia (Mr. CARTER).

Mr. CARTER of Georgia. I thank the gentleman for yielding.

Mr. Speaker, the First Congressional District of Georgia includes all 100 miles of Georgia's coastline and barrier islands. It was on one of these islands that the founder of Georgia, General James Oglethorpe, built a fort in 1736 to protect the new British Colony from the Spaniards. He named the fort and nearby town ''Frederica'' in honor of the Prince of Wales. In 1742, Fort Frederica's strategic location helped the British win a decisive victory against the Spanish in the Battle of Bloody Marsh. After this battle, the Spanish abandoned their attempts to take over the territory, and Georgia was fully secured as a British Colony. Today, Fort Frederica National Monument is a popular destination in Glynn County, featuring portions of the original fort, a museum, and extensive hiking trails.

H.R. 494 would allow for a small addition of adjacent land that contains artifacts from prehistoric human settlements. With this addition, visitors will be able to see a more complete story of the history of Georgia—from its earliest human residents, to colonial times, to modern day.

I thank the chairman for his consideration of this bill, and I thank the Natural Resources Committee's staff for its efforts. I also thank the entire Georgia delegation for supporting and cosponsoring this legislation.

Mr. POLIS. Mr. Speaker, I thank my colleagues for advancing this bill. I look forward to working with them to advance similar legislation that expands, protects, and enhances our public lands. It is particularly a privilege for me to work on a bill that uses resources and that highlights for the American people the value of the Land and Water Conservation Fund.

I urge a ''yes'' vote.

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

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

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Colorado (Mr. LAMBORN) that the House suspend the rules and pass the bill, H.R. 494.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

□ 1730

## EMAIL PRIVACY ACT

Mr. YODER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 387) to amend title 18, United States Code, to update the privacy protections for electronic communications information that is stored by third-party service providers in order to protect consumer privacy interests while meeting law enforcement needs, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 387

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE.**

This Act may be cited as the ''Email Privacy Act''.

**SEC. 2. VOLUNTARY DISCLOSURE CORRECTIONS.**

(a) IN GENERAL.—Section 2702 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by striking ''while in electronic storage by that service'' and inserting ''that is in electronic storage with or otherwise stored, held, or maintained by that service'';

(B) in paragraph (2)—

(i) by striking ''to the public'';

(ii) by striking ''divulge'' and inserting ''disclose''; and

(iii) by striking ''which is carried or maintained on that service'' and inserting ''that is stored, held, or maintained by that service''; and

(C) in paragraph (3)—

(i) by striking ''divulge'' and inserting ''disclose''; and

(ii) by striking ''a provider of'' and inserting ''a person or entity providing'';

(2) in subsection (b)—

(A) in the matter preceding paragraph (1), by inserting ''wire or electronic'' before ''communication'';

(B) by amending paragraph (1) to read as follows:

''(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication, or to an agent of such addressee, intended recipient, subscriber, or customer;''; and

(C) by amending paragraph (3) to read as follows:

''(3) with the lawful consent of the originator, addressee, or intended recipient of such communication, or of the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication;'';

(3) in subsection (c) by inserting ''wire or electronic'' before ''communications'';

(4) in each of subsections (b) and (c), by striking ''divulge'' and inserting ''disclose''; and

(5) in subsection (c), by amending paragraph (2) to read as follows:

''(2) with the lawful consent of the subscriber or customer;''.

**SEC. 3. AMENDMENTS TO REQUIRED DISCLOSURE SECTION.**

Section 2703 of title 18, United States Code, is amended—

(1) by striking subsections (a) through (c) and inserting the following:

''(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by that service only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

''(1) is issued by a court of competent jurisdiction; and

''(2) may indicate the date by which the provider must make the disclosure to the governmental entity.

In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.

''(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—

''(1) IN GENERAL.—Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of remote computing service of the contents of a wire or electronic communication that is stored, held, or maintained by that service only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

''(A) is issued by a court of competent jurisdiction; and

''(B) may indicate the date by which the provider must make the disclosure to the governmental entity.

In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.

''(2) APPLICABILITY.—Paragraph (1) is applicable with respect to any wire or electronic communication that is stored, held, or maintained by the provider—

''(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communication received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

''(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

''(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—

''(1) IN GENERAL.—Except as provided in subsections (i) and (j), a governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of a record or other information pertaining to a subscriber to or customer of such service (not including the contents of wire or electronic communications), only—

''(A) if a governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that—

''(i) is issued by a court of competent jurisdiction directing the disclosure; and

''(ii) may indicate the date by which the provider must make the disclosure to the governmental entity;

''(B) if a governmental entity obtains a court order directing the disclosure under subsection (d);

''(C) with the lawful consent of the subscriber or customer; or

''(D) as otherwise authorized in paragraph (2).

''(2) SUBSCRIBER OR CUSTOMER INFORMATION.—A provider of electronic communication service or remote computing service shall, in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means available under paragraph (1), disclose to a governmental entity the—

''(A) name;

''(B) address;

''(C) local and long distance telephone connection records, or records of session times and durations;

''(D) length of service (including start date) and types of service used;

''(E) telephone or instrument number or other subscriber or customer number or identity, including any temporarily assigned network address; and

''(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber or customer of such service.

''(3) NOTICE NOT REQUIRED.—A governmental entity that receives records or information under this subsection is not required to provide notice to a subscriber or customer.'';

(2) in subsection (d)—

(A) by striking ''(b) or'';

(B) by striking ''the contents of a wire or electronic communication, or'';

(C) by striking ''sought,'' and inserting ''sought''; and

(D) by striking ''section'' and inserting ''subsection''; and

(3) by adding at the end the following:

''(h) NOTICE.—Except as provided in section 2705, a provider of electronic communication service or remote computing service may notify a subscriber or customer of a receipt of a warrant, court order, subpoena, or request under subsection (a), (b), (c), or (d) of this section.

''(i) RULE OF CONSTRUCTION RELATED TO LEGAL PROCESS.—Nothing in this section or in section 2702 shall limit the authority of a governmental entity to use an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction to—

''(1) require an originator, addressee, or intended recipient of a wire or electronic communication to disclose a wire or electronic communication (including the contents of that communication) to the governmental entity;

''(2) require a person or entity that provides an electronic communication service to the officers, directors, employees, or agents of the person or entity (for the purpose of carrying out their duties) to disclose a wire or electronic communication (including the contents of that communication) to or from the person or entity itself or to or from an officer, director, employee, or agent of the entity to a governmental entity, if the wire or electronic communication is stored, held, or maintained on an electronic communications system owned, operated, or controlled by the person or entity; or

''(3) require a person or entity that provides a remote computing service or electronic communication service to disclose a wire or electronic communication (including the contents of that communication) that advertises or promotes a product or service and that has been made readily accessible to the general public.

''(j) RULE OF CONSTRUCTION RELATED TO CONGRESSIONAL SUBPOENAS.—Nothing in this section or in section 2702 shall limit the power of inquiry vested in the Congress by article I of the Constitution of the United States, including the authority to compel the production of a wire or electronic communication (including the contents of a wire or electronic communication) that is stored, held, or maintained by a person or entity that provides remote computing service or electronic communication service.''.

**SEC. 4. DELAYED NOTICE.**

Section 2705 of title 18, United States Code, is amended to read as follows:

**''§ 2705. Delayed notice**

''(a) IN GENERAL.—A governmental entity acting under section 2703 may apply to a court for an order directing a provider of electronic communication service or remote computing service to which a warrant, order, subpoena, or other directive under section 2703 is directed not to notify any other person of the existence of the warrant, order, subpoena, or other directive.

''(b) DETERMINATION.—A court shall grant a request for an order made under subsection (a) for delayed notification of up to 180 days if the court determines that there is reason to believe that notification of the existence of the warrant, order, subpoena, or other directive will likely result in—

''(1) endangering the life or physical safety of an individual;

''(2) flight from prosecution;

''(3) destruction of or tampering with evidence;

''(4) intimidation of potential witnesses; or

''(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

''(c) EXTENSION.—Upon request by a governmental entity, a court may grant one or more extensions, for periods of up to 180 days each, of an order granted in accordance with subsection (b).''.

**SEC. 5. RULE OF CONSTRUCTION.**

Nothing in this Act or an amendment made by this Act shall be construed to preclude the acquisition by the United States Government of—

(1) the contents of a wire or electronic communication pursuant to other lawful authorities, including the authorities under chapter 119 of title 18 (commonly known as the ''Wiretap Act''), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act; or

(2) records or other information relating to a subscriber or customer of any electronic communication service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18 (commonly known as the ''Wiretap Act''), or any other provision of Federal law not specifically amended by this Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kansas (Mr. YODER) and the gentleman from Michigan (Mr. CONYERS) each will control 20 minutes.

The Chair recognizes the gentleman from Kansas.

GENERAL LEAVE

Mr. YODER. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and to include any extraneous material on H.R. 387, currently under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Kansas?

There was no objection.

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

Thank you for this opportunity to have this very important debate on a critical piece of legislation that has been a long time in the coming. I thank the chairman of the Judiciary Committee, Representative GOODLATTE, and Ranking Member CONYERS for their work and leadership in shepherding this bill through the process and getting us to this moment on the floor today. I thank my colleague, Mr. POLIS, for cosponsoring this legislation and working so tirelessly over the past few years.

I think we originally introduced this bill back in 2013, and it takes a while sometimes for a good idea to reach this point in Congress, Mr. Speaker, and this is an idea whose time has come. So I rise today to support these long overdue, bipartisan ideas in this legislation that will bring our digital privacy laws into the 21st century.

Mr. Speaker, the year was 1986. We can all try to think back where we were in 1986. I am sure Kentucky had a good basketball team back then. I know Kansas did. I was 10 years old, hoping to get a new Nintendo game console for Christmas so I could play Super Mario Brothers. You could buy a ticket to see Top Gun for $2.75. In the tech world, 1986 marked the debut of the first laptop computer. It was 12 pounds. A mobile phone was the size of a small pet.

Mr. Speaker, it was also the year in which Congress passed the Electronic Communication Privacy Act. Now, this law, at the time, there were only 10 million email users worldwide. Most of us probably didn't have email at that time. Most Americans didn't for sure. Now, today, 232 million Americans send an email at least once per month. The first text message wouldn't be sent for another 6 years, and now Americans send more than a billion texts each year.

Mr. Speaker, the times and technologies have changed, but the laws have not kept pace. Federal laws regarding how we treat and protect the privacy of digital communications have been unchanged since 1986 and, because of it, our digital content is not afforded the same Fourth Amendment protections as our paper documents on our desks in our home.

Now, the Fourth Amendment protects the ''right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.'' Yet when it comes to what is on Americans' cell phones, their home computers, what might be in the cloud, or on their business computer, whatever it is, our laws allow Federal agencies like the IRS, the SEC, or law enforcement to kick down their virtual doors and search an innocent American's private communications and data storage without a warrant, without probable cause or any type of due process.

Now, many Americans take great precautions to protect and store their digital communications on services

like Dropbox, for example, or an iCloud. Yet our Federal laws perversely treat that data storage as if somehow that data has been abandoned by its owner and, therefore, that data loses its constitutional protection.

Well, in 1986, Mr. Speaker, lawmakers believed within reason that individuals and families wouldn't store mass amounts of data online. They wouldn't leave their Gmail stored online. They might have their own servers, or they would delete the emails or delete the data.

Therefore, if an individual actually left information on a third-party storage, it was akin to that person leaving their documents in a garbage can at the end of their driveway, therefore, voiding its Fourth Amendment protections. Thus, that individual had no reasonable expectation of privacy in regards to that email under the Fourth Amendment.

As we all know, virtually everyone now stores millions of emails and tons of gigabytes of data and other personal items on third-party servers. Those emails contain pictures and videos of our kids, our business transactions, our most sensitive information that the government shouldn't have access to without a warrant, without due process as required by the Constitution of the United States.

Establishing these privacy protections are critical for both ensuring that American's rights are protected, but also, Mr. Speaker, ensuring that companies that do business in America know that they can ensure their customers that if they store with them, they can protect it; that that information won't be intruded upon or searched and seized without due process of law, without their permission, without the government proving that they have a need for that information and protecting individuals' rights.

We ensure that cloud computer services are covered by the same warranty for content requirements and that all data is treated as if it is paper documents given our law modernization that is desperately needed.

In addition to updating our constitutional rights, these privacy protections do create business certainty, making sure consumers will be happy to continue to use cloud storage services.

Mr. Speaker, fundamentally, these changes in my bill codify the Sixth Circuit's decision in U.S. v. Warshak, which held that email content is protected by the Fourth Amendment. A decision which, while important, needs to be enshrined in law as it only currently applies in the Sixth Circuit. It must be applied nationwide.

Mr. Speaker, today we can cast a unifying vote in these divided times. We so desperately want to find points of bipartisanship and collegiality and to tell the American people that this Congress, this government is doing great things to help protect Americans' rights and to help modernize our laws in a way that is consistent with how we communicate today.

I thank my colleagues on the left side of the aisle for their strong work and strong support. This is a unifying bill. It passed the House last year 419–0. So it is the type of thing that is great policy coming out of the Judiciary Committee. I look forward to seeing it pass again on the floor later today.

So, Mr. Speaker, we can send a unifying vote and a unifying message to the American people today. We can dispel the myth that Congress doesn't work together, and we can send a strong message to the American people that their privacy matters.

I urge passage.

I reserve the balance of my time.

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

In 2014, in a unanimous ruling delivered by Chief Justice Roberts, the Supreme Court concluded that the police may not search a cell phone without first demonstrating probable cause.

Citing an obvious Fourth Amendment interest—namely, the right to be free from unreasonable search and seizure—in the vast amount of data we store on our personal devices, the Court wrote:

''The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.''

With that decision, the Court took a bold step toward reconciling the Fourth Amendment with the advent of modern communications technology.

Today the House takes a similar step to reconcile our interests in privacy and due process with the realities of modern computing. We do so for the second time.

H.R. 387, the Email Privacy Act, recognizes that the content of our communications, although often stored in digital format, remains worthy of Fourth Amendment protection. And to investigators and government agents who seek access to our email, our advice is rather simple: get a warrant.

It is an idea whose time has long since come. So this bill will allow us to move to a clear, uniform standard for law enforcement agencies to access the content of our communications; namely, a warrant based on probable cause.

H.R. 387 also codifies the right of the providers to give notice of this intrusion to their customers, except in certain exigent circumstances that must be also validated by the court.

We should note the absence of a special carve-out from the warrant requirement for the civil agencies, like the Securities and Exchange Commission and the Internal Revenue Service.

Last Congress, in the Judiciary Committee, we reached quick consensus that a civil carve-out of any kind is unworkable, unconstitutional, or maybe both. I would have preferred to keep the notice provisions of the original bill, which are absent from the version we reported from committee.

In the digital world, no amount of due diligence necessarily tells us that the government accessed our electronic information. The government should have an obligation to provide us with some form of notice when intruding on a record of our most private conversations.

I fully understand that not everyone shares this view, and I am willing to compromise, for now, in order to advance the important reforms that we will adopt today.

I am proud of the work we have done. Last Congress, the House passed this legislation that has already been noted by 419–0. I hope that today we can send our colleagues in the Senate a similarly strong signal to pass this bill.

This legislation is several years in the making, and it should not be delayed any further.

Accordingly, I urge my colleagues to support H.R. 387, the Email Privacy Act.

I reserve the balance of my time.

The SPEAKER pro tempore. Without objection, the gentleman from Virginia (Mr. GOODLATTE) will control the time of the majority.

There was no objection.

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

Today, the House of Representatives will again vote to approve legislation that reforms and modernizes the Electronic Communications Privacy Act or ECPA. Last year, identical legislation passed with unanimous bipartisan support by a vote of 419–0.

Reforming ECPA has been a top priority for me as chairman of the Judiciary Committee. I have worked with Members of Congress, advocacy groups, and law enforcement agencies for years on many complicated nuances involved in updating this law.

The resulting bill is a carefully negotiated agreement to update the procedures governing government access to stored communications content and records.

Thirty years ago, when personal computing was still in its infancy and few of us had ever heard of something called the world wide web, Congress enacted ECPA to establish procedures that strike a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.

In 1986, mail was sent through the U.S. Postal Service, a search engine was called a library, and clouds were found only in the sky. In 1986, computer storage was finite and expensive. It was unheard of that a commercial product would allow users to send and receive electronic communications around the globe for free and store those communications for years with a third-party provider.

So much has changed in the last three decades. The technology explosion of the last three decades has

placed a great deal of information on the internet, in our emails, and on the cloud. Today, commercial providers, businesses, schools, and governments of all shapes and sizes provide email and cloud computing services to customers, students, and employees.

□ 1745

The Email Privacy Act establishes for the first time in Federal statute a uniform warrant requirement for stored communication content in criminal investigations, regardless of the type of service provided, the age of an email, or whether the email has been opened.

The bill preserves the authority for law enforcement agents to serve the warrant on the provider because, as with any other third-party custodian, the information sought is stored with them. However, the bill acknowledges that providers may give notice to their customers when in receipt of a warrant, court order, or subpoena, unless the provider is court-ordered to delay such notification.

The bill continues current practice that delineates which remote computing service providers, or cloud providers, are subject to the warrant requirement for content in a criminal investigation.

ECPA has traditionally imposed heightened legal process and procedures to obtain information for which the customer has a reasonable expectation of privacy, namely, emails, texts, photos, videos, and documents stored in the cloud. H.R. 387 preserves this treatment by maintaining in the statute limiting language regarding remote computing services.

Contrary to practice 30 years ago, today, vast amounts of private, sensitive information are transmitted and stored electronically. But this information may also contain evidence of a crime, and law enforcement agencies are increasingly dependent upon stored communications content and records in their investigations.

To facilitate timely disclosure of evidence to law enforcement, the bill authorizes a court to require a date for return of service of the warrant. In the absence of such a requirement, H.R. 387 requires email and cloud providers to promptly respond to warrants for communications content.

Current law makes no distinction between content disclosed to the public, like an advertisement on a website, versus content disclosed only to one or a handful of persons, like an email or text message. The result is that law enforcement could be required to obtain a warrant even for publicly disclosed content. The bill clarifies that commercial public content can be obtained with process other than a warrant.

Lastly, H.R. 387 clarifies that nothing in the law limits Congress' authority to compel a third-party provider to disclose content in furtherance of its investigative and oversight responsibilities.

Thirty years ago, the extent to which people communicated electronically was much more limited. Today, however, the ubiquity of electronic communications requires Congress to ensure that legitimate expectations of privacy are protected, while respecting the needs of law enforcement. I am confident that this bill strikes the necessary balance and does so in a way that continues to promote the development and use of new technologies and services that reflect how people communicate with one another today and in the future.

I would like to thank Congressman YODER and Congressman POLIS for introducing the underlying legislation.

It is my hope that today the House will once again approve this legislation that embodies the principles of the Fourth Amendment and reaffirms our commitment to protecting the privacy interests of the American people without unduly sacrificing public safety. I urge my colleagues to support this bipartisan legislation.

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

Mr. CONYERS. Mr. Speaker, when the gentleman from New York (Mr. NADLER) was chairman of the Constitution, Civil Rights, and Civil Liberties Subcommittee in 2010, he held three hearings on various aspects of ECPA, including the need for a warrant requirement.

I yield 3 minutes to the gentleman from New York (Mr. NADLER).

Mr. NADLER. Mr. Speaker, I rise in strong support of H.R. 387, the Email Privacy Act. I am proud to be an original cosponsor of this legislation, which will provide a critical update to the privacy laws governing electronic communications.

The Electronic Communications Privacy Act, or ECPA as it is known, was enacted in 1986. It was an attempt to reestablish a balance between privacy and law enforcement needs at a time when personal and business computing was becoming more commonplace. Over the last 30 years, however, we have seen a revolution in communications technology, and what might have made sense in 1986 is vastly out of date today.

New technologies, including cloud computing, social networking, and location-based services, have rendered many of the law's provisions outdated, vague, or inapplicable to emerging innovations. For example, even a single email is potentially subject to multiple different legal standards under current law.

In 2009 and 2010, when I was the chairman of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, we held multiple hearings to consider reforms to our Nation's electronic and privacy laws. This work culminated in the Electronic Communications Privacy Act Modernization Act of 2012, a bill I introduced along with Ranking Member CONYERS requiring law enforcement to obtain a warrant based on probable cause before searching emails. That approach, now embodied in the Yoder-Polis Email Privacy Act, is what we are here today to consider.

In an era in which government access to an individual's private information held by third-party providers has become far too easy, this legislation will finally update our laws to reflect our new understanding of what it means, in the words of the Fourth Amendment, for ''people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.''

Clarifying the laws will also help industry stakeholders who currently struggle to apply the existing, outdated categories of information to their products and services, and it will provide a clear standard for law enforcement.

This bill is not perfect and, clearly, there is more to be done. In particular, we must keep working to require a probable cause warrant for location information. However, this bill is an important step forward toward ensuring that our laws strike the right balance between the interests and needs of law enforcement and the privacy rights of the American people. I urge my colleagues to support it.

I congratulate all those involved in its development.

Mr. GOODLATTE. Mr. Speaker, I yield such time as he may consume to the gentleman from Minnesota (Mr. EMMER).

Mr. EMMER. Mr. Speaker, the American people's Fourth Amendment right against unreasonable search and seizure by our government must always be protected. Unfortunately, our privacy protections from government intrusion have not kept pace with the way we communicate with each other. It is long past time that we update our Nation's electronic communication privacy laws.

The last time we updated these laws was 1986. That was 6 years after the U.S. Olympic Hockey team's Miracle on Ice, 2 years after I graduated from college, and 1 year before the Minnesota Twins won their first World Series. Simply put, Mr. Speaker, that was a long time ago.

Today, more than 200 million Americans have access to a smartphone, and many more use email and cloud technology. However, many Americans may not realize that these antiquated laws allow law enforcement to read every email that is more than 6 months old, without a warrant.

The Email Privacy Act would codify the reasonable expectation of privacy Americans already have in their electronic communications by requiring a search warrant for private digital communications.

I was pleased to support this legislation when it passed unanimously in the House last Congress, and I look forward to its swift consideration in both Chambers in the 115th. I urge all of my

colleagues to support this long overdue modification of the law.

Mr. CONYERS. Mr. Speaker, I yield 4 minutes to the gentleman from Colorado (Mr. POLIS), a former member of the Judiciary Committee and the lead Democratic sponsor of this bill.

Mr. POLIS. Mr. Speaker, the passage of the Email Privacy Act is long overdue. The fact that the law that governs the government access to emails dates from 1986, before email was really a mass phenomena, is a glaring loophole in our privacy protection laws.

1986 was a time when we used floppy disks to store our information, when, if any internet existed at all, it was just a few people at research universities communicating with another. It was far from a mass phenomena.

Today, this bill catches up with the reasonable expectation that consumers already have that their emails are private. Just as Americans view their phone conversations as private, their physical letters through the mail private, Americans view their emails the same way. Yet, until we close this loophole, the government maintains access, without a warrant, to emails that are older than 6 months in a way that they do not allow access to your old personal letters filed away in a filing cabinet in your office. They don't allow access to old voice mails, and emails are, frankly, no different.

The Email Privacy Act requires that Americans have the same legal protection for our emails as we do for paper letters, faxes, and other types of communication that may remain sitting around. Updating this law simply aligns the law to the digital and physical world. It has taken too long already. Today is a major step forward.

I would like to highlight the House has already passed this bill unanimously last session. How rare it is not just Democrats and Republicans coming together, not just Chairman GOODLATTE and Ranking Member CONYERS, but every single Democrat and Republican coming together, Mr. Speaker. That is rare, and yet this body has spoken overwhelmingly last session and I hope will speak overwhelmingly again today to encourage the Senate to promptly bring up this bill and pass it into law.

This bill is a strong victory for bipartisanship. This bill has been one of the most popular bills in the entire Congress. I am proud to say, as the lead Democrat, this bill had 314 cosponsors last Congress and passed unanimously.

Back when Congress passed the Electronic Communications Privacy Act in 1986, it is fair to say that electronic communications meant something different than it means today. Thirty years ago, modern email simply didn't exist. And today, with 24/7 accessibility, accessibility on our smart devices, in our homes, everywhere else, it has been estimated that there were 205 billion emails sent each day by Americans. Those emails contain private communications for millions of us, and they deserve the same right of privacy as the letters in your file cabinet or your desk.

You often hear Members talk about commonsense bills. Well, this bill really defines common sense. When you read our bill, there is nothing more common sense than the Email Privacy Act, which is why the bill passed 419–0 last Congress. Unfortunately, the bill didn't make it to a Senate Judiciary Committee vote, which is why I am so thrilled that Chairman GOODLATTE and Mr. CONYERS have succeeded in having Mr. MCCARTHY and Speaker RYAN bring this bill forward so early this session, giving the Senate a chance to act.

I want to thank my colleague, Mr. YODER, for his hard work as the lead sponsor on this bill. I remember he and I, in gathering floor sponsors, would have these friendly contests of who could get more, Democrats or Republicans. That is how popular this bill was in terms of gaining 314 cosponsors, more than any other bill in the House of Representatives at that time.

I urge my colleagues to vote ''yes'' on this bill. Send a strong message to the Senate to vote immediately on the Email Privacy Act. Tell the Senate it is time to stand up for the privacy of Americans. This bill must be passed. I urge my colleagues to vote ''yes.''

Mr. CONYERS. Mr. Speaker, I have no further speakers.

I yield back the balance of my time.

Mr. GOODLATTE. Mr. Speaker, I urge my colleagues to vote for this good legislation.

I yield back the balance of my time.

Mr. SWALWELL of California. Mr. Speaker, I rise in support of H.R. 387, the Email Privacy Act.

As I said last Congress, current law is woefully out of date when it comes to protecting privacy in electronic communications. I support H.R. 387, just as I supported the same legislation previously, because it is long past time we afforded Americans the privacy they are due online.

At the same time, I am disappointed this bill has come straight to the Floor, and not through the Judiciary Committee, a committee on which I sit. Nor are any Members able to offer amendments on the Floor. Going through the committee process and allowing amendments on the Floor would have enabled us to address some of the concerns raised by law enforcement about H.R. 387, such as its view that the bill fails to enable personnel to expediently obtain critical evidence. As a former prosecutor I share its interest in making sure that while we improve privacy protections we do not impede the ability to bring people swiftly to justice. I urge the Senate to work to address the points raised by law enforcement so we can continue to improve H.R. 387.

I encourage all Members to support H.R. 387.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Kansas (Mr. YODER) that the House suspend the rules and pass the bill, H.R. 387.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

## RESIGNATION AS MEMBER OF COMMITTEE ON ARMED SERVICES

The SPEAKER pro tempore laid before the House the following resignation as a member of the Committee on Armed Services:

FEBRUARY 6, 2017.

Hon. PAUL D. RYAN,
*Speaker of the House,*
*Washington, DC.*

DEAR SPEAKER RYAN: I, Pete Aguilar, am submitting my resignation from the House Armed Services Committee effective immediately. It has been a privilege and honor to have served on this committee and I look forward to serving my constituents in a new capacity as a member of the House Appropriations Committee.

Sincerely,

PETE AGUILAR,
*Member of Congress.*

The SPEAKER pro tempore. Without objection, the resignation is accepted.

There was no objection.

## RESIGNATION AS MEMBER OF COMMITTEE ON ARMED SERVICES

The SPEAKER pro tempore laid before the House the following resignation as a member of the Committee on Armed Services:

HOUSE OF REPRESENTATIVES,
*Washington, DC, February 6, 2017.*

Hon. PAUL D. RYAN,
*Speaker of the House,*
*Washington, DC.*

DEAR SPEAKER RYAN: I, Scott Peters, am submitting my resignation from the House Armed Services Committee effective immediately. It has been a privilege and honor to have served on this committee.

Sincerely,

SCOTT H. PETERS.

The SPEAKER pro tempore. Without objection, the resignation is accepted.

There was no objection.

## RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess until approximately 6:30 p.m. today.

Accordingly (at 5 o'clock and 58 minutes p.m.), the House stood in recess.

□ 1830

## AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. WOODALL) at 6 o'clock and 30 minutes p.m.