through additional changes. An independent audit will give us the tools we need to make additional changes if necessary.

I want to commend, once again, the distinguished gentlewoman from Texas, SHEILA JACKSON LEE, ranking member of the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the Judiciary Committee, for her leadership on this important issue.

I also want to thank the chairman of the full committee, Chairman GOODLATTE, and former chairman of the Judiciary Committee, Chairman SENSENBRENNER, for their assistance in bringing this important legislation to the floor today.

I join with all of those who are with us in supporting this measure.

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

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, in concluding, a lot of thanks go to, as I indicated, the chairman, Chairman GOODLATTE; Ranking Member CONYERS; Mr. RATCLIFFE, who is a member of the committee; and my colleagues on Homeland Security as well, who have a great interest in this legislation.

Our commitment in this legislation is to leave no stone unturned, no page unturned, and no iota of information that will be necessary to make this list a more viable and secure list. That work now will be done by this legislation, the No Fly for Foreign Fighters Act. It will help to make the Terrorist Screening Center a further asset to our Homeland Security infrastructure.

We want to make certain that those men and women have the tools they need to continue to keep the Nation safe. With 30,000 foreign fighters and others going every day, 250 Americans who have gone to the caliphate, have gone to the fight, individuals who may have an interest in returning to this country and doing us harm, doing us damage, I believe H.R. 4240 is the next step in ensuring that the screening and watch-listing process works as it was intended to have worked and works without as many errors as possible—errorless, if you will—because that is what we need to secure this Nation.

I urge all my colleagues to support this commonsense, bipartisan measure.

I yield back the balance of my time.

Mr. GOODLATTE. Mr. Speaker, this is good legislation. It is common sense to conduct a review of the terrorist watch-listing process.

I urge my colleagues to support the legislation.

I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Virginia (Mr. GOODLATTE) that the House suspend the rules and pass the bill, H.R. 4240, as amended.

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

A motion to reconsider was laid on the table.

EMAIL PRIVACY ACT

Mr. GOODLATTE. Mr. Speaker, I move that the House suspend the rules and pass the bill (H.R. 699) 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, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 699

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'';

(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 Virginia (Mr. GOODLATTE) and the gentleman from Michigan (Mr. CONYERS) each will control 20 minutes.

The Chair recognizes the gentleman from Virginia.

GENERAL LEAVE

Mr. GOODLATTE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous materials on H.R. 699, currently under consideration.

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

There was no objection.

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

Today is an historic day. Today, the House of Representatives will be the first Chamber in Congress to approve legislation that has been pending before the House and Senate for several years to reform and modernize the Electronic Communications Privacy Act, or ECPA. Reforming this outdated law has been a 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.

Two weeks ago, the House Judiciary Committee unanimously reported a revised version of H.R. 699, the Email Privacy Act. 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, tweets were the sounds made by birds in the trees, 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 over 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.

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 provider, 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. 699 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 on 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. 699 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 Web site, versus content disclosed only to one or a handful of persons, like an email or a 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. 699 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 into the future.

I would like to thank Congressman YODER and Congressman POLIS for introducing the underlying legislation and for working with the committee on improvements to the bill.

With this historic vote today, Congress will approve 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.

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 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.

H.R. 699, 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 the investigators and government agents who seek access to our email, our advice is accordingly simple: Get a warrant. It is an idea whose time has long since come. 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. 699 also codifies the right of the providers to give notice of this intrusion to their customers, except in certain exigent circumstances that must also be validated by the court.

□ 1415

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. In the House Judiciary Committee, we reached quick consensus that a civil carve-out of any kind is unworkable, unconstitutional, or both. I would have preferred to have kept 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 has accessed our electronic communications. The government should have an obligation to provide us with some form of notice when intruding on a record of our most private conversations; but I 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. This legislation is several years in the making, and it should not be delayed any further. I compliment our colleague Mr. POLIS. Accordingly, I urge my colleagues to support H.R. 699, the Email Privacy Act.

I reserve the balance of my time.

Mr. GOODLATTE. Mr. Speaker, I yield 5 minutes to the gentleman from Kansas (Mr. YODER), the chief sponsor of the legislation.

Mr. YODER. I thank the chairman.

Mr. Speaker, today is a great day for the Constitution. It is a great day for the spirit of bipartisanship in this Chamber. It is a great day for Americans everywhere who use modern technology, such as emails and text messages and cell phones, to communicate with one another.

This day has been a long time in the making, and I want to thank the chairman and his staff, Ranking Member CONYERS, my colleague Mr. POLIS, and everyone who has worked on this legislation. This is the most cosponsored bill in the entire United States House—the most popular bill—because it is a commonsense piece of legislation that affects every American and will clear up a long-time hole in the law that has allowed the government to intrude on Americans' privacy.

You have to go back to 1986 when this law was passed: Halley's Comet was passing by Earth; ''Top Gun'' was coming out as a new movie; Cabbage Patch dolls were flying off the shelves. It was a good time in America. It was also the time in which Congress last wrote the laws that updated the Electronic Communications Privacy Act. At that point, there were only 10 million Americans who even had email accounts. Today, there is an estimated 232 million Americans who have email accounts. It wasn't until 6 years later that someone sent the first text message in 1992. Yet, now, we expect 1 billion text messages to be sent every single year.

The current law, which is the law that was written in 1986, allows an abuse of our constitutional rights by treating our digital information as if it is not private information—as if it can be searched and seized by the government without a warrant, without probable cause, without due process. The theory in 1986 was, if you left your email on a server, once it was left there, it was considered abandoned. It was like trash that was left out on the street corner, which didn't have an expectation of privacy anymore. We know the ways that Americans communicate today is in a way in which they expect that those transmissions are private, and they expect that the government will honor that and not search those emails or capture them for other purposes. The Fourth Amendment is being violated.

Today, we restore the Fourth Amendment by treating digital information just like paper information, and we stand strong on the notion that Americans do have an expectation of privacy in their email accounts. I would think, if I and my colleagues would each ask our constituents if they expect that their email conversations are private, they would know that they are, and they would expect that they are. As we are debating this bill, Americans are sending emails and text messages back and forth, and they expect that their government is not reviewing those.

What we do in this legislation is require a warrant. We say the government must have probable cause. They must go to a judge whether it is at the

Federal level, the State level, or the local level. To review those pieces of digital information that are stored either in a drop box or on the iCloud—or just a text message that is sent back and forth—you have to have a warrant, and in a civil matter, you have to have a subpoena, and that subpoena is served on the individual.

We have documents on our desks at home. The police can't kick in your door and go read those documents unless they have a warrant backed up on probable cause. We have a digital set of documents that goes around with us wherever we go. There is a file cabinet with us. When we store things, we are doing so not because we are abandoning it. We are storing it because we are wanting to protect it, and we are wanting to ensure that we can keep it. We don't want to lose our Fourth Amendment protections because of that. This legislation would require that a warrant or a civil subpoena exist in order to read that information so that due process occurs.

This is a great unifier. Quite often on the House floor, we are divided—Republicans and Democrats—and we are not able to find resolution on some of the biggest challenges that face us; but the Fourth Amendment in the Constitution has to be preserved. I am heartened by the fact that my colleague Mr. POLIS and groups on the left and groups on the right and groups in the center and that America has come together on this legislation to say we are going to fix this, and we are going to ensure that this Congress modernizes its laws and that it does so in a bipartisan fashion so that we can put this bill on the President's desk and he will sign it into law. As we continue to advance, we must remember to advance the laws that this country utilizes, and as Americans communicate in different ways, we have to modernize the way the laws treat that communication.

I am proud of the work we are doing in the House today. I thank the chairman and his team. I thank Ranking Member CONYERS and my colleagues on both sides of the aisle. This is a great day for America, a great day for the Constitution, and a great day for each and every one of us who uses email to correspond to know that the Fourth Amendment continues to protect us and to know that the Internet is not immune from the protections of the Constitution.

Mr. CONYERS. Mr. Speaker, I yield 3 minutes to the gentleman from Colorado (Mr. POLIS), one of the authors of the measure before us.

Mr. POLIS. Mr. Speaker, the passage of the Email Privacy Act is an enormous victory. It is a victory for all Americans who believe in the right to privacy, in the Fourth Amendment, and in due process.

The Email Privacy Act mandates, for the first time, that Americans have the same legal protection for their emails as they do for papers, letters, faxes, and other old communications. The bill protects those of us—myself included and many Members of this body—who have email accounts in the cloud. Maybe it is Google mail or Yahoo Mail or AOL or other email accounts on their hard drives. It makes sure that the government doesn't have the right, without a warrant, to search emails that are older than 180 days.

This bill is also a victory for bipartisanship. When I introduced the bill, along with my colleague Mr. YODER, in the winter of 2015, we knew it would be popular. Yet, as this bill sits before us today, ready for passage, I am very proud to say it has garnered 314 cosponsors, and it stands as the single most popular bill in this session of the House of Representatives. I am excited that it is scheduled for a floor vote.

When Congress passed the Electronic Communications Privacy Act in 1986, electronic communications were different than they are today. They didn't really exist as such. A few professors were using a predecessor for the Internet. It was not a mass form of communication. Today, with 24/7 accessibility with mobile devices and laptops, over 205 billion emails are sent every day, according to some estimates, including many that contain our private communications for millions of Americans who deserve the same right to privacy as documents in a file cabinet.

With the passage of the Email Privacy Act, Congress will ensure that your emails that are older than 180 days are subject to the same protection under the Fourth Amendment. You often hear Members on both sides of the aisle talk about commonsense bills. When you read our bill and when you look at the immense support, there is nothing more common sense than the Email Privacy Act.

I urge my colleagues to vote ''yes'' and pass the bill. I urge the Senate to take it up and act. There is the unanimous support from the House Judiciary Committee and, as of today—hopefully soon—overwhelming support on the floor of the House. This bill should be passed. It should be brought to the desk of the President of the United States. We should finally bring our email privacy laws into the 21st century.

Mr. GOODLATTE. Mr. Speaker, I yield 3 minutes to the gentleman from Texas (Mr. POE), a member of the Judiciary Committee.

Mr. POE of Texas. I thank the chairman for bringing this bill up and for his work on it in a bipartisan way.

I especially want to thank Congressman YODER for pushing this legislation that has overwhelming support in the House of Representatives.

Mr. Speaker, the Electronic Communications Privacy Act was passed in 1986—30 years ago. It was an eternity. Understand that IBM invented and put on the market its first laptop in 1986. A lot has changed since that day 30 years ago. As the chairman mentioned, the cloud was where rain came from, or sometimes we see it here in Washington, D.C.—the cloud. No one even knew what that was. The Electronic Communications Privacy Act needs to be fixed because it does not protect the right of privacy of Americans.

If something is stored in the cloud that is over 180 days old, then it is open season for government to seize all of that information. All governments—local or State or Federal—can go in and get those emails, texts, photographs, documents that you are storing. Up to 180 days, it is protected by the Constitution. Interesting—180 days of constitutional rights—but on the 181st day, you have no right of privacy. That is absurd. This bill fixes that former legislation.

I used to be a judge in Texas for 22 years, and I had peace officers all the time come to see me who wanted a warrant. They followed the Fourth Amendment and described the place to be searched. They would go in with that warrant, after stating probable cause, and they were allowed to seize whatever they could seize under the warrant. The Fourth Amendment ought to apply today. It ought to apply in the electronic age. It ought to apply to emails that are stored in the cloud or to anything else that is stored in the cloud. If the police officers have to have a warrant to go into your house and take documents you store in your desk or wherever, then they have to have a warrant if you store documents in the cloud. That is what this legislation does, and it makes sense that we protect the constitutional right.

The government cannot tap our phones without a warrant, it can't read hard mail without a warrant, and it can't enter our homes without a warrant because of the Fourth Amendment. We are unique among all peoples because we have in our Constitution the Fourth Amendment that protects Americans—I think better than any other population anywhere—of their rights.

Speaking of rights, the government doesn't have rights. People have rights, and the Bill of Rights protects the citizens of the United States. Government has authority—it has power—and if you read the Bill of Rights, the 10 Amendments especially, it is to limit government power and authority against us, the citizens. So, of course, the Fourth Amendment should apply to the Federal Government in this area.

Unfortunately, we have seen in our own government abuses of the government in the area, especially of snooping and spying on Americans, with the NSA and its story that we are all familiar with. We have to control government, and it is our obligation, the House of Representatives, to protect the Constitution—the Bill of Rights especially—from government intrusion.

I support this legislation. It is a good piece of legislation. I thank the chairman and the ranking member and Ms. LOFGREN for her support of this legislation that we have been working on for a long time. Let Congress speak out

and support the right of privacy for all Americans and keep the government out of the snooping business.

And that is just the way it is.

Mr. CONYERS. Mr. Speaker, I yield 3 minutes to the gentleman from New York (Mr. NADLER), a senior member of the House Judiciary Committee.

Mr. NADLER. I thank the chairman.

Mr. Speaker, I rise to support the Email Privacy Act.

It has long been evident that we need to update the laws impacting electronic communications and privacy. I am pleased that, today, the House will take a major step forward by considering and approving the Email Privacy Act. Its passage is long overdue.

In 2009 and 2010, when I was the chair of the House Judiciary Subcommittee on the Constitution, Civil Rights and Civil Liberties, we held multiple hearings on ECPA, or electronic communication and privacy laws, and began to seriously consider reforms to our Nation's electronic communication and privacy laws. During the 112th Congress, Representative CONYERS and I introduced the Electronic Communications Privacy Act Modernization Act of 2012, which would have required law enforcement to obtain a warrant based on probable cause before searching email. That approach, now embodied in the Yoder-Polis Email Privacy Act, is what we are here to consider today.

The Email Privacy Act requires the government to obtain a warrant in order to access people's electronic communications from a third-party provider, protecting Americans' privacy rights while still enabling law enforcement to do its job.

□ 1430

This is consistent with a stark American practice going back to the Fourth Amendment. Current law is inconsistent and unclear regarding the standards for government access to the content of communications, and a single email is potentially subject to multiple different legal standards.

Clarifying the laws will 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.

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

This bill is not perfect, and clearly there is more to be done. In particular, we must ensure that we keep working to require a probable cause warrant for location information.

I am pleased that Chairman GOODLATTE has announced that he plans to hold hearings on location information, and I look forward to those hearings and to subsequent legislation.

I am proud to be an original cosponsor of this bill, and I applaud the House for considering this landmark legislation today.

I urge my colleagues to support the passage of this bill to ensure that our laws strike the right balance between the interests and needs of law enforcement and the privacy rights of the American people.

Mr. GOODLATTE. Mr. Speaker, I yield 2 minutes to the gentleman from South Carolina (Mr. SANFORD).

Mr. SANFORD. Mr. Speaker, I want to applaud my colleagues from Kansas and from Colorado for their work in crafting this bill. I think it is awfully important.

I think it is what people expect. When they think about government, they want a government that works for them. Part of having a government that works for them means actually updating laws as technology has changed.

So I think that, at the core, this is about keeping current with the rate of change in the world of technology.

It is amazing to me—I pulled the numbers—that there are roughly 205 billion emails sent every day around the world. If you presuppose that America's economy is about 20 percent of that world pie, that means around 40 million or more emails are sent across this country every single day.

In contrast is the U.S. Postal Service. There are about 600 million letters that go across this country every day, which is to say, mathematically, you are saying that about 1.5 percent of the communication flow, either via mail or electronic means, are sent by the Postal Service.

The other, in essence, 99 percent of the communications are sent via email, which is to say we have a real problem with a law that was created in the 1980s that doesn't take into account the way the world has changed.

So I applaud the crafters of this bill for what they have done in recognizing technology change. I applaud them for the way that they stayed true to the Fourth Amendment.

Our Founding Fathers were so deliberate in recognizing the notion that you didn't want to have British soldiers coming into a house and rumbling around until they finally found something to charge you with and then moving forward.

The Fourth Amendment is about protecting individual liberty. Jefferson said: ''The natural progress of things is for the government to gain ground and for liberty to yield.''

Fundamentally, what this bill is about is pushing back in the way that the government has now encroached on that space of individual liberty.

Finally, I would say simply this: This is about recognizing how true history is on the importance of protecting liberty.

The SPEAKER pro tempore (Mr. COSTELLO of Pennsylvania). The time of the gentleman has expired.

Mr. GOODLATTE. Mr. Speaker, I yield an additional 1 minute to the gentleman from South Carolina.

Mr. SANFORD. Mr. Speaker, Edward Gibbon wrote a book back in 1776 about the fall of the Romans. In it, he harkens back to the fall of Greece and the Athenians.

He said, at the end of the day, in the end, more than they wanted freedom, they wanted security. They wanted a comfortable life, and they lost it all—security, comfort, and freedom—when the Athenians no longer wanted to give to society, but to receive. And he goes on with a long quote from there.

He talks about the fundamental tension that exists in any developed society between freedom and security. We have moved too far in the opposite direction as it relates to email. This bill brings us back toward the center.

I again applaud Mr. YODER and Mr. POLIS for what they have done. I also applaud Chairman GOODLATTE for what he has done on this front.

Mr. CONYERS. Mr. Speaker, I yield 2 minutes to the gentlewoman from Washington (Ms. DELBENE), a very effective member on the Judiciary Committee.

Ms. DELBENE. Mr. Speaker, updating our laws to reflect the way the world works in the 21st century has been one of my top priorities in Congress.

After spending two decades in the technology sector where things change at light speed, it can be hard to understand why we still have laws on the books that don't reflect how society functions in the digital age. Nowhere has this been more obvious than in our email privacy laws that date back to the 1980s.

Under current law, there are more protections for a letter in a filing cabinet than an email on a server. This was never really the intent, but email's evolution has made it clear that our policies are woefully outdated.

I have supported a number of different proposals to reform our electronic privacy laws, and I will continue to push for those. Today's vote on the Email Privacy Act is a great step forward for American civil liberties.

I urge all of my colleagues to vote ''yes'' on this important legislation, and I urge our friends in the Senate to take up the bill without delay so we can send it to the President and ensure Americans are guaranteed the privacy protections most think that they already have.

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

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

I would like to close today by thanking Chairman GOODLATTE of the Judiciary Committee and his staff for working with us to develop the final draft of this legislation. Once again the chairman has helped us find a way to resolve our differences and advance core civil liberties and constitutional values.

I would also like to thank the gentleman from Kansas (Mr. YODER) and

the gentleman from Colorado (Mr. POLIS) for their leadership on this issue from the very beginning.

The Email Privacy Act comes to the floor today in large part because of your work in gathering more than 300 cosponsors for this bill.

Finally, I want to express appreciation to the coalition of technology companies, civil liberties organizations, and individual experts whose persistence and dedication have made this moment possible.

I urge my colleagues to support H.R. 699, the Email Privacy Act. I believe that they will do so. I also urge our comparable body in the Senate to take up this measure as quickly as possible.

I yield back the balance of my time.

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

Mr. SCALISE. Mr. Speaker, I thank Chairman GOODLATTE for moving this bill through his committee. I especially thank Congressman YODER of Kansas for bringing this bill forward and for being bold enough to say let's modernize a law that is so outdated that it goes back to 1986, governing email communication when we didn't even have email and text messages.

Why do we want to do this? We want to do it because Federal agencies are abusing this law to invade the privacy of hardworking, law-abiding citizens all across this country.

Mr. Speaker, this is a document from the Internal Revenue Service titled ''Search Warrant Handbook.'' In this document by the IRS, their protocol says: ''In general, the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server, because internet users do not have a reasonable expectation of privacy in such communications.''

The IRS has made it clear that they don't believe that American citizens have a Fourth Amendment protection of privacy for their email communications. The IRS has gone further and is actually reading emails of American citizens, and no one across the country knows about it unless the IRS finds something that then they are going to go after you criminally on.

So they are reading the private emails, Mr. Speaker, of American citizens every single day, and they have been doing it for years. It is time for this abuse of power to end.

We need to pass this bill with strong bipartisan support, send it over to the Senate, and get it to the President's desk so that American citizens have real privacy protections that they deserve, that they think they have, but they don't have, Mr. Speaker, because Federal agencies like the IRS today are reading the private emails of American citizens and using them against them.

It is wrong. They ought to go get a warrant, but they should not be reading our private emails when people haven't done anything wrong.

Let's pass this bill.

Mr. GOODLATTE. Mr. Speaker, how much time is remaining?

The SPEAKER pro tempore. The gentleman from Virginia has 1½ minutes remaining.

Mr. GOODLATTE. Mr. Speaker, I yield 45 seconds to the gentleman from Texas (Mr. FARENTHOLD), a member of the Judiciary Committee.

Mr. FARENTHOLD. Mr. Speaker, we are here today talking about modernizing a law, but we are modernizing a law that encompasses a centuries-old principle.

Back in the days when the Founding Fathers wrote our Constitution, they were concerned about the government rifling through our papers. Today we have electronic papers. Stuff is stored in the cloud.

This piece of legislation brings us back in line with the intent of the Founding Fathers that the government can't just rifle through your papers.

I urge my colleagues to support it.

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

I want to take this time to thank the ranking member, the gentleman from Michigan (Mr. CONYERS), and many Members on his side of the aisle, including Mr. POLIS.

I especially want to thank Mr. YODER, who has worked long and hard on this legislation for which he is the chief sponsor.

I most especially want to take note of the fact that we have very disparate points of view from a whole array of people around this country, from law enforcement, to technology companies, to civil liberties organizations. It took a long time to sort through that and find the common ground that is the legislation we have before us today.

That ground would not have been found without the outstanding work of our staff, most especially Caroline Lynch, the chief counsel of the Judiciary Committee's Crime, Terrorism, Homeland Security, and Investigations Subcommittee, and her able team of attorneys, and Aaron Hiller, minority counsel as well.

They deserve a great deal of gratitude for the years of work to bring us to this point where we can pass this important, important legislation by what I believe will be a resounding majority.

I yield back the balance of my time.

Mr. SWALWELL of California. Mr. Speaker, I rise in support of H.R. 699, the Email Privacy Act.

Current law protecting electronic privacy is drastically out of step with modern technology, and H.R. 699 represents a long overdue update. This bill would provide Americans the privacy protections in their electronic communications they expect and deserve.

While it is important that the House advance H.R. 699 today, no bill is perfect. Law enforcement has raised a few concerns about it, such as that it does not provide them the ability to access to critical information quickly enough. As a former prosecutor, I take their views seriously. I hope we can continue the dialogue with law enforcement and consider ways to improve the bill as it moves along in the legislative process.

I encourage all Members to support H.R. 699.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 699, the Email Privacy Act.

This is an important and long negotiated bill that will update the Electronic Communications Privacy Act, a law that both protects the privacy of our email communications and provides a critical tool for law enforcement to investigate crime.

I want to thank Judiciary Chairman BOB GOODLATTE and Ranking Member JOHN CONYERS for their leadership and for working together on this legislation to accomplish the goals of this bill for the benefit and protection of citizens, law enforcement, and communications providers.

I am an original cosponsor of this bill, which has 314 cosponsors, enjoying overwhelming bipartisan support.

The Electronic Communications Privacy Act, or ECPA, was enacted in 1986.

The statute is outdated and provides unjustifiably inconsistent standards for law enforcement access to stored communications.

The law was designed at a time when few of us used email or could have imagined a world in which we could securely share information and edit electronic documents online with others, or where businesses could input, store, process, and access all data related to their operation.

The outdated, inconsistent, and unclear aspects of this statute undermine both our privacy interests and law enforcement goals.

It is critical that we enact the central reforms provided by this bill.

For instance, a probable cause standard should apply to the government's ability to compel a communications provider to disclose a customer's email message—no matter how old the message is.

Currently, the statute requires the government to obtain a warrant based on probable cause to compel disclosure of an email that is in storage for 180 days or less.

However, the statute only requires a subpoena for the government to obtain email messages that are older than 180 days.

This makes no sense because citizens have the same, reasonable expectation that these stored communications are private.

Therefore, we must change the law so that the higher standard applies regardless of the age of these communications, and H.R. 699 would accomplish this.

In addition, the law does not adequately protect communications stored ''in the cloud'' by third parties on behalf of consumers, and a probable cause warrant should be required for government access.

ECPA additionally provides a lesser standard for some cloud storage than it does for many communications stored by electronic communications services.

To further complicate matters, many companies provide both communications services and remote storage, making the services to the same customer difficult to separate for purposes of determining which standard applies.

Applying inadequate and unclear standards to government access to cloud communications undermines consumer confidence in cloud privacy and threatens to hamper the development of this important engine of economic growth.

H.R. 699 addresses this issue by providing a clear and consistent probable cause standard for access to the contents of stored communications for which customers have a reasonable expectation of privacy.

H.R. 699 would accomplish these fairly straightforward reforms and that is why it has the support of privacy advocates and electronic communications companies.

I urge all of my colleagues to support this commonsense, bipartisan measure.

Mr. BABIN. Mr. Speaker, as a proud original cosponsor of H.R. 699, the Email Communications Privacy Act (ECPA), I am pleased to rise in full support of this bill on the House floor.

Since being introduced on February 4, 2015, we have been able to secure more than 300 cosponsors of this important bill, which will improve privacy protections for the email communications of ordinary American citizens.

Under current law there is little protection for the content of electronic communications stored or maintained by third party service providers. ECPA corrects this oversight and updates our laws to require a court ordered warrant that is based on probable cause before an email service provider can disclose these private communications.

In the current era where individual privacy is often overlooked or sidelined, this bill takes an important step to protect your privacy.

It is long past due that we update our privacy laws to give emails—a major means of communication today—the same protection as traditional mail and telephone calls. This bill has been endorsed by a broad range of privacy groups, including such conservative organizations as the Heritage Foundation and FreedomWorks.

Our bill modernizes these outdated statutes to ensure that the rights protected by the Fourth Amendment extend to Americans' email correspondence and digital data.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Virginia (Mr. GOODLATTE) that the House suspend the rules and pass the bill, H.R. 699, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. GOODLATTE. 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 motion will be postponed.

DEFEND TRADE SECRETS ACT OF 2016

Mr. GOODLATTE. Mr. Speaker, I move to suspend the rules and pass the bill (S. 1890) to amend chapter 90 of title 18, United States Code, to provide Federal jurisdiction for the theft of trade secrets, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 1890

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 ''Defend Trade Secrets Act of 2016''.

SEC. 2. FEDERAL JURISDICTION FOR THEFT OF TRADE SECRETS.

(a) IN GENERAL.—Section 1836 of title 18, United States Code, is amended by striking subsection (b) and inserting the following:

''(b) PRIVATE CIVIL ACTIONS.—

''(1) IN GENERAL.—An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.

''(2) CIVIL SEIZURE.—

''(A) IN GENERAL.—

''(i) APPLICATION.—Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.

''(ii) REQUIREMENTS FOR ISSUING ORDER.—The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that—

''(I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;

''(II) an immediate and irreparable injury will occur if such seizure is not ordered;

''(III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;

''(IV) the applicant is likely to succeed in showing that—

''(aa) the information is a trade secret; and

''(bb) the person against whom seizure would be ordered—

''(AA) misappropriated the trade secret of the applicant by improper means; or

''(BB) conspired to use improper means to misappropriate the trade secret of the applicant;

''(V) the person against whom seizure would be ordered has actual possession of—

''(aa) the trade secret; and

''(bb) any property to be seized;

''(VI) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;

''(VII) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and

''(VIII) the applicant has not publicized the requested seizure.

''(B) ELEMENTS OF ORDER.—If an order is issued under subparagraph (A), it shall—

''(i) set forth findings of fact and conclusions of law required for the order;

''(ii) provide for the narrowest seizure of property necessary to achieve the purpose of this paragraph and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;

''(iii)(I) be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and

''(II) provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access shall be consistent with subparagraph (D);

''(iv) provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including—

''(I) the hours during which the seizure may be executed; and

''(II) whether force may be used to access locked areas;

''(v) set a date for a hearing described in subparagraph (F) at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; and

''(vi) require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure under this paragraph.

''(C) PROTECTION FROM PUBLICITY.—The court shall take appropriate action to protect the person against whom an order under this paragraph is directed from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order.

''(D) MATERIALS IN CUSTODY OF COURT.—

''(i) IN GENERAL.—Any materials seized under this paragraph shall be taken into the custody of the court. The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.

''(ii) STORAGE MEDIUM.—If the seized material includes a storage medium, or if the seized material is stored on a storage medium, the court shall prohibit the medium from being connected to a network or the Internet without the consent of both parties, until the hearing required under subparagraph (B)(v) and described in subparagraph (F).

''(iii) PROTECTION OF CONFIDENTIALITY.—The court shall take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized pursuant to this paragraph unless the person against whom the order is entered consents to disclosure of the material.

''(iv) APPOINTMENT OF SPECIAL MASTER.—The court may appoint a special master to locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized. The special master appointed by the court shall agree to be bound by a non-disclosure agreement approved by the court.

''(E) SERVICE OF ORDER.—The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate, but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may