STATEMENT

Of

Paul Rosenzweig
Visiting Fellow, The Heritage Foundation
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

Before the

Committee on the Judiciary
United States House of Representatives

December 1, 2015

The Email Privacy Act

Introduction

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the Email Privacy Act, H.R. 699. My name is Paul Rosenzweig and I am the principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice. I am also a senior advisor to The Chertoff Group and a professorial lecturer in law at George Washington University where I teach a course on cybersecurity law and policy. In addition, I serve as a visiting fellow in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.[1] From 2005 to 2009 I served as the deputy assistant secretary for policy in the Department of Homeland Security.

[1]The Heritage Foundation is the most broadly supported think tank in the United States. During 2014, it had more than 500,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2014 operating income came from the following sources:

- Individuals 75%
- Foundations 12%
- Corporations 3%
- Program revenue and other income 10%

Needless to say, my testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Indeed, to be clear, I work extensively in the cybersecurity and tech space and many of my clients are following this debate with great interest. That having been said, today I am testifying as an individual discussing my own independent research. The views expressed are my own. In addition. Inasmuch as I am appearing under my Heritage Foundation affiliation it is important to note that Heritage scholars neither endorse, nor oppose legislation. Our views on the substance of particular proposals should not be read as advocating for or against the adoption of a particular piece of legislation – we write and speak about the underlying polices in question only.

There is, of course, a great deal that can be said about the privacy of email communications and proposals to protect them. In the interests of brevity and to avoid repeating much of what my colleagues on the panel will say, after offering some introductory thoughts, I will make three simple points:

- Proposals to protect by warrant requirement the content of email are consistent with fundamental values held by the Framers and the origins of the Fourth Amendment. I think, frankly, the Founding Fathers would be shocked to learn that this question is even in dispute;
- Some in law enforcement object to the notice requirement that many proposals for reform include – the idea that before (or sometimes after a period of delay) securing an individual's email, that individual should be notified of the execution of the search. But the concept of notice has been an integral part of warrant requirements for over 200 years. There is little reason to expect that law enforcement can't accommodate notice today; and
- Finally, some argue that email privacy reform will harm national security. As a former official in the Department of Homeland Security I yield to no one in my concern for national security. In my judgment, however, properly drafted exceptions can and will easily insulate ECPA reform from this concern.

I will close by offering some thought on the important context within which this debate arises, as I think there is inadequate appreciation of how broad the import is of the questions you are considering.

The top five corporate givers provided The Heritage Foundation with 2% of its 2014 operating income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Introductory Thoughts

The basic question before this Committee is simple: Should the contents of your email messages be protected from law enforcement scrutiny to the same extent as your physical letters sent through the mail?

To ask the question makes the answer seem obvious. Email is today's postal service and the personal contents of your email messages are as private to you as the letters we used to send through the U.S. Post Office.

But even though the answer seems obvious, that is not, as this Committee knows, what the law actually says. At least today, some of the contents of your email (most notably the emails you store on a server, like on a Gmail service or in Dropbox) are not as well-protected. To read your mail in transit with the Post Office, the government generally needs a warrant, issued by a neutral magistrate, and based on probable cause to believe that the search will provide evidence of a crime. To read the content of email messages stored on a server for an extended period, it doesn't need a warrant at all – it can get the content by issuing a subpoena to your cloud service provider. Unlike a warrant, a subpoena is not based on probable cause and it isn't reviewed by a judge before it is issued. In practice, it is issued by a prosecutor, unchecked by a judge, based on any reasonable ground.

The reason for this difference in treatment is more historical than malevolent. The law that protects email – the Electronic Communications and Privacy Act – was written in 1986, when cloud servers were a dream of the future and when nobody could imagine storing email for any length of time because digital storage costs were so high. Indeed, in 1984 it cost more than $100 to store a single megabyte of data. Today, you can buy a 2 terrabyte storage drive for less than $100 – and that makes the assumptions which underlie the ECPA out of date. This coming year we celebrate the 30th anniversary of the law. Indeed many of the staff working for Congress today were not alive when it was passed.

As a result, under current law, as data moves from local storage to the cloud, the government contends that it does not need to go to the owner of the data to get copies of the data. Instead, the government claims that it can go to the cloud provider, demand the data with a subpoena, and prohibit the data owner from being notified. This needs to change: When government agents want ISPs and cloud providers to disclose sensitive data, they should get a warrant from a judge.

The Fourth Amendment

Any discussion of email privacy must, in my view, be grounded in an historical understanding of the Fourth Amendment. Properly construed, I think that early history demonstrates an

overarching concern with the privacy of personal papers and effects. That, after all, is the language of the Amendment and I think that the Founders would be surprised to know that the words “papers and effects” do not cover my personal love emails to my wife, simply because they are written in electronic form rather than with pen and ink.

More to the point, the history of why the Fourth Amendment was adopted stands as a powerful reminder that the security of our personal thoughts and effects lay at the core of the Framers concerns about government overreach. The story is, by now familiar, but it bears repeating. Two seminal cases from pre-revolutionary days shaped our thinking about the proper balance between government scrutiny of the content of our communications and individual privacy intersts.

The first case, of course is *Wilkes v. Wood,* 98 Eng. Rep. 489 (1763). Wilkes was a well known memper of the opposition party in parliament. He published a pamphlet “The North Briton” criticizing the government and accusing King George III of lying. Robert Wood, an agent of the King, possessed of a general warrant, broke into Wilkes house and seized his papers. The warrant named no suspect nor any specific place to be searched. It was a “general warrant.” After the fact Wilkes charged Wood with an act of trespass. He argued that a seizure of his papers and personal effects was an intrusion into his most private concerns. Wood defended, of course, on the ground that a general warrant was sufficient to the matter at hand and protected him from liability. A jury found for Wilkes and awarded him 1000 pounds – an astronomical sum in those days. He also recovered 4000 pounds from Lord Halifax, who had issued the original general warrant.

As Professor Akhil Reed Amar of Yale notes, *Wilkes* was the “most famous case in late eiteenthe-century America,” one whos “plot and cast of characters were familiary to every schoolboy in America.” Its lessons against sweeping warrants and roving government inspections of personal papers were at ehte core of what the Fourth Amendment intended to prohibit.

The other case, of course, was the Writs of Assistance case that arose in the colonies in 1761. Writs of Assistance were general warrants allowing officials to search for smuggled goods anywhere they suspected the goods might exists. James Otis was on the side of the crown when the Writs were issued, but he resigned his post as Advocate-General and took up the case for the Boston merchants who opposed the writs. He argued that the unwarranted search of personal effects was against British law and violated the rights of Englishmen. Otis lost the case, but his argument, and the resulting controversy galvanized the revolutionary movement. Indeed, his argument was witnessed by a young John Adams who said that "the child independence was then and there born, [for] every man of an immense crowded audience appeared to me to go away as I did, ready to take arms against writs of assistance." It is no

exaggeration to say that concern for overly intrusive government behavior and intrusion was a critical ingredient of the thinking of the Founding Fathers.

Nor is the view I've espoused idiosyncratic. To the contrary, at least one Federal court of appeals has reached the very same conclusion. In *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010) the Sixth Circuit considered the very issue that is at the core of the legislative proposal before you – whether a warrant should be required before an ISP is compelled to turn over to the government the contents of a subscriber's email. The answer it gave was an unequivocal "yes."

As the court recognized communication via email is functionally identical to the types of communication known to the Framers -- letters, for example – and to the types of communication more common in the early 20th century like telephone calls. Indeed, the court noted, email today is as pervasive and ubiquitous as those forms of communication used to be and it is equally personal in nature. For that reason the court correctly noted that it would be wildly incongruous to treat email, letters, and telephone calls differently because of the method of delivery. As the Court said: "It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."

Today, internet service providers like Google, Dropbox and Yahoo are the functional equivalent of the post office and their cloud based storage is the functional equivalent of the filing cabinet I still keep in my office. As *Warshak* put it: "It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception."

Indeed, to put the matter bluntly and directly, if I were to have mailed this testimony to the Committee and the staff were to have stored it in a file cabinet in the offices behind this hearing room, the law would (leaving aside the fact that it is Congress we are talking about) require that law enforcement get a warrant to intercept it in transit and either get a warrant or issue a subpoena directly to the recipient – you, Mr. Chairman – to get it otherwise. By contrast, because I sent this testimony in by email (and because I chose to use an ISP to send it) the government can access that same communication by way of subpoena to my service provider without notice to me and without the need to establish any probable cause to believe I've committed a crime.

One can just imagine what John Wilkes and James Otis would have to say about that state of affairs.

Notice

Many proposals, including the Yoder-Polis bill that is presently before this Committee, require that the government provide notice to the subject of the investigation when it receives electronic data about a subscriber from a provider of electronic communications services, like an internet service provider or a cloud data storage system. For law enforcement this notice is required within 10 days; for other government agencies the timeline is 3 days.

Some in law enforcement oppose this notice requirement. They suggest that it might be unworkable and/or that it would give the subjects of investigation advanced notice of the pendency of an inquiry. Neither concern, it seems to me, is at all well founded.

As to unwieldiness, based on my experience as a former prosecutor, notice is the norm; concealment the exception. For example, it is normal practice – and indeed inevitable – that the execution of a search warrant at an individual's home provides notice of an inquiry and that, absent a sealing order from the court, the subject of the investigation will get a copy of the search warrant. The same should be true of intensely personal effects like email correspondence when that data is held in a cloud storage system – just as it would be if hard copy letters were in a file cabinet in the house.

Nor should we persuaded that subjects of an investigation will be tipped off by an inquiry. There is a long-standing set of rules, codified in Section 2705, that allow a court to delay notification to the subject of an investigation if providing the notice would seriously jeopardize the investigation. I see no reason at all why that same rule of general practice – which presently covers such covert activities as bugging a suspects home – would not suffice in this context.

Indeed, the standard used in deciding whether or not to delay notice to the subject of an investigation was added to the law (codifying earlier common law provisions) at the request of the Department of Justice when the Patriot Act was enacted in 2001. It seems passing strange, indeed, that the same standard thought adequate for critical national security counter-terrorism investigations is now criticized as inadequate under the ECPA.

Finally some in law enforcement have raised concerns with the requirement that, at the expiration of a delay in notification, a customer should be advised of "the nature of the law enforcement inquire with reasonable specificity." Again, this text from the proposal before you is nothing new – it is standard language for administrative subpoenas (12 USC § 3405) and other delayed notice requests (e.g. 12 USC § 3409).

One suspects, with some justification, that the suggestion of confusion is overblown and serves more as a makeweight to conceal a broader and more fundamental objection to the proposal. But since generally opposing a warrant for content requirement cannot be politically or legally sustained (at least not after the *Warshak* case) the objections must be couched in different, but less persuasive terms.

National Security

Third, I want to briefly address the idea that proposals to amend the ECPA somehow threaten national security. As an initial matter, I want to register my disagreement with the general idea that anything that enhances investigative power is, *per se*, an improvement in national security. As I said at the outset, my views are strongly conservative and national security is at the core of my professional life. But I can see no basis for saying that the application of traditional Fourth Amendment principles derogates from national security. To the contrary, it enhances it. I could say more on the topic, but I think the best summary was offered by Robert Mueller, the former FBI director under President Bush, in a speech he gave reflecting on the pressures that arose in the wake of 9/11. As Mueller put it so eloquently: ""The rule of law, civil liberties, and civil -rights — these are not our burdens. They are what makes all of us safer and stronger."

More to the point, beyond the thematic, the assertion is simply incorrect. At least as I read it, the proposals before you have a savings clause that explicitly exempts lawful activity under the Foreign Intelligence Surveillance Act. Thus, as I read the proposal, ECPA reform will not affect intelligence investigations and counter-terrorism efforts. The Foreign Intelligence Surveillance Act has its own set of rules for government access to email and documents stored in the "cloud." ECPA reform legislation will not change those rules in any way. To be sure, there may be some edge cases, where the counter-terrorism connection is not sufficiently clear to permit invoking FISA – but I think we should all be comfortable with a default rule that favors civil liberties, rather than government intrusion.

The Broader Context

Before concluding I want to place the ECPA debate in a broader context. In my judgment one of the reasons that this discussion resonates so in Congress today is that it is emblematic of a broader failure of our Legislative and Executive institutions to come to grips with the changing technological reality of our times. Consider some of the other legal and policy challenges arising from a more greatly-interconnected globe-spanning cyber-network. We see:

- authoritarian nations increasingly restricting content on the web and using domestication requirements as a way of both suppressing dissent and protecting their own native corporations against competition;

- the privacy/security dispute dividing natural allies in America and Europe at the expense of our ability to jointly combat mutual threats;
- data localization requirements that degrade the efficiency and effectiveness of cloud architectures; and
- efforts to apply domestic laws with extraterritorial effect, putting internet providers in the untenable position of choosing between competing legal obligations.

To a large degree, our inability to deal with these challenges is fueled by parallel forces resisting the new technological reality – the unwillingness of the executive branch to modify settled behaviors and the inability of the legislative branch to find consensus for action.

As to the former, my colleagues at The Chertoff Group put it this way in a white paper we released earlier this year:

> The future prospects for law enforcement . . . is a time of uncertainty. For now, US law enforcement is still able to take advantage of American unilateralism, grounded in the circumstance that American companies dominate the market and that they can be compelled to assist American investigations. But this form of mandated assistance cannot be sustained in the long run. Even if the legal power to compel American companies to cooperate is sustained, they cannot provide that which they do not possess. A predictable reaction to such a legal régime is that American companies will lose market share because of these demands. They will be increasingly faced with stringent countervailing foreign law demands. Some nations may adopt both domestic storage requirements and, ultimately, domestic corporate preference requirements, both of which will increasingly put data beyond the effective reach of American criminal investigators.

See The Chertoff Group, "Law Enforcement access to Evidence in the Cloud Era," (May 2015). In short, law enforcement's entrenched resistance to technological change – exemplified paradigmatically by their opposition to ECPA reform – is a classic case of valuing short-term gain at the expense of long-term harm. Harm to the American public; harm to the American competitiveness abroad; and, ultimately, harm to law enforcement's own interests.

As to the latter, I find it remarkable that even though there is broad agreement within Congress on the need for ECPA reform (witness the 300+ co-sponsors of the Yoder-Polis bill and the plethora of other bills reforming other aspects of the law) we seem institutionally incapable of responding to changed circumstance. The Email Privacy Act is, or should be, an easy case. If Congress cannot muster the will to see this reform through, we might despair of its ability to deal with other, more complex and complicated questions of law and policy. In the 1960s Congress was able to pass Title III of the Omnibus Crime Control and Safe Streets Act; in the

1970s, intelligence reform under the Foreign Intelligence Surveillance Act; in the 1980s, the ECPA. These were big achievements – notable efforts by this body to deal with significant challenges of technological evolution. Today, I fear, even the most modest of reforms are locked in stasis.

Conclusion

The time is ripe for change and the principle is clear – in the normal law enforcement context, police and FBI officers should have no more access to our stored email than they do to our stored private letters. Technology has changed the way we live. Today everyone stores their email in the cloud. But the law hasn't kept up. That's why Congress needs to modernize the law. Senators and Representatives have introduced bi-partisan bills to update ECPA into the 21st century. Both chambers should give the proposals plenary consideration.