Hearing on

"Reforming the Electronic Communications Privacy Act"

United States Senate Committee on the Judiciary

September 16, 2015

Washington, DC

Testimony of Victoria Espinel
President and CEO
BSA | The Software Alliance

Testimony of Victoria Espinel
President and CEO, BSA | The Software Alliance
Hearing on "Reforming the Electronic Communications Privacy Act"
September 16, 2015
Washington, DC

Good morning Chairman Grassley, Ranking Member Leahy, and members of the Committee. My name is Victoria Espinel, and I appreciate the opportunity to testify today on behalf of BSA | The Software Alliance ("BSA"). BSA is the leading advocate for the software industry in the United States and around the world.[1]

BSA members have a keen interest in today's hearing on "Reforming the Electronic Communications Act." We support efforts to update ECPA, and urge this Committee to advance legislation that would better reflect today's technology. Importantly, updating ECPA would remove outdated distinctions in the law that provide lower levels of legal protections for digital communications.

Ensuring that customers have faith in the security and privacy of their email and other online data is vital to ensuring their trust in digital services. Simply put, if consumers do not trust technology they will not use it. That result would have damaging implications for general productivity and the continuing growth of the digital economy.

The bipartisan ECPA Amendments Act, introduced by Senators Lee and Leahy, improves the trust equation between providers and customers by: 1) protecting email communications from government intrusion without a warrant; and 2) providing clarity to technology companies on their legal obligations to law enforcement, so that providers can be transparent with their customers about how they treat their customers' stored content.

We are generating an enormous amount of data every day – just think: more than 90 percent of the world's data was created in the past two years[2] – but the policy environment tied to data services has not kept pace with this increased use or technological progress. The protections for this 21st century world of data services rest on a framework of 20th century law. Because the law has not kept pace, consumers, businesses and law enforcement all lack sufficient clarity and predictability about the regulations and laws that govern the gathering, storing, sharing, and beneficial use of data.

As the data services sector continues its rapid growth, crucial issues have emerged that will affect its future, such as government access to information, cybersecurity, trade rules and cross-border data flows. Uncertainty over these issues will only continue to grow as time passes and technology evolves, with important implications at home and abroad. In order to realize the full beneficial potential of these data services, and in order to reach the best possible decisions, we must have clear rules.

Congress must update ECPA to bring the law in line with industry practices that have been adopted to protect the constitutional interests of our customers. Many of these reforms are so non-controversial that

[1] BSA's members include: Adobe, Altium, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

[2] IBM, *What is big data?*, at: http://www.ibm.com/software/data/bigdata/what-is-big-data.html.

even today's federal government witnesses accept their wisdom. But these reforms should not be weakened by other changes that would force software companies and other digital service providers to be put in the middle of disputes between the government and the targets of civil investigations.

In addition, BSA members believe that Congress should address issues emerging now, specifically those related to demands by law enforcement agencies in one country for data held in another country. This issue has significant implications for our law enforcement and privacy interests, and for the global competitiveness of our digital services sector. The issue is thoughtfully addressed in the bipartisan Law Enforcement Access to Data Stored Abroad (or LEADS) Act, introduced by Senators Hatch, Coons, and Heller and co-sponsored by a bipartisan group of 12 senators.

Software and the Economy

The commercial software industry is one of the world's most powerful engines of economic growth, with global software revenue exceeding $407 billion in 2013.[3] That was a 4.8 percent increase from 2012 revenue of $388.5 billion and significantly higher than the global GDP growth rate of 3.4 percent.[4] [5] The software industry also generates millions of high-quality, high-paying jobs – with a median salary that far exceeds the national average, and a growth rate that should make it the second-fastest growing U.S. industry sector over the next few years.[6]

But the true impact of the software industry is much more difficult to measure. This is because software is creating entirely new opportunities for growth. Consider, for example, one type of software: apps. That industry is expected to grow from $11 billion in 2014 to $77 billion in 2017.[7] And the just-emerging data analytics market, which relies on software to gather and analyze once-incomprehensible datasets, will reach $125 billion worldwide by 2015.[8]

Software also increasingly enables everything we do and is revolutionizing every other market sector. From financial services and health care to education and entertainment, software generates even greater economic returns through its use by customers because it enables businesses and individuals across the economy to become more efficient, productive, and competitive, and because it provides them with the tools for further innovation.

But the promise of that growth is not guaranteed. In fact, if our laws do not continue to grow with our technology, the global competitiveness and growth of the US software industry will suffer.

---

[3] Gartner, *Gartner Says Worldwide Software Market Grew 4.8 Percent in 2013*, available at http://www.gartner.com/newsroom/id/2696317

[4] *Id*.

[5] International Monetary Fund, *World Economic Outlook Database*, http://www.imf.org/external/pubs/ft/weo/2015/01/weodata/weorept.aspx?pr.x=28&pr.y=2&sy=2006&ey=2015&scsm=1&ssd=1&sort=country&ds=.&br=1&c=001%2C110%2C163%2C200&s=NGDP_RPCH&grp=1&a=1

[6] *See* BSA, *Powering the Digital Economy: A Trade Agenda to Drive Growth* (2014), at http://digitaltrade.bsa.org/pdfs/DTA_study_en.pdf.

[7] Entrepreneur, *By 2017, the App Market Will Be a $77 Billion Industry*, (Aug. 26, 2014), at http://www.entrepreneur.com/article/236832.

[8] Forbes, *Big data and analytics market will reach $125 billion worldwide in 2015* (Dec. 11, 2014) http://www.forbes.com/sites/gilpress/2014/12/11/6-predictions-for-the-125-billion-big-data-analytics-market-in-2015/

The Trust Equation

Americans in every corner of our country, and in every facet of our personal and working lives, rely on digital technologies and the Internet. Reflecting this fact, the software industry is in the midst of a transformation. Our industry is changing from an industry that sells a product in a box to one that provides a range of data-driven services to our customers – customers who could be anywhere in the world. This shift means that an increasing amount of sensitive data – from an individual user's personal correspondence to corporate communications – is held by our companies on behalf of their customers.

This new technological dynamic is built on a foundation of trust: individuals and small companies will take advantage of the convenience of global, always-on services from a software company that holds *and protects* data. Those users must trust that our companies will guard their data with the best possible security and protect it from unlawful access – by anyone.

If consumers and companies do not trust that their data will be safe, they will be reluctant to take advantage of such software-enabled services. They will lose out on the cost savings and tremendous efficiencies that cloud computing can provide, all of which harms our global competitiveness.

That trust is currently being challenged by a range of factors, including the misperception that US law enforcement has unfettered access to the data held in US companies' data centers. In order to restore and maintain customer trust, BSA members believe Congress must update US privacy laws, particularly the Electronic Communications Privacy Act of 1986 ("ECPA").

BSA Supports the ECPA Amendments Act

BSA supports S. 356, the ECPA Amendments Act. We thank Senator Lee and Senator Leahy for introducing this bipartisan, bicameral legislation to modernize the current framework for law enforcement access to electronic communications in a manner that strengthens privacy protection while ensuring the needs of law enforcement are met. And we thank Senators Cornyn, Blumenthal, Coons, Franken, Vitter, Durbin, and Cruz, all members of this Committee who have cosponsored this important legislation.

We have been working alongside CDT and the other members of the Digital Due Process coalition almost from its inception. For more than five years, we have worked to close the loophole that allows access to email without a warrant based on the law's outdated conceptions of technology. When ECPA was enacted, the high cost of computer storage meant that email users who wanted to "archive" an electronic communication needed to print it out and file it in a desk drawer.[9] The thought of an inbox with years' worth of sensitive personal communication was simply inconceivable. It made a certain amount of sense for Congress to draw a line at 180 days and consider email older than that as "abandoned" and allow law enforcement access with something less than a warrant.

Today, ending this warrant exception is at the core of the ECPA reform conversation, and the ECPA Amendments Act is much-needed legislation that will help ensure continued user trust in digital services. The ECPA Amendments Act requires the Government to obtain a warrant for **all** electronic content and clarifies rules regarding notice to customers, so that companies can be transparent about privacy protections.

BSA supports the ECPA Amendments Act because consumers, businesses and governments all will benefit from greater clarity in the law about the appropriate ways for law enforcement to access data. Just

[9] In doing so, it should be noted, such an "archived email" again enjoyed the protection of the warrant requirement by being placed in a drawer rather than disappearing deeper into a virtual inbox.

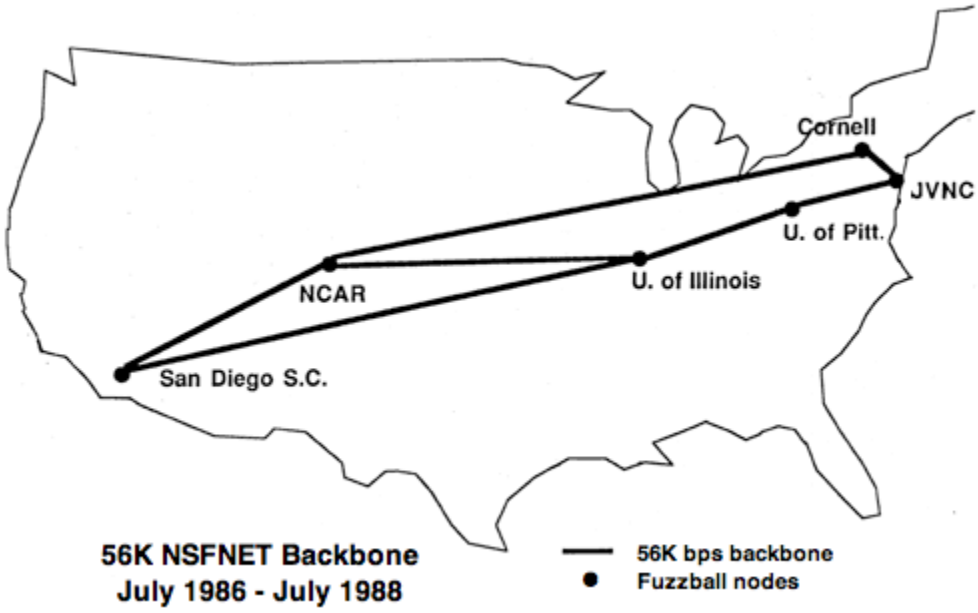
as the Government must show a warrant to an individual when it searches her home, the Government should show an individual a warrant authorizing a search of her email.

These "core ECPA reforms" are essential. Unfortunately, more than five years after we began the Digital Due Process effort, additional unanticipated consequences flowing from ECPA's age have emerged.

The Need to Address Cross-Border Data Requests

Today, in addition to ECPA's lack of a clear, consistent warrant requirement for access to data, it has become clear that the law provides no guidance for handling law enforcement data requests that cross borders. US law enforcement is increasingly using US process to gain access to information that is held outside the United States regardless of whether it is stored on behalf of customers in the United States.

Why did ECPA not anticipate or provide for law enforcement access of content stored abroad? It is helpful in this regard to remember that the "Internet," as we know it today, looked much different in the 1980s. In fact, today's globe-spanning network looked something like this:



Not only did ECPA not consider a world where vast amounts of data could be stored for mere pennies, it also did not imagine a worldwide network of connected computers and devices. The thought of being able to communicate in real time from our phones to nearly any place on earth was barely even the stuff of science fiction. The ECPA of that time did not consider that one day major US service providers would have customers in countries all around the world, or that they would be storing years' worth of their communications in data centers in a whole range of locations. Today, as one social media company portrays it, the Internet looks something more like this:

Source: https://www.facebook.com/notes/facebook-engineering/visualizing-friendships/469716398919

Today's Internet, clearly, is a much different network. Now, a person can log on to a computer in London in order to access their email, which is held by a US company on a server in Ireland, in order to email their family here in Washington. The network transcends borders. And while the Internet may easily reach across borders, the case is not the same for US laws.

Such an approach would never be acceptable in the offline world. Consider, for example, if the Justice Department were seeking evidence that was being held in a safe in a Marriott in London. The FBI would never serve a warrant on Marriott's headquarters in Maryland, demand that their employees send someone into the room, take pictures of the items in the safe, and send them back to Washington. Such a search would be seen as an incredible affront to British sovereignty.

This not only threatens the trust that our international customers place in us to protect their data. It also forces US software companies to choose between violating ECPA by refusing a US demand or breaking the law of the country in which the data is held. This is true even though there is a system for access to evidence held overseas – the Mutual Legal Assistance Treaty (MLAT).

BSA Supports the LEADS Act

BSA and its member companies support the bipartisan, bicameral LEADS Act to address this issue. We thank Senators Hatch, Coons, and Heller for introducing S. 512, and Senator Vitter and the other nine Senators who have cosponsored it.

As proposed by Senator Hatch, the LEADS Act creates a clear framework for access to data stored abroad. Warrants can only be used within the territory of the United States. LEADS recognizes that law enforcement has a legitimate need to obtain the content of electronic communications relating to US persons even when the data is stored abroad. LEADS therefore authorizes an ECPA warrant to be used for data stored abroad if the warrant seeks the content of a US customer. If the data of a non-US person is

stored abroad, then US law enforcement would coordinate with foreign law enforcement agencies to obtain the data, just as it would in the physical world.

One way that is done is through an MLAT.

MLATs create frameworks that allow a law enforcement agency in one country to obtain evidence located in another. The LEADS Act will improve and modernize the MLAT process. If the customer is not a US person, law enforcement can still obtain the data in a number of ways, including through the MLAT process. LEADS would require updates to the MLAT process to improve efficiency and transparency.

BSA supports the creating an international framework to address this issue. We believe the LEADS Act is a good way to accomplish this. Creating that framework will protect Americans' privacy by setting strong international standards. We will be in a better position to protect the privacy of American citizens if we are not setting an example for foreign governments to reach back into the United States.

Further, the international framework that LEADS creates is critical to the international competitiveness of US technology providers. BSA member companies are at a competitive disadvantage when competing for customers abroad if foreign customers believe US law enforcement will be able to access their information stored in their own country.

Finally, the LEADS Act also would prevent providers of data services from being put in the position of having to violate one country's law or another's when served with a US warrant for data of a foreign customer stored outside the United States.

Action in the Courts: A Call for Congressional Action

The misperception that US law enforcement agencies have unfettered access to data is exactly that – a misperception. But that misperception and the harm it is doing to user trust in software-enabled solutions is real.

Already, amid the ongoing international surveillance revelations, European governments and businesses are openly questioning the trustworthiness of US technology companies. The German government, for example, has crafted procurement rules that will bar many US companies from providing software solutions and services to the state. And the German government is not stopping there. They are sending signals to the private sector that industry should follow regulators' lead. But Germany is not the only example. Brazil, Nigeria, Russia, China are among the countries taking similar steps.

Perhaps most damaging to customer trust are real examples of US law enforcement trying to obtain data without using the proper channels. A case argued in the Second Circuit Court of Appeals in New York last week has the potential to set a significant precedent. In that case, the Department of Justice is seeking to force Microsoft to turn over the contents of one customer's email inbox. In the United States, such a demand requires a warrant, and the Department of Justice has successfully obtained a warrant for the information Microsoft holds here in the United States.

The problem in this case is this: Microsoft's customer is likely in the vicinity of the company's Dublin datacenter—where the data is stored—and which Irish law governs. In the same way that U.S. police can't simply fly to Ireland and knock down a suspect's door to raid their home, their jurisdiction online must be respectful of borders as well. Barging into an Irish data center, however it's done, would be an incredible invasion of Irish sovereignty. And imagine the uproar if foreign police tried such a move in the United States.

Instead, through a long-standing and well-developed process, many countries have developed rules for obtaining access to information that is held overseas. Those rules are embodied in Mutual Legal Assistance Treaties, or MLATs, and the United States even has an MLAT with Ireland. The Irish government has filed a brief in the 2nd Circuit case letting the court know that, had the Justice Department used the MLAT process, they would already have the information that they will be in court this week to seek.

Rather than using that MLAT process, however, the Justice Department is misguidedly arguing that a user's email belongs not to the user – but to the email provider. This flies in the face of what digital customers the world over believe about owning their own online files and communications, and it runs contrary to generations of understanding about the privacy of our papers and letters.

Consider the United States Postal Service: would the Justice Department ever try to argue that the contents of your envelopes no longer belong to you once they are dropped in the mail? They wouldn't, and that is the bedrock of the years of trust between customers and the companies and institutions we all rely on to deliver our communications.

Rather than taking this battle to the courts, we urge the Justice Department to work with governments and industry around the world to craft a forward-looking system to address these questions. The goal should be a system of rules that both preserves the rule of law and applies effectively across borders. If the United States does not take a lead in guiding this process, we will be left instead with countries racing to establish a system with the fewest protections possible. Such a regime would neither respect international sovereignty nor fundamental human rights or online privacy. As the digital economy continues to grow, our world will only continue to shrink. Already some online crime is global. The tools that law enforcement uses to investigate and prosecute such crime should be global as well.

That effort should begin here in Congress, with ECPA reform. As Judge Lynch noted in his concluding remarks, "It would be helpful if Congress would engage in that kind of nuanced regulation."

In the coming weeks and months, the court must wrestle with these issues itself. But the judges in the case already have made at least one determination: Congress needs to act.