golden frog™

reseller@goldenfrog.com | www.goldenfrog.com
Golden Frog, GmbH., Obergrubenweg 8, Meggen 6045, Switzerland

The Post Snowden World One Year Later: What Has Changed?

Increased awareness about government surveillance practices has changed the way society understands privacy, values and due process of the law, leaving individuals and businesses unsure about who has access to their private information. Now more than ever, we must work together to ensure that significant reforms are made to maintain the open and free nature of the Internet as we know it.

SPEAKERS

Marvin Ammori

Marvin Ammori is a prominent First Amendment lawyer and Internet policy expert. He has represented several companies and coalitions including Google, Dropbox, eBay, Automattic, Tumblr, Twitter, and others. Currently a 2014 Future Tense Fellow at the New America Foundation, one of the nation's most prominent think tanks, he also serves on the boards of the nonprofit advocacy groups Fight for the Future and Demand Progress and also on the Board of Engine Advocacy, a national organization that gives startups a voice in DCChristian DawsonChristian Dawson joined ServInt in 1998. He was appointed Chief Operating Officer in 2009. In his current role, he is responsible for the overall management of ServInt's business operations, including sales, marketing, business development and customer support.

Gregory Nojeim

Gregory T. Nojeim is a Senior Counsel and Director of the Project on Freedom, Security and Technology at the Center for Democracy and Technology (CDT), a Washington, D.C. non-profit public policy organization dedicated to keeping the Internet open, innovative and free.

Michelle Richardson

As Director of Public Policy, Michelle Richardson spearheads the ACLU of Florida's policy agenda by planning and implementing statewide legislative and advocacy campaigns, analyzing and drafting policy proposals, lobbying state, local and federal policymakers, preparing and presenting testimony, building and working with allied organizations and coalitions, and engaging ACLU supporters throughout the state.Amie StepanovichAmie Stepanovich is Senior Policy Counsel at Access. Amie is an expert in domestic surveillance, cybersecurity, and privacy law. At Access, Amie leads projects on digital due process and responds to threats at the intersection of human rights and communications surveillance.

Ron Yokubaitis

Ron is the Co-Founder and Co-CEO of tech companies: Golden Frog, Giganews, Data Foundry and Texas.net. Golden Frog was created to develop services that give people the ability to protect themselves online and access an uncensored Internet.

PANEL MODERATED BY

Michael Petricone

Michael Petricone is the senior vice president of government affairs for the Consumer Electronics Association (CEA). Petricone is responsible for representing the CE industry's position before Congress and the FCC on critical issues such as Internet freedom, wireless spectrum, and high-skilled immigration. He is a frequent speaker on policy issues impacting the innovation industry.

Full Transcription

Michael Petricone: Christian, thank you so much. I am thrilled to be here, thank you for coming. This is an extraordinary panel we have today. I don't know if you have ever watched the Rock and Roll Hall of Fame inductions where you have like The Rolling Stones and then they are up there with Nirvana. Then Jack White jumps on the stage. Then Run D.M.C. Jumps on the stage. Today we have that equivalent as a privacy panel. We just have a bunch of truly remarkable, amazing panelist. And we are going to have a good interactive discussion. I am going to try very hard to keep the discussion moving and just stay out of the way.

Michael Petricone: Let me introduce them very quickly. First we have Marvin Ammori, this is not going to be in order so you can raise your hand. He is an activist, he is a scholar, he's a writer, he is a one man internet defense team. He advises companies like Google and Dropbox. He currently has articles in Slate, Foreign Affairs and Harvard Law Review all at once; which is quite a trifecta. Next, Christian Dawson. You all know Christian, COO of Servlnt. One of the founders of the i2Coalition. I just want to say to Christian, I am hoping that everybody in this room is a member of the i2Coalition. If you are not, you ought to be because I see what Christian does in Washington every day. He does a tremendous job of representing this industry. As Christian said this started after PIFA and SOPA when Christian realized that one of the problems we had, one of the challenges we had is that the vast majority of members of Congress don't really understand how the internet works. And if you don't understand how something works it is really difficult to care about it. He help set up the i2Coalition. Their mission is to help educate Congress about this industry and how it works. He has being doing a fantastic job so please support him in the i2Coalition.

Greg Nojeim, Senior Counsel to the Center of Democracy and Technology. Renown expert on national security, terrorism and 4th amendment protections. Then we have Michelle Richardson, she is Legislative Counsel with the ACLU. The ACLU is a fantastic group. I just renewed my membership. You should too. She focuses on national security and government transparency issues. She also served as the Counsel for the House Judiciary Committee.

Amie Stepanovich is the Senior Policy Counsel at Access Now where in her on words she works hard to keep the government out of your life. That is a good thing. She also co-chairs the very prestigious Computers, Freedom and Privacy Conference.

Finally, Ron Yokubaitis is an internet pioneer who founded one of the first fifty ISP's in the United States back in the day. He is an old school internet advocate. Again, just a true pioneer of our industry and he is now CEO of Data Foundry.

Let's go into the discussion. The title of this panel is Snowden One Year Later. I am going to make a request of the panel. I think Snowden, himself, is an interesting guy and you can debate about him and his motivations and who he is and him personally. A lot of the debate has been focused around him as a person. I think, while it's understandable, that it has also taken away from the debate about exactly what our government is doing and what the response ought to be. Snowden while important, he is an agent, right? He is an agent of radical transparency. The real issue is our government and our government's actions. What I am going to ask the panel to do over the next hour is to the best of your ability don't mention the word Snowden and focus instead on the actions. That is what the real issue is all about.

Let me start with Amie. Just looking back a year, how do we get here? What have we learned over the last year about the U.S. Government's surveillance practices?

Amie Stepanovich: Sure. I remember a few years ago I was litigating Freedom of Information Act request against the NSA. The Freedom of Information Act allows you to go to government agencies and request documents. We were talking about their cyber security authority, about their surveillance actions. And all we would get was this hugest wall. We would hit a wall. The NSA would say no then the courts would say no. You just had no window into the National Securities Agency's activities whatsoever.

In the last year one of the things that we have been able to carve out using one of these documents that an unnamed person helped disclose, is this window into the activities of the National Security Agency and an idea about what surveillance activities are going on and to what extend those activities are unlawful. To what extent those activities go beyond the bounds of what we would like our government to be doing. Without naming many, many programs that have been disclosed and that I think a lot of people on this stage spent a lot of time tracking, trying to figure out how they fit together. I think the big thing we have learned is just the scope, the size and the extent to which our government is spying not only on people within the United States but also around the world.

Michael Petricone: Michelle, Marvin - anything you want to add to that? What specifically is our government doing that we did not know about last year that we should be perhaps concerned about?

Marvin Ammori: I took some notes on this so I can l give a few and then you can fill in if you like. This morning I decide to look through 'What do we know now that we didn't know last year'. I'll just give you a few examples of some of the programs that we know just so we can ground the discussion a little bit. What we know is that the U.S. Government collects records of who is calling whom for just about every phone call in the U.S. Let me know if I get any details wrong here. They are engaged in upstream collection directly from Telecos. They gather information about a target of the investigation even if the target isn't in the emails. They determine who a target is with only 51% presumption of whether or not a person is 51% foreign or not. If you are foreign they can just spy on you is the idea. They presume you are foreign unless they positively identify that you are not under certain circumstances. Despite the lax rules an NSA audit showed that they violated their own rules and policies over two thousand times within one year - about twenty seven hundred times. They, perhaps, destroyed evidence that the head of the NSA, perhaps, misstated the fact to a senator during a hearing claiming that there is no program under which they collect data on millions of Americans. We believe that the top lawyer for the government mislead the Supreme Court about the NSA's activities in an argument before the Supreme Court. They also intercept millions of images and use facial recognition on them. They collected two years of cell phone location data on American's as part of a pilot program. They have a program they call Muscular where they tap into the lines between data centers at Google and Yahoo, perhaps other companies. They have a Bullrun program that undermines encryption. Including undermining standards at the, sort of, national standard agency, NISS as well as paying a company ten million dollars for potentially back doors in their encryption technologies. And they also, to avoid some rules, apparently share data with the Five Eyes governments. New Zealand, Australia, Canada, the U.K. and the U.S., to be able to share information on one another's citizens. If you want, sixty five things you've learned in the last year are thanks to Snowden. The Electronic Frontier Foundation has a blog for this where you can read them and weep. That is what we know now among other things.

Michelle Richardson: I think the thirty thousand foot summary is we've learned definitively, since 9/11 all these changes in the law have taken suspicion based investigations. They no longer go after a suspected bad guy and build a case from him. They collect everything. If it's digital and it's collectible they get it. They don't believe you have any rights in that information and it can be used for all different purposes against you. That is how these programs are flourishing. This promise that somewhere in this data we are going to find a terrorist or the criminals and it will make us safer. Ultimately, that has not been the case. A year later lots of Congressional Hearings, there are no concrete examples of how domestic spying, especially, has ever caught a terrorist.

Michael Petricone: Can we just expand on that a little bit because before we delve into the implications of all this I've got to ask. A government's primary responsibility to its citizens is to keep its citizens safe. Our government says that these programs, like them are not, are necessary to stop terrorism and keep us safe. Why? How would you respond that, Michelle or why don't we start with Amie and then go to Michelle.

Amie Stepanovich: One of the programs that Marvin had alluded to is where the NSA is undermining encryption standards and I want to focus on that just for a second. What they are doing is they are actually making everybody less safe online in order

to preserve their own surveillance authorities. The encryption standards that we all rely on to protect our communications, our bank transactions, our emails, basically anything you do online have been messed with by the NSA behind the scenes in ways that not even the encryption setting body is aware of and has said that they have no idea what the NSA did or why, in order to make it easier for them to conduct surveillance. This idea that they are actually trying to make us all safer is undermined by their own programs and their own surveillance operations.

Michelle Richardson: There have been a number of terrorist attacks in the United States since the Patriot Act passed or the FISA Amendment Act. Like the Boston Marathon, right? All the surveillance and we didn't catch that before. They shooting at Fort Hood. We find, actually, in a number of these incidents the shoe bomber, the Christmas Day underwear bomber, these guys we had tips about but nobody ever ran them down because we are so preoccupied with big data. We've got all the guys in a room with a computer pulling down all of our phone records instead of putting the man power towards catching suspected terrorist in a way that has proven to work.

Christian Dawson: I'll tell you one thing. That we've seen reports now form both Forbes and The New York Times about the potentially billions of dollars flowing out of U.S. economy as a result of these actions of the NSA because of a lack of consumer confidence in the U.S. cloud and a belief that the U.S. cares about privacy. I posit that it does not make the USA safer to have a weaker economy and to have fewer jobs.

Michael Petricone: Greg?

Gregory Nojeim: One of the things that was most startling to me was in the revelations was that companies know when the government is making demands on them and they have to meet those demands. The law requires that they turn over data in response to those demands. What really struck me from the disclosures was that in addition to this coming through the front door - the NSA was essentially wiretapping the companies themselves. It was going through the back door intercepting the flow of data between the data centers the companies had that they had located to provide service that were better for their users. It really struck me that they were using this executive authority to get this data instead of going through the front door and saying, "We have a suspicion about this person. You must turn over this data."

Michael Petricone: I think that is a good summary of what we know. Yes?

Marvin Ammori: Can I just disagree on one point?

Michael Petricone: Okay.

Marvin Ammori: Not really disagree but a clarification.

Michael Petricone: Sure.

Marvin Ammori: Even if it did make us safer there is a sort of tradeoff. This class of tradeoff between liberty and security. Our founders gave us the Fourth Amendment protection against unreasonable search and seizure probably realizing that would probably make some people less safe. That is a trade off in a free society. You could move all the way to a totalitarian police state, have more security, but we have chosen to not go in that direction. I just wanted to say that even if there were examples of some terrorist being caught we is still want to make sure the tradeoff is worth it.

Michael Petricone: I think that is a good summary of what currently know. Let me switch topics. Given this information, let me go to Ron, what has been the business impact? The practical business impact on your companies and others in the hosting industry and why.

Ron Yokubaitis: The practical impact is that five years ago we got tired of talking to people and being looked at as nuts. Of course, we're from Texas so we're a right wing nut. You are an Alex Jones lover which he is a very interesting man. Nevertheless, we would talk about this and people would go, "Your are being surveilled. AT&T is surveilling you. Verizon is survelling you and you gave them permission in your term of service. You might need to be a Telecom lawyer to understand the terms but you give them permission. Of course, since we don't have an open internet, we have a monopoly internet, you had no choice. But what we did, recognizing the reality, 'What are we going to do about it'. We put the business into Switzerland. Because you are not going to buy from us, good Europeans. Because they understand it. We Americans may be dodos and believe our government, "Hi, I'm from the government. I am here to help you. We are going to regulate the internet and give you transparency", and all this yammer. We were going to sell the encryption to people. We put it in Switzerland. Now we are in a hundred and seventy countries. The world wants it. Mr. Snowden has woken everybody up that you could run on the internet. You just can't hide. If they want you they are going to get you - Osama Bin Laden. They're surveilling all of us all of the time. What are you going to do about it? We put it in Switzerland and now they are going to have to talk to a Swiss judge. Not me. Talk to the judge.

Michael Petricone: Christian, let me go back to you again. Same question, specific terms, how are hosting companies being impacted by this? What's happening?

Christian Dawson: I can tell you a little bit about my company and that the numbers are a little bit staggering. Our company has been around for nineteen years. Historically, we have seen more business come from outside of the United States than in. On the level of about 60% international business and 40% U.S. based businesses. In the past year 70% of our business has been U.S. based business so you are talking about a dramatic shift form 60% of our business usually being international to 30. I strongly believe that that can be directly attributed to what is going on with the NSA revelations and frankly how good the rest of the world is at marketing around those revelations.

Michael Petricone: Just to get a sense of the room. How many of you represent companies that host data or are cloud providers? Put your hands up. Okay, keep your hands up. Now, how many, with your hand up, if your business has lost a customer or a specific opportunity as a result of government surveillance practices. Okay, that's a good number. To Greg and Christian, are customers demanding? What do customers want? Do they want better protection? Do they want reassurances? Are they just pulling their data off and putting it someplace else?

Christian Dawson: We're really lucky if a customer tells us what they think. A customer can move their business in two clicks of a mouse. We have really anecdotal evidence about a lot of this stuff. But when the big numbers like that, going form 60% to 30% of international business we feel like 'Yes, they really are demanding more privacy." More transparency of how their data is being managed. We are trying to step up to the plate and give that to them.

Michael Petricone: Ok let's talk now about what's going on in D.C. Legislative responses, legal responses. Let's start with Michelle. Congress is now actively considering legislation to restrain the NSA's power. Most prominently the USA Freedom Act and other measures like the FISA Amendments Act. Can you give us in lay-men's terms, an overview of what these would do and would they solve the problem.

Michelle Richardson: Sure. This bill was introduced last fall. It is now passed the House with bipartisan support - Lots of cosponsors. It started in a much broader form, right? To address a lot of the different revelations but it has been whittled down and here is what's left. The phone program will continue in a much smaller form. All of the laws in the foreign intelligence statutes that allow the government to request records and digital information without a warrant, right, this is not the content but all of the data flow and the stored records, have to be based on selection terms. This is not narrowly defined but the idea was that you can no longer go to a company and say, "Give us literally everything. Every day download to the NSA". We are going

to come to you with some sort of request and this is getting towards what all of the advocacy groups wanted. We wanted them to focus on specific people. Maybe you go out, a ha, and see who their associates are but no more of this grab everything. It does leave some of things to be desired. We would want to really, specifically say with the selection term. This is like a name, an account number, a facility. Something much more specific. I think one of the things that's upset me most with revelations is that they have misled the courts. The courts are authorizing things that Congress and the public never envisioned. Even the ACLU got worked up about it. So now we need to be so incredibly specific about what we need. There is no warrant, perpetual secrecy, compulsory progress. It needs to be targeted. It is now on to the Senate. It will be in the Intelligence and Judiciary committees and we are asking them to be much more specific. Go back to the idea that you starting an investigation with a seed and you go out from there but there is no more bulk grabbing of all this data.

Gregory Nojeim: One of the important things about the legislation is it doesn't address your problem, Christian. Your problem is if you can't get clients from abroad because they are worried about the security of the communications that they have - and this legislation is not about that. It really only addresses the domestic use of these authorities. So for example, the program that allows the government to target a person abroad because they are a person abroad. That's it. That's the standard. It is not affected by this legislation. It is not going to be helpful to companies that want to give assurances to people who are abroad.

Michael Petricone: Amie and Marvin, let me just rephrase the question. Is the Freedom Act, as it currently stands, the answer here and if not what needs to be done? Amie.

Amie Stepanovich: Sure. I think USA Freedom Act, as it stands right now coming out of the house needs to be strengthened. It doesn't allow some of the terms we use in D.C. It doesn't allow bulk collection, necessarily, you can't collect everything, but it allows bulky collection. As in you might be able to put in 305 and get all of Miami which is greatly concerning and I think that needs to be narrowed down. And I wanted to touch base - there actually is another piece moving through Congress, that is not USA Freedom that I do want to highlight just because it might be of interest to people in this room. I had started talking about the cryptography standards and encryption. Actually, when that revelation came out NIST, which is I promise the only acronym I'll use, it is the standard setting body within the United States on encryption, said that they didn't know and they couldn't have known because legislatively, by law, they have to consult with the NSA on encryption standards. They have to get feedback. There is now a proposal that has passed out of House Committee that hopefully will be on the way to the House floor saying that NIST no longer has to consult with the NSA. They strike that requirement from the law which is a huge step forward and means that the NSA, in small part, will be taken out of the encryption standards. I think we are going to see a lot more movement on that front. Accesses have pushed for greater use of encryption by companies. We actually have Golden Frog as one of our supporters saying that more information needs to be protected.

Michael Petricone: Ron?

Ron Yokubaitis: Yes. Following up on Amie's point. The encryption standards are already compromised as soon as you are talking about it. The Surveillance State is going to put their work and break it. What the one thing that we do and I encourage, I spoke at LinuxFest last week. It was a response from one of the geeks in the audience. That was a pretty high dense geek environment. What about 'Let's all get together and agree on some standards and open sources?' My feeling was that is just serving it up on a platter. I said, "More of y'all need to start companies or create new encryptions among yourselves and between your servers and da da da da da. Let's get creative. We created a new one. We call it Chameleon. It's frustrating a lot of the great firewalls and getting people out of a surveilled state to the open world of free expression. I was just encouraging the geeks there to get busy. Let's use our creativity rather than ... I am not an inside the beltway person. We're out here not too far from the Mexican border in Texas. Some of us speak Spanish. We're just busy. Now, they are going to have a standard and pass legislation like this, but in Texas we did - last legislative session. We only let them meet every other year. We passed requirements. You've

got to have a search warrant for email. We've been working for six years in Washington so this Freedom Act is the ECPA. In Texas, of all things, to a lot of people there is a little bit more liberty left to the state and passed … Requires a search warrant for email and your web content. We made it for, not just email, but content. We suggest y'all go back to your state legislatures and do the same thing. Florida has looked at it, South Carolina. Andy McFarland ran that for us. It is y'all go back. Inside the federal these folks will represent you. Join their organization they do a tremendous amount of good work but still it's all open. You just got to go back to hack for liberty in your own damn town. Your own state. It is that diversity, that where they just can't control it so easily. We were at LinusFest and folks were kind of thinking, 'How can we do this'. Said, "Well, you know. Let's rent some hosted machines. Just set up chat channels, email and just have them talk. Have them use all the key words that they are going to surveil on and just feed them bull corn. Let them store a bunch of bull corn. Let them send their investigators looking at these terrorist or whatever it is and just send them spinning around. If they are going to have the Surveillance State, it is like in the old days when I had learned to program computers. You know you had punch cards and they would say on them, "Don't fold spindle or mutilate". A lot of people would fold the corners so the program wouldn't run. You know, hack it up. I am saying we are just as citizens, as free born people, have just got to learn to disrupt. They are going to surveil us. I don't have … I have zero confidence that we are going to get any transparency out of the Federal Surveillance State. No matter what they say, they are going to nod and go ahead and do whatever they want. It's really what are we going to do to hack for our self for liberty and freedom and join other people who are concerned about it around the world. It's on an individual basis. I am not very confident any more about, 'we're going to set some policy and there is going to be transparency'. It is a nice effort and I agree with it but you've got to work on that front but I think individually you've got to arm up and encrypt. As Snowden says, "Now you are not a paranoid freak". Snoweden says it's encryptions. You've got to encrypt up.

Christian Dawson: I do agree that our customers are demanding in encryption to the point where I really feel that as though, and you mentioned this, the surveillance state, what we're seeing is the next Cold War is really going to be the encryption economy versus the surveillance state. We are part of that encryption economy giving our customers what they need. Honestly, making it more difficult and more expensive for the NSA to continue doing what they are doing while at the same time being practical and sensible actors when we engage law enforcement. When they come to us for warranted content we want to make sure that they have the proper tools that they need to get what they need to solve their problems.

Michael Petricone: Let me just pick up on that for a second.

Christian Dawson: Yeah.

Michael Petricone: So far you have been talking about the NSA disclosures and they focus on the NSA's capabilities to obtain information covertly. Thinking of the people in this audience, let's suppose as you were talking about you are a cloud provider and the government requests your data. Do you have to comply and is there any legal recourse?

Ron Yokubaitis: You do.

Christian Dawson: It depends on what form.

Gregory Nojeim: If it's a lawful request, yes.

Christian Dawson: Yes, lawful request.

Gregory Nojeim: If it's not a lawful request…

Christian Dawson: You don't comply.

Gregory Nojeim: Then it should push back. That is why a lot of firms have a lot of lawyers who can push back.

Marvin Ammori: Can I ask you a question? The people who had their hands up, that are with companies that host data, could you raise your hands again? How many of you have a lawyer on staff? Keep your hands up if you do.

Gregory Nojeim: How many of you would like one?

Marvin Ammori: About 90% of the hands went down. What should they do if they're faced with a situation? Should they call EFF? Call VA Cellular? What should they do?

Gregory Nojeim: People call EFF

Marvin Ammori: The Electronic Frontier Foundation.

Gregory Nojeim: As you know there are outside counsel.

Marvin Ammori: They might not know. Tell them who to call.

Gregory Nojeim: There are outside counsel and you probably want somebody who is local who will know the law because they have a lot of clients that do compliance. It is good to have somebody who you can call when those questions come up. One big question, I want to allude to what Ron was saying, was what do you do when you get a demand for content that is in the form of a subpoena. That is one of the big problems right now and the reality is that there is a 6th Circuit court decision that says law enforcement needs to have a warrant for content. The large providers, pretty much across the country, are requiring warrants for content. If you are not doing that you should know that you are something of an outlier particularly with respect to the large companies.

Michael Petricone: Yes?

Ron Yokubaitis: I would just like to follow up on the outside counsel. I am a bringer. I used to be a trial lawyer until I started an internet company in '94 but I also practiced criminal trial law. I am a little practiced in saying no to law enforcement. That is really the most important word is no. You've got to go back and get this right. You've got to dot your i's, cross your t's. In the previous panel, you didn't get to see, it was downstairs, upstairs, I am not sure, but you might rather than get your usual exorbitant and hourly rate civil lawyer, I would talk to your criminal bar. The criminal bar, they know how to say no to law enforcement because they are constantly doing that. They are a much braver bunch of folks than, 'Well, let's see how complicated we can make this' because that runs up the billable hours and they'll probably give you some free advice for sending them some DWI cases which everybody in the room here has under threat. Consider your local criminal law. Make friend of your DWI lawyer. He knows how to make sure you only say, 'Keep your mouth shut and only say stuff that your are compelled to say. You are required to say'.

Michael Petricone: That is good advice.

Marvin Ammori: Can I get to more...

Michael Petricone: Sure.

Marvin Ammori: Sort of non-policy, non-legal, to some extent, things that people have done. In the last year, after the revelations, a few companies have done two things that are non-policy. One, there has been a rise in transparency reports. A

lot of bigger companies and some of the smaller companies now issue a report every year detailing the number of warrants, subpoenas, national securities letters, all of that to the extent they can in a report. Two reports that were fairly good recently from smaller companies on a pretty big … The Dropbox report was very good, had a lot of transparency in it. I thought the automatic WordPress.com report was very good. Dropbox also answered a set of principles that they set out for their users including posing to make a request and trying to treat all users, foreign and American, the same. Transparency reports are something companies have done. It doesn't require you going to D.C. It doesn't even require … Consulting with a lawyer a little bit but it gives your clients and understanding as to how many requests you might be getting. Especially when Europeans assume that you're just handing stuff over to the NSA on a day by day basis. That is one thing.

The second thing is and this just happened a week ago, something interesting. There was a day of action called Reset the Net. If you go to resetthenet.org you'd see all the companies that were involved. On this same day, I think it was the one year anniversary or around there at the revelations. A whole bunch of companies announced new encryption and security tools for their users. Google was part of it, Twitter, Dropbox, Mozilla a whole slate of companies. I think Mozilla. What they did is they, I thing Google announced new encryption in some of their email. If you have new security tools you want to embed and use. If you make it clear to your users why you are doing it and that is sort of part of fighting the surveillance state or making users more secure. Those are two things that you can do that are sort of non-legal and people are doing to sort of respond to revelations. Transparency reports and added encryption.

Christian Dawson: One plug for transparency reports is that the Internet Infrastructure Coalition, the i2Coalition is, we are collaborating with the BMI Technology and OTI and the Berkman Center. They are doing the heavy lifting. We're consulting with them. I am trying to create templates for transparency reports for companies like ours. If that is something you are interested in finding out more about come to the i2Coalition booth.

Michael Petricone: Let's switch back to policy again. If there is one thing this industry has learned over the last couple of years it's the engagement with government, if done smartly and strategically, it works. It worked with PIPFA, it worked for SOPA, it's worked with other issues. The government can be made to do things and not do things. Let me just address the panel. I am going to go down the line on this one. Assuming there are people in this audience who are convinced that government surveillance practices are damaging their business and their ability to compete internationally and they want to engage and make the government adjust its surveillance practices so they are not damaging. How do they engage? What do they do? Christian.

Christian Dawson: I have been so convinced over the past couple of years that we have a tremendous amount of strength if we come together with a singular voice. That is why I helped build the Internet Infrastructure Coalition and why I ask everybody in this room to become a member. Groups like CEA are also fantastic in helping us drive forward our goals. Really, join business groups. Use your business expertise in a collective way and help us achieve this stuff together.

Michael Petricone: Marvin.

Marvin Ammori: Being in D.C., D.C. is a totally different world from most of the rest of the country. It is a place where every other person is a lawyer and they assume every company like the second hire is a lawyer who is complying with rules. They only hear from really big companies that have lobbyist on hand – entire lobbying firms at their beck and call. The way that government officials get information is from really huge companies, legacy companies and from the intelligence agencies. Two things that you guys can do to help. One, they never hear your stories. They don't know anything about, from what I can understand, they don't know much about smaller business. To the extent that i2C and others can tell those stories. 'Here is what it's like to have a small business. Here is something we face', this something that the CEA did very effectively where they flew in CEO's of startups and smaller companies. Just understanding what you guys do and that it is so different from the bigger

companies they hear from every day. They hear from the oil companies to the Telco's. So, one, simply telling your stories, and it is probably most effective to do through an association. The other thing is getting your users engaged. It is something that is sort of delicate and you don't want to do every day but even just sort of informing your users, posting on your blog, letting them know what you're doing. Your users probably love you. If your users ever pick up their phone and call their member of Congress, those things actually have an impact. Actual stories and real life impactive laws I think actually has more of an impact than you'd expect.

Michael Petricone: Greg.

Gregory Nojeim: I think in engaging with your local elected officials, as Ron was saying, and with you with you federal officials is really important. We've been working, for three years now, to try to get this warrant for content rule established nationwide. Every now and then we get a call from Data Foundry saying, "Hey, we just delivered another cosponsor for your effort. We have almost half of the House of Representatives cosponsoring this bill."

Ron Yokubaitis: No, it's more.

Gregory Nojeim: You know what? Texas went ahead and did it. They went ahead and did Warrant for Content because people in Texas, a lot of the supporters were companies who would be affected by it, went to their local legislatures and said we want this and here is why. I think that can be very, very affective.

Michael Petricone: Michelle.

Michelle Richardson: I'll just echo that. Right now the game is in the United States Senate. Many of you are probably from California and probably the number one decider over in the Senate is Senator Dianne Feinstein and she needs to hear from you. Our pleas of privacy have not gotten through to her. She may be more open to hearing about the business impact this is having and we would love for you to reach out to her.

Michael Petricone: Amie.

Amie Stepanovich: Stay very well informed. There are groups that are trying to let you know when action is needed. I would pay attention to those groups. I would start, if you are going to collect information about people, I would discuss in advance what you are going to do to protect that information. That is so incredibly important. Making sure that the federal government is not going to tap in to your backbone and get information off of your servers or about your customers. If you are not having those conversations early it might be too late and you are not going to want to be the company that is in the next story about how the government is getting unauthorized access to your equipment.

Michael Petricone: Ron.

Ron Yokubaitis: My understanding is there are now two hundred and sixteen sponsors to the bill when we last left. It needs two eighteen. Just call your local Congressman and Senator and ask them if they sponsored this. There is a lot of people of good will that are there who if they knew it wasn't on their priority list for legislation. They are, "Lord, really this". We are talking about extending a search warrant to their email and your web browsing of you and your staff. That makes a lot of sense. They need minimum two more sponsors and I am not up on the legislative, the parliamentary of it but that is what gets them over the hump to where it's going to go the next step. It needs that step. Everybody here, if they called, should be, it'll get it over the top. I'll say that.

Michael Petricone: Christian. Then we are going to do questions and answers so please start formulating questions.

Christian Dawson: One more thing. We started this fight talking about what we have learned in the past year and I think honestly, the scariest thing we have learned in the past year is that there has not been a tremendous amount of outrage from the American public over these issues. There are not pitch fork building mobs of citizens at the gates of the NSA or in front of Congress demanding change. These are things that we think are extremely important to the future of America, the future of the economy and the future of the world. The one thing that I ask you guys is to not get complacent and to do what you can to help drive forward these very important issues.

Michael Petricone: If I can add to that, there is no more powerful lobbyist to your member of Congress than you as a local job creator. Members of Congress, Republicans, Democrats, they disagree on a lot of things. Right? But the one thing they all agree on is they want to come back. That requires being re-elected. As a job creator you are critically important. The NSA practices, are they necessary to combat terrorism? You can have a debate on that. Is the person this panel is named after, is he a hero or not a hero? You can have a wonderful debate on that. But when you go in and you say to your member of Congress, because of the government's practices, I, your constituent, I am losing jobs. I am unable to hire. I am losing jobs in my company. That is tremendously affective because every debate, every discussion in Congress right now, every issue, it comes down to jobs. That is far away the most effective way you can frame this debate or any debate - so with that let me go to the audience for questions. We maybe have a microphone or else you can speak very loudly. Yes?

Jeff: I'm a ...

Michael Petricone: Can you just say who you are and who you are with.

Jeff: Exactly, Jeff

Michael Petricone: A microphone is on its way.

Jeff: There we go. I appreciate it. A comment was ... Can you guys hear me?

Michael Petricone: Yes.

Jeff: A comment was made earlier about 4th Amendment protections. I just kind of pose the question, especially since we have attorneys on the panel, that it is not purpose of the 4th Amendment to protect against search and seizure as search being a quest for evidence -and the NSA not being a law enforcement agency, not looking for evidence, not using it to prosecute Americans. I just kind of pose that as a question...

Michael Petricone: Who wants to take that?

Gregory Nojeim: There is actually two legal regimes. One is a criminal regime and the other is the intelligence regime. On the intelligence side ... On the criminal side to get content you get probable cause that a crime has been, is being willfully committed. On the intelligence side you prove probable cause that the person you want to surveil is an agent of a foreign power. Like a terrorist organization or that they are a spy. There's different standards and that is for surveillance in the United States. For surveillance outside, the constitution doesn't extend outside. Rights don't extend outside. The law permits the government to surveil a person outside because they are a person outside who is not American.

Jeff: With that said my argument becomes ...

Marvin Ammori: Let me respond then, let me respond. My point was that our founders realized the tradeoff between security and liberty. To the extent that, and historically there was a division between surveilling Americans and surveilling folks outside. A lot of these programs involve surveillance of Americans. What we have to do is we have to think through is it worth the tradeoff between security and liberty to have the kind of surveillance we are having over Americans. We can get into the legalities of whether or not the 4th Amendment extends to American companies housing foreign data or not. There are lots of different arguments you can make but my point was even if we caught one terrorist as a result of surveilling all Americans, we'd have to ask, "Was it worth it?"

Michelle Richardson: I think there is a misunderstanding there about the 4th Amendment. It applies to the entire government not just law enforcement. It may flush out different when they do searches and seizures for different purposes and they've got all these different test depending on what type of information it is. I think long term we want to move towards a 4th Amendment where you need a warrant to collect anything - whether it's a record or its content. That has come together in a digital world that just does not make sense to separate anymore. That is where we want to be.

Marvin Ammori: I don't get that.

Michael Petricone: Yes.

Ron Yokubaitis: Ron Yokubaitis again. All of this is just really trenched. There's another little thing that is going on and part of what's has been hanging up the new electronic privacy act, the American Freedom Act, has been the SCC wanting to have their back door an exception and flaunted it around terms like 'an administrative search warrant' with a lower standard than probable cause - the bureaucracy protecting itself. You notice there has been no perk walks on Wall Street since The Great Financial Crisis so the SCC is obviously doing its job. They want to not surveil miscreants they want to surveil us. They are using kind of trick language, a search warrant, an administrative search warrant, at a lower standard than the probable cause standard that Greg enunciated for the criminal warrant. It kind of gets mumbo jumbo but the bottom line is you've got to learn to say no and make them prove to you their authority and to get all this stuff. Make them dot their i's, cross their t's. You don't have to be a lawyer to say no. They've got the burden. You don't have the burden. The government has the burden to convince you. And hey, they are not going to haul you down to jail, y'all. You know they're just going to go on to the next one that is dumb enough to agree with them. So, stand up. Your own private - drink a cup of coffee and say no. It's not real hard. You don't need a lawyer.

Michael Petricone: We have time for maybe one more question. Do I see anybody? Okay, let me ask one. Generally our industry is our strategy is to avoid regulation, we don't like regulation. On the other hand regulations might be able to bring some clarity to our obligations as hosting and cloud providers in response to government data request. Should we be requesting additional help in the form of regulation from Congress, the regulators? Greg.

Gregory Nojeim: One thing that I think lifts all folks is clarity. We have an unclear statutory regime that everybody is laboring with. That is not good for privacy because people don't know when their data is going to be given away to the government. It is not good for law enforcement - they don't know what process to use. And it is not good for companies who are caught in the middle and have to hire lawyers to deal with all these request. The Email Privacy Act that Ron is talking about would add a degree of clarity and require this warrant for content. The USA Freedom Act, I think intended to deal with a serious problem that would add some clarity but frankly it's gotten so weak that we can't tell you to just go out and tell people to support it. It needs serious strengthening.

Amie Stepanovich: As to Greg's point. We have a Section 215 authority under The Patriot Act that says that you can only get business records that are relevant to an authorized investigation. And as clear as that language is, you already have a court saying that all records within the United States could be relevant to an authorized investigation. So we are looking at additional

to further clarify the language that we thought was clear. So it is a really huge problem where people have spent their entire career studying this language have no idea how things are being interpreted and how they are being rewritten.

Michael Petricone: This has been a fantastic panel. Thank you very much to our panelists. Support these companies. Support these groups. Have a wonderful time at hostingcon. And a mandatory plug, please come visit our little show every January in Las Vegas called the International CES. You are all invited. Have a wonderful day. Thank you.