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

LinuxFest 2014—Protecting Digital Privacy in the NSA Era

"Online Privacy" and "Internet Freedom" are at the top-of-mind for many because of the constant new revelations about government surveillance, and massive data collection by corporations. Golden Frog is pleased to welcome a very distinguished panel that will examine the current state of online privacy, what simple steps citizens can take to protect themselves and where government legislation is heading in the "NSA era."

SPEAKERS

Ron Yokubiatis, Co-CEO of Golden Frog

Ron Yokubaitis 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.

Scott McCollough, Principal at McCollough|Henry PC

W. Scott McCollough is an attorney whose practice focuses on telecommunications, Internet law, and economic regulation. He represents the interests of consumers, competitive communication companies, and technology application or service providers.

Scott Henson, Policy Director at Innocence Project of Texas

Scott Henson is a political consultant who has worked on Texas criminal justice policy for twenty years. He writes a widely read blog at gritsforbreakfast.org and is a co-founder of the Texas Electronic Privacy Coalition.

Brian Hauss, Legal Fellow at ACLU

Brian Hauss is a legal fellow with the ACLU's Speech, Privacy, and Technology Project. At the ACLU, he has worked on a wide variety of free speech and privacy litigation, including challenges to the government's use of location tracking technology, the suspicionless search of electronic devices at the international border, and the compelled disclosure of an internet service provider's private encryption keys.

PANEL MODERATED BY

Justin Freeman, Corporate Counsel, Rackspace

Justin Freeman is Corporate Counsel at Rackspace Hosting. With expertise in both the legal and technical areas of the rapidly expanding field of cloud computing law, Justin primarily represents Rackspace Hosting in technically complex enterprise transaction agreements (with a focus on Rackspace's OpenStack portfolio), data privacy and compliance matters, legal review of product development efforts, and public policy matters with a focus on intellectual property, security and privacy issues.

Full Transcription

Justin Freeman: We're going wind our way through a couple of topics focusing on data privacy, internet security and open access on the internet. I'm going to pause naturally between some of the topics so feel free to hold your questions but ask them based on each topic throughout the presentation.

Introducing myself, I'm Justin Freeman. I'm the corporate counselor with Rackspace. I'll be moderating today. Going down the panel here, in no particular order from my left to the end is, we start off with Mr. Scott McCollough who's the principal of Nicola Henry PC. He's an attorney whose practice focuses on telecommunications, internet law, economic regulation and he represents the interest of consumers, competitive communication companies, and technology application and service providers.

To his immediate left is Mr. Ron Yokubaitis, the co-CEO of Golden Frog, Giganews and Data Foundry. Ron has founded a number of tech companies including Giganews, Data Foundry, and Texas.net. Some of you probably used that for your modem access back in the day if you were up in Texas. Golden Frog was created in particular to develop services that give people the ability to protect themselves online and to access the internet in an uncensored fashion.

Directly to his left is Mr. Brian Hauss, who is a legal fellow at ACLU. Brian is a fellow ACLU speech, privacy, and technology project. He's worked on a wide variety of free speech and privacy litigation including challenges to the governments use of location tracking technology, the suspicion list search of electronic devices at the international border, and the compelled disclosure of an internet service providers private encryption keys.

And down at the far end here, we have Mr. Scott Henson who is the policy director of the Innocence Project in Texas. Scott's a political consultant who's worked on Texas criminal justice policy for over 20 years. He writes a widely-read blog at gritsforbreakfast.org and is co-founder of the Texas electronic privacy coalition. I would like you to join me in welcoming our panelists.

Privacy's a pretty broad area. We're going to dice it up a little bit but just to kind of kick it off with something, put a pin on it, I'd like to just go head and start with you Scott. What do you see as the biggest threat on consumer privacy in the technology space and do you have any solutions you would propose to either illuminate, litigate, or alleviate that threat?

Scott McCollough: I consider that there are really three basic problems and one really important potential solution. Society is now becoming much more aware based on these Snowden revelations and other things. I don't think that folks really understand the scope of surveillance that we have in our society today; both by governments and private interests.Nor do people really understand how the information is being captured and what it is used for after it is being captured. Many folks may believe that they have nothing to fear from a surveillance society. I think that everybody does. People close their blinds to their windows at the house for a reason. They close the bathroom door for a reason. Everybody has something to hide.

To bring it home to the electronic society, if you happen to be using a tablet or cellphone while you're sitting on the toilet, folks may not be aware that there's a technology that allows the webcam to be turned on and the microphone be turned on; even if perhaps the on switch is not on. They can see everything in its glorious detail. People do have something to hide; even honest, upstanding, god-fearing citizens. In fact, I would suggest that in some respects they have the most to fear from a surveillance society.

Justin Freeman: Ron, I would like to hear your thoughts.

Ron Yokubaitis: Well, I think I am here. Can you all hear me all right?

Male: Yes, perfect.

Ron Yokubaitis: I would say even non-god-fearing people have a lot to fear too. It's everybody .... Can you still hear me? I'm just trying to unplug the device. Even like I said, non-God-fearing. This is something that we've ... Can we get the audio down. Do we have an audio control on here? That's better ... we filed back in '06 about this with the FCC about the deep packet inspection by AT&T and it's in your terms of service. So anybody with AT&T service, you gave them permission when you clicked right in considerations in filtering spam and everything to collect all your data and keep it safely [inaudible 00:05:34].

That's the short for the legal jargon—you didn't read and you don't accept an Internet or Telecom board to really snap to what they are doing. You already gave it up voluntarily. It's hit with all the Linux gurus in the room—ya'll are giving up stuff right and left, the Gmail account of course.. now Google says "Ah, we have encryption to protect your privacy".. except you can't do it; you can't protect it from Google. Nevertheless I am just so happy that Mr. Greenwald got people's attention because you are just crying in the wilderness and even good geeks sit here and just push, push, push back, but you are not going to be anonymous.

That is ... We've argued against that on Usenet—you can run but you can't hide. You can do all sorts of things but if they want you, they are going to get you and if you don't believe me go and talk to Osama Bin Laden. Again, with Bitcoin it's not anonymous, it's just pseudo-anonymous, they even say so. The block chain is a sausage but still they can chase back down that chain. You just need to put your clothes on as Scott would say . It's not so much that you've got something to hide, just my wife taught me long ago in every family, it's just none of your damn business, it's that simple. It's none of their business. You have to private stuff and it's yours. I think Andy Everton in Washington has got Senator Cruz to say an answer to a question ... Is people's information their own property, their private property and he said yes. Well that is what they are getting, they are stealing your private property. You wouldn't do that. You've got to hold on to your wallet and keep it out of view. I would just try and activate it personally, you are going to take the blinders off. I'm sure you secure your networks and servers and everything but here you are flapping in the wind out here. It's ongoing but we are not going to be anonymous, we're just going to be able to let them go pick the low hanging fruit next-door. We're just trying to not be the nail that sticks up too high.

Justin Freeman: Brian, your thoughts on the largest threats facing consumers?

Brian Hauss: My pleasure. I'm going to start off by just issuing a general disclaimer. What I say here are my own personal views and not the views of the ACLU. I think the biggest threat in the world of privacy is what I call the mosaic problem. All the time, consumers and citizens are giving up lots of bits of seemingly anonymous information; where you are, what your IP address is when you login, all kinds of ... Just tiny little bits of data that you are just giving up all the time as you go about your daily life.

In addition to just location information or IP address, you also got now biometric data—fingerprints, eye scans, and face scanning technology is something that we're seeing increasingly used. The government and large corporations like Google or Facebook or what have you, are increasingly able to collect, retain, store, and analyze this data. Then thanks to the use and development of big data algorithms, they are able to take the data and figure out incredibly personal things about your life.

They can figure out whether you are a heavy drinker, whether you cheat on your spouse, what church you go to, what libraries you visit, how late you stay up, when you get up, all kinds of things. Even just little variances in those things can be surprisingly revealing about the personal things that are going on in your life, what you are thinking, what you are doing, what your habits are, what your vices are, what your virtues are. These are things that we traditionally thought of as private that the government couldn't get without at the very least a warrant. Sometimes we thought that they were just practical barriers that prevented the government from getting it at all but increasingly, the government is able to figure out all these things and it's able to figure it out from data that is publicly available to it, at least under current laws.

I think the big problem today is how do we address this Mosaic problem. It's a hard thing to do. I think the first step is just to recognize that there is a problem. In that regard, I think Edwards Snowden's revelations had been incredibly helpful for showing people the scope of the surveillance that's been going on, the size of the dreadnought that everybody's getting caught up in. Once we recognize that there is a problem, the next that is figuring out what to do about it. I think a big step in that regard would be to pass significant legislative reform. The electronic communications privacy act is more than 20 years old and it's about time it got updated to actually regulate the technologies that exist today.

In 1986 you didn't have Google, you didn't have Facebook, email was a completely different kind of thing. You would actually just download it from some server and store it on your laptop and you wouldn't keep it up in the cloud forever where it is now. That law is just not at all designed to protect the kind of information that we actively store online now. In addition, we want to encourage companies to self-regulate. If companies realize that consumers really care about the privacy, that they value it, that it's not something that they can just take for free, that there are economic cost to invading consumers privacy, then I think we will start to see more self-regulation from companies and hopefully will move toward a more privacy protected sphere.

Justin Freeman: Great thinking Brian, Scott, your thoughts?

Scott Henson: Thanks for having me and I apologize, I've got a little cold coming on so nobody shake my hand and I apologize for my…. There you go. All right. I guess the thing I will add is that there are just a lot of layers to these issues. It's like peeling back and onion. We have to distinguish between the federal and the state areas. The federal EPCA as we just heard is a mess. It was kind of a mess in 1986. It is just a ridiculous mess today. It was written at a time when no one had any … written at a time when no one had a significant amount of storage, how much storage was on your computer in 1986. The idea is that someone would keep 10 years' worth of email was deluded, almost mind blowing. Who doesn't have that or close to it somewhere on an email account? Texas law incorporates EPCA by reference. It says that they can get it under these three different standards that all conflict or you can get something under that federal EPCA standard. We sort of linked ourselves to that. As far as … Another thing I would add on the commercial and the consumer aspect, I try and make a distinction between some of the commercial privacy issues and issues surrounding law enforcement and the government.

I think it's one thing if you're sharing data in an app via these terms of agreement. It's another thing if the police just have the authority to track you because they also then have the authority to try and arrest you and put you in jail. Those raise civil liberty's issues beyond the terms of service. I couldn't agree more, that is another big mess that I don't know how to get out of that hole…

There was a famous episode about—I'm sure many people here have heard of — where a company in England created terms of service as sort of a satire spoof and said, this isn't an exact, but something to the effect of, "If you sign these terms of service, you agree to hand over your firstborn to Satan and to pledge your eternal allegiance to his dark holiness or whatever it was." And did this for several weeks and then announced it, "Hey this is just a joke, just wanted to let you know that nobody is reading these things." That no one in that whole time had ever read through it and say, "Wait, can I get your email service without selling my firstborn to the Dark Lord." That is a huge issue but I think that it is separate to me from some of the law enforcement issues which are just cleaner. You're just handing out so much consumer information that it just makes a lot muddier and there are some people who would say, "You know what, I'm willing to give a little personal information to a company because I want a dollar or a quarter off of my next box of detergent," or whatever it is they are going to get savings for that. That is muddy. The law enforcement issues to me, do you have to have a warrant? Does the law enforcement have to have a warrant? Does the IRS have to have a warrant? That's … Yeah go ahead.

Ron Yokubaitis: Yeah Scott. When you were talking about how Texas refers to the ECPA, the Electronic Communications Privacy Act in the last legislature I believe we passed the statute… because I know Scott wrote some of it and Andy… [inaudible 00:15:25] that is that in Texas now, a search warrant is required for email, content of your Internet communications. We have done a remedy in Texas. We're the only state so far. Other states have been looking to follow in Texas' steps. You know, Andy

that works with us, went to South Carolina and in Florida. We are trying to get the ECPA in Washington where it's the crips and the bloods - to follow the Texas statute that they require a search warrant and probable cause they are going to do surveillance. We are freer here in Texas than any other state. You are more secure and more private in the law enforcement issues.

Scott Henson: On email content. There were two big bills last session on these topics. There was one on Geo-location data and there was one on the email content. Email content passed, geo-location data was approved in one chamber by 126 to 4 vote and in the other chamber, didn't get out. The geo-location really is what I'm referring to. Definitely email was good, the email content was great. I will tell you, the tea party folks were ready here in Texas, it's kind of funny. The breed of Republican who is populating the Texas legislature today is not your granddaddy's Republican. It's pretty funny to see some of the more libertarian minded kind of folks who see this stuff and just automatically … "Well obviously they shouldn't do that." It's been pretty remarkable.

Ron Yokubaitis: The days of law and order of the Republican Party is now over because you've got too many tea party people coming in and saying, "Problem with the constitution."

Scott Henson: It's funny, some of these guys believe their own hype. You hear it and it sounds, "Oh that's government, hypocritical." Some of them are fairly real about it. I've had tea party type guys telling me, "Look, the US incarcerates more people than anyone else in the nation. Texas incarcerates more people than any state in the nation, which is true." If I'm for less government then how can I actually support that. How can I not try and scale that back? Some of those guys believe that stuff, that's not just rhetoric to them and they are in charge of that, so you will see …

Scott McCollough: I don't know if there is enough copies, but I left a recent poll … Some thirty copies of a recent poll dealing with how the various liberals versus conservatives view the NSA program in particular. The information is quite surprising. Almost across the border, you will find that we think all conservatives are far more opposed to the NSA surveillance program then our liberals. There is a bit of an over generalization but generally speaking you will find that in today's environment, those who call themselves conservatives are far more suspicious of surveillance programs by the government then are those who call themselves liberals.

On the other hand, you will find the conservatives are far more understanding and willing to countenance the gathering and use of information, private information, by private companies. In my own personal opinion, I am concerned about both because ultimately if a business gets it, then of course they can use it for its own purposes but also once a business gets it, then the question becomes how easy is it for the government to then obtain it?

Brian Hauss: If I could just jump in for a second on that. The third party doctrine is this kind of strange document constitutional law document when it came out in the 70s but what it essentially says and what the government is used it to say is that when you give a business your private information, even if that information is basically necessary for that business to operate …

So your cell phone location is used by cell phone companies to provide a cell phone service. As a result, they also collect private information about where you are through your cell phone just pinging the cell towers. Then the government and then the cell companies say, the consumer has already given up that information to you, no more expectation for privacy in that information, you have to turn it over to us. Enter the third-party doctrine now, what happens when you give information to a business, the government then comes in and say's well there is no more privacy on this information, it's already been given over so we are entitled to it.

That's really I think … In the constitutional sense, they are connected in that way and that's why I think it's really important maybe

legislatively to try to overturn the third-party doctrine so the ACLU can hide in the courts to try and limit it because clearly the results were never intended or foreseen by the Supreme Court when they handed out that decision, bad decision.

Justin Freeman: It sounds like we have a consensus then. A couple of things. First of all, one of the major problems facing people is that lots of private companies gather lots of data about you, which could be accessed by law enforcement or which they can share, putting together a big picture of you that substantially invades your privacy.

Do you guys think … You've talked about how problematic it is when companies use and effectively boiler plate their terms of service that often state or bury what they are going to do with your information. Does any company stand out to you or do any corporations stand out to you that are particularly bad in terms of companies informing users about what type of information they are gathering and how they may be using it?

Scott McCollough: I have both drafted and analyzed the privacy policies of countless companies. When I am drafting them, it is an exercise in taking away your privacy, it is an exercise in having you waive all expectations of privacy, all rights to its, giving the property rights to me and allowing me to use it for anything I want. It is much like HIPPA that you all do when you go to the doctor.

In the name of protecting your medical privacy, you're supposed to file this form and you think, oh great, my privacy is protected. Instead, it is an exercise in wavering. Who has good policies? Since Ron over here is my favorite clients I won't tell he's privacy policies, I would commend them to you.

They basically say your information is yours, we don't want it, we don't want to fool with it, we think you ought to encrypt it and keep the key and the only time we are going to turn it over is when the government gives us a warrant. They say it's clearly and so simply and without qualifications.

I challenge you to find any other company, and in particular internet access providers, and in particular, even my friends over at Google, to be so clear about what it is in terms of protecting privacy. There are reasons people do not read these privacy policies. They are obtuse, they are impenetrable, and only a lawyer can understand them, and that takes effort and we don't do anything unless we're billed.

Ron Yokubaitis: Let me defend myself. Listen, I could talk to some of the enlightened ones in this room and I really feel like I'm talking to a pretty hard head because they're very combative but assume, assume, assume; and you just can't assume. Assume the worst to protect yourself. Just because somebody say's they don't log, they are logging, especially in the cloud setting. You are renting servers but you don't control the logging on cloud based server or the network flow stats on upload drivers, somebody else does. It's not to say that you don't log in because the login, you just quickly go to the hosting provider, you get whatever you want to get off the hosting provider who will divulge you. We can let Rackspace talk about how corrupt their policies are. There is severe problems, unless you are heavy around the servers, know router switches and even your DNS. Okay, a Google DNS, "Hi I'm from Google and I'm here to help you for free" . You know Google DNS has got all that critical data to be able to seek for an IP address that you or your customer, anybody uses.

You need to start looking at the big hole in your privacy that is open DNS and Google DNS. There is no free lunch as you all know, you should know. We didn't grow up with a free lunch box, there is no free lunch on the end of that. When you find a free lunch, you're the lunch of course. You're just going to need to take … First you are going to have to believe there is a problem other than what Snowden says. The thing I am reading, well my son is reading me, Greenwald's book. I'm about a third of the way through it and fall asleep but no, it's a good book.

But like he said, you can't hide. You can run, you can encrypt, you can go from here to there, you can run your proxies around the world but still, you can't hide. You're basically turning to … It's still security through obscurity, that you need to obscure yourself.

Brian Hauss: I think Ron is exactly right. I think you should be suspicious of any service provider that gives you something for free. Dry speak on the Internet and nobody does anything for free; Drop Box are a classic example of a company that provides what seems like free storage but actually it just has access to tremendous amounts of your personal data that you just load up there for them to look at whenever they want.

I'm really gratified to see that now we're finally seeing some companies like Golden Frog and previous Lava Bit before it shut down, come forward and offer these paid services. What we're seeing is actually consumers really want to pay to protect their privacy. They are willing to pay to protect … it's something they value and hopefully going forward there will be more options for people who really want to protect their information. The danger still is that companies that want to help protect your information aren't always able to do it. I think Lava Bit is a perfect example here.

Lava Bit was a security known service provider crated by Ladar Levison I think right here in Texas. It encrypted all your … Gave you the key. The idea was that Lava Bit itself could not read any of your email. Its profit model was based solely on your pay subscription to the email service. The government decided it was very interested in somebody who was using Lava's servers. There is speculation … No one has ever confirmed it but there is speculation that it was Edward Snowden and they want to do an investigation. They went to Lava Bit and they said okay, we want to install a PIN register device, a surveillance device on your servers so we can collect all the information that people are using as they are interacting with your service. From that, we're going to figure out what the private key, what their private keys are and then we're going to decode all the information; or all information of the person we are looking for. Lava Bit said to the governments, "I can't give you my private keys, those protect everybody. I've got one set of private SSL encryption keys that secure the email traffic for everybody who is interacting with me so they know it's me they are interacting with, not some other company, not the government." The government said, "Too bad. We promise we will I be look at the person we are looking for, we promise we won't look at anybody else." It's not like they were going to sign a contract saying that, they were just telling them this. He said, "I'm not going to do that. You can't force me to blow up my business just to give you this one person's information. If you want this one person's information, come with a court order for that person and I will give you that information myself. I will create code in the program to download that specific information to give it to you without compromising the rest of my users security." The government said, "Too bad, we don't want that. That is not the kind of process we want to do, we want to run it ourselves. We want to install the device and we want access to everything and then we want to take out the person. We don't want to have to rely on you." And Ladar did very well and said, "I am not going to do this to my users, I made a promise to them, I advertise it this way, people trusted me," and he was trying to do his business. The government still moved for sanctions against him. I think it was on the order of about $5000 a day or something like that. He appealed it up to the Fourth Circuit—the ACLU files these briefs to have - but ultimately the Fourth Circuit said, "Oh well you know, you waived all your arguments," because he was representing himself before the District Court. He wasn't able to hire a lawyer in time. The government was just railroading this through the district court process.

He didn't know what he was doing, he's not a lawyer. He didn't know when two object, what to say, and how to say it. The Fourth Circuit's, they go, "Too bad, you have waived your arguments; there is nothing for us to do here." [inaudible 00:29:05] That company was shattered and you know with regard to the finding it was held in place. In the wake of that, you saw a number of security email search providers said wait a minute, the government can get these keys, our users information is not secure either and they all shut it.

So one the things we are going to do if we want to see companies actually take this really take this really proactive stance and we want to encourage this, we have to make sure that there are reasonable limits on what the government can do as far as its

investigations; even when it has a court order.

That order should be specifically limited—the fourth amendment was all about fighting general warrants, the idea that the British could just come into your house and look for whatever they wanted. The idea was that they would be specifically limited to the specific thing they need and I think we need to make sure that those limits are put back in place.

Scott McCollough: Meanwhile, find a service provider that lets you have your own key and where the service provider does not retain that key.

Justin Freeman: Scott, do you have anything else to add?

Scott Henson: Especially for this crowd, one of the things that even Scott mentioned, if someone comes with a general warrants signed by a judge that they can go ahead and give the information. If it's encrypted, that's one more hoop they have to jump through. It's not impossible for them to eventually … to get to that. For folks who are developers, for folks who are producing products that may use location data or have that as part of what your service is, keep in mind that there is one kind of data that they [the government] cannot access and that is data that you have not stored. If you don't actually store non-essential meta data over time, then it is not there for them to get. That just sort of solves the problem on that end. Now that everybody sees Snowden and then the aftermath, that becomesmore reasonable saying that two years ago in December…

I'm telling you right now, especially because I learn more on government type issues, government type databases, making sure that that data doesn't just sit there forever so there is no chance of getting it years from now. It matters and data retention is going to be a bigger and bigger issue. I also have a lot of … While I agree with most of what you said, I would also say that was more of a textbook example of how not to handle a legal situation. Law enforcements comes down and knocking on your door and there are a lot of writings on the sort legal setting actually of how all of that went down, a lot of hotshot defense lawyers think that if instead of trying to do this per say, "This poor guy …" I say poor guy … You make the decision to represent yourself against an attorney, I thought that was silly. There is a Darwin's law scenario there, that is just going to happen. If he had actually understood his situation and immediately lawyered up and immediately went out and saw somebody, who really knew what they were doing to fight it, I think they wouldn't have set some these really bad precedents.

There is a blog for a lawyer called civil justice who has written a lot about this and leads to all sorts of pros and cons, debates about how to handle this… so read his blog… Gosh "how did you let that happen" … [inaudible 00:33:33] $5000 just to [inaudible 00:33:35]. That would keep the data; call the lawyer, when they show up and don' try to do something on your own.

Justin Freeman: I think Scott and I could both … You can't argue rather with your advice that you should always find and pay a lawyer when you have the opportunity. I'm going to pause here for a moment for some questions. I know that we are diving almost head first and under the surface of all this discussion … It is comments about law enforcement and legal reform from government access. I would like to pause though for questions about commercial and consumer privacy if you could limit those for the moment.

Male: I have one question, have we ever considered the idea of doing some kind of open standard with these agreements? If user things or license things had common frame work across the industry, just like any of the other standards be for whatever protocols, maybe that would make it easier for people to understand what the actual agreement is.

Justin Freeman: For those of you that couldn't hear, the question is relating to whether we can have a common platform or sort of an open source standard for privacy and user information and disclosure.

Scott McCollough: I would certainly commend it, there are several models for that in the intellectual property world and I'd

be happy to work on a project such as that. I've never heard of one being tried. I think the industry would be well served best for the consumers if there was a specific template for privacy enhancing, set of privacy terms that people could understand and rely on.

Male: Especially if that included a scoring component.

Scott McCollough: Yes.

Justin Freeman: Anyone else?

Scott Henson: Above my pay grade.

Male: Who actually installs all the equipment or software that's out monitoring us? Is it the FBI or NSA? Who can we talk to about making them stop?

Scott McCollough: I generally make my business, make my living representing businesses. Sadly I'm quite often pointing a finger at those very entities. The folks who have installed this surveillance mechanism for our country are the same ones who sold the information to the Iranians and the Chinese for the Great Wall of China. They're very prominent companies, one of them begins with C and ends in O, they have equipment in virtually every company that is in this space. You all might be shocked to see what's running on their motherboard and in their firmware.

Ron Yokubaitis: Also a provider like us gets a FISA court warrant which we now say we have. A few months ago you could never be divulged that you got it. But those will be located piece often below say piece equipment of port sailing a hoster. Their center operator gets the thing; the hoster may or may not know. We insist that the hoster knows and not be in treated like a suspect so they don't do like they did to kem.com or the fact that Steve Jackson Gains here, in the secret service back in 1991.

The case starting, the EFF started here with Steve Jackson Games, online games, illuminati online, then it became the ispio.com, but they just took all the servers and now all the innocent people and even the suspects was innocent but they didn't just hit on his stuff, they got everybody else at kem.com. They whirlwind in it, anybody that was storing a hard above the alleged cabal copyright purchase, they got their stuff stored. It's pretty clumsy, they had the same thing. They wanted to come in, take it off, take the whole server out and still to this day … You got to resist, resist, make them specify the person or property that's being seized and searched and it's just still … They just want to blunder and you got to resist, call council on the back door. This is all [inaudible 00:38:18] sources and benefits and not [inaudible 00:38:21].

This is an FBI agent shows up, get out a brief case with a zipper on it, a lock and its top secret hush hush, you can't tell anyone in the company you got one. Because I'm the guy that can serve that stuff. I can't tell anybody in my own company! I just … that's how it happens, that's the operation of it and until the owner is satisfied to keep saying no but you have to, you have to say no until they get their stuff together. They're going to try and wonder blunder bust you and you've got to make them constitutionally which the Tea Party is saying. We already got a law, they just won't follow it.

I got a question for Scott, as the chief of this project, the ACLU, when it comes down to ya'll—you've got somebody wrongfully in prison in Williamson County. Have ya'll looked into the fact that the federal judges are paid by the very company they're … outfit that they're out to sanction, the federal government. I mean the judges, they're asked to bite the hand that feeds them. For me, I don't think that's very constitutional, I think the federal judges ought to have … It can't be that damn much money, probably the [inaudible 00:39:53] federal forces … we can put up the money to wear the [inaudible crosstalk 00:39:57] but they don't owe fealty to the federal government, state government, they are truly an independent judiciary. I didn't think we have one so we get

the Fourth Circuit shoving it down in.. all the really crony decisions I see out of the law enforces, especially the official FISA court.

Justin Freeman: Sorry for stopping you for a second to respond, I have one more question then we're going to move on to something else.

Scott Henson: At first I should mention that the Innocence Project of Texas is one of my two main clients but the reason I'm up here was my involvement in the Texas Electronic Privacy Coalition. Hence it's project doesn't work on these issues per say but it's very, very easy to get … once you get caught up in a criminal investigation, even if it's by accident, it could take a life time to get extricated.

The worst of these guys get thirty three years plus in prison for [inaudible 00:41:01]. The consequence of errors in some of this stuff is huge. This is sort of untested forensics, never really no error ways. You're tracking from cell tower to cell tower but you don't necessary know which four towers connect, which one you're really closest to. And so anyway I thought all that say that is all I can say.. well that actually is all I have to say.

Justin Freeman: One last question for the patient gentleman in the back with the sore arm.

Male: Yeah so, several services have cropped up. They offer something called client site encryption. That's where you encrypt it before you send it to the server so nobody at the server; even if they have a court order, have nothing to turn over except the encrypted information.

Do you see that as becoming the norm in operate services and how do services that depend on actually analyzing aggregate data, build your business around that kind of standard or stat?

Brian Hauss: I think the most likely thing we are going to see is that there is going to be a range of options. I don't think the big aggregating service; I don't think Google's going anywhere. I think that the services offer client side encryption with hopefully become much more popular as people start to value that stuff.

They will likely need to make their money partly by charging their clients and so some people will say, "You know what I don't care, whatever, just put it on Google, I'm fine, really, just send me the ads." Obviously with them you would argue that it's not as innocuous as it sounds but I think that there will probably be a range of options and people will have to choose how much they value their privacy at the end of the day.

Ron Yokubaitis: I would just like to say of course you can do crypt your own content. PGB's been around twenty plus years and … but one thing you might want to consider is what you can do with, for a law professor now terms a Geo-location evasion, or as we do for VyprVPN for Golden Frog. We take your surveiled IP address from AT&T, Time Warner, whatever. And put it on a shelf and encrypt you to another location or another country and lets you be assigned an IP address from that country; so that all the data is all about some person in Amsterdam.

We take your surveiled IP address from AT&T, Time Warner, whatever. And just kind of put it on a shelf and then encrypt you to another location or another country and let you be assigned an IP address that's your located to that county. Such that the data is all about somebody in Amsterdam or Russian so that you can let them have an encrypted VPN to some place that is not identified with your locality via your ISP so there's ….

You still running, but in the end you can't hide and you not going to … I don't think you prepared for them. You're going to realize that there are some things you do, some applications you use that you're going to want to encrypt and some other stuff you

going to say, "Ah what the hell, it's the price of Google."

The point is that it's your choice that then… if you don't, it takes folks to get active. Some guy, or someone else is going to do it, you going to do it, you need to click on the EFF letter to whoever you're compromised congress critter is. No matter what either party, it doesn't really matter.

There's a few that are more guilty than others because they got more awareness in the Internet, but Ya'll have to do something, its personal, personally to encrypt, personally to protect and [inaudible 00:45:25] publicly via letter, email - put in the pressure because they're only going to respond to awareness and pressure.

Scott McCollough: In some respects the law generally tracks the technology here. There is a distension between the so called federal information which when we in practice call meta data, and the actual payload which we call the content. It is difficult in many respects to have any real protection of the meta data unless you are using a VPN service which can only protect some of it even in any event.

It is far more possible for you to take action to protect the actual content, the substance of the information that you are conveying because you have the right to avail yourself of some of the encryption options that are available, but even then it's limited. There are now offerings on the market .. Ron over here has one, it's called Dump Truck where you can encrypt your information and upload it to the cloud and it is stored in an encrypted fashion where you still keep the key.

If Ron gets a warrant, what he hands over is gibberish. If you are talking between two edge points, two edge devices who are going through each other on the network; it is still to this day somewhat difficult to have good encryption of the content on an end to end basis.

The two edge points have to have a way to negotiate the exchange of the key. You guys are the technologists in the room, if you can come up with a way to better facilitate the exchange of the key between two edged devices and make it ubiquitous, I think you got yourself a business. It's out there now but it's still very difficult for a common ordinary citizen to make themselves available to it.

Justin Freeman: We're going to go now to law enforcement which I think will be with the largest area of questions. I know I saw a whole lot of hands going up the last break, don't worry we're going to reserve a lot of time at the end of this.

I'd like to put to the panel, the USA freedom act is currently winding its way, its wound its way through the house and its now in the center. Of all your concerns about the last minute changes or course to run that bill, I'd just like to get your sense of whether an NSA reform or just generally US government's surveillance reform is possible and what your criteria would be to consider that reform effort is successful. We'll start at the far end with Scott.

Scott Henson: Sure. It would be just a suckers bet for anybody to bet on any particular piece of legislation to pass in congress any time soon. Maybe it will happen, maybe it won't, maybe it becomes a bit of the World Series …

There are lots of big maybes, but I would not count on that at all. I've been very hardened to see after Texas; which by the way we were just a tad ahead of our time. The Texas bills on cell phone location data and email require warrants for both … were filed a few months before, written and filed a few months before the Snowden revelation. To date, only two months earlier, they both were passed. One did, one didn't but they both would have easily started,just happened a little bit earlier. Then for us it was a bit of a slog trying to educate people about things they didn't understand. Now everyone has heard of it, even average folks know what you're talking about and I think that makes it easier that you don't have to just drag people who are not

technologically savvy, into understanding why they should care about this.

Maybe something will pass at federal level. If it does—go team, if it doesn't … Tennessee within the past week, the governor signed their state level legislation, saying state local cops can't get cell phone location data without …

Ron Yokubaitis: Where is this?

Scott Henson: Tennessee. We've had Montana, Maine … two others, Utah and one other area that I'm forgetting. Who've done a full legislation. Then New Jersey and Massachusetts have done it at their state's Supreme Court level. That's just in the past two years. Texas have already passed what would have been the first in the country. We were the first in the country on email, to extend that warrant requirement to content in the cloud. There's a national push for this … Virginia is the other. A lot of these are in probably red states and so this is …

I think we've got a great chance. I think that for this to happen with the state's first, then the Feds who are still running around kicking and screaming; is more how I see this happening in the end. I guess I haven't seen it pass anything so… maybe they will or won't.

Justin Freeman: Brian?

Brian Hauss: I think with the ACLU you have to believe that NSA reform or intelligence reform it is a possible reason to spend so many time, so many resources fighting for it. I think the really important thing to remember here is just to look at what's happened in the year, the year since Edward Snowden came forward. It's almost exactly a year anniversary this month.

Over a year, just a little over a year ago we had a fight in the Supreme Court … Clapper v. Amnesty. Where we challenged the government; we believed the governments meta data surveillance program was … we got kicked out of standing on judicial ground saying, "If you can't show an injury then we're going to throw you out of court." Basically what the court said is you can't even show what the government's doing this. We have no idea if they are doing this or not. You can't prove that any of your clients or you have ever been surveiled in any way or form so there's no case here, we're throwing you out. And then a month later, or two months later, we sitting in court and not only were our clients surveyed, we were surveyed, everybody was surveyed.

What you showed us was that the fifth [circuit court], the court that the government has set up to regulate intelligent surveillance, had been interpreting the relevant statutes in such a way that it clearly eviscerated that meaning. What the statute said was that the government could collect relevant data. The Fifth [circuit court] had interpreted relevant in anyway even marginally useful to the government. So if it's useful for the government to have that haystack so it can find its needle, fine, give them the haystack. That's just not a reading that anybody reasonably … any number of the public who didn't know what the NSA was doing reasonably thought they were going to do.

Of course the senators on the committee knew it, but they were misled because they were afraid they'd get prosecuted for giving classified information. They asked, Senator Wyden asked General Clappert at the correctional hearing … Are you collecting Americans meta data, are you collecting Americans data, and he said, "No, not really." He basically lied to congress. This was an entire bill of secrecy on this program and you couldn't have the debate because the government was not willing to admit the very things it was doing. Now it's out in the open, we know what the government is doing and I think that the public opinion has changed really quickly. The fact that we're having this discussion at all about the USA freedom act just goes to show, what a difference the Snowden revelations made in this very short space of time. So we're hopeful as time goes on, people really dig in and learn about this stuff and fights are waged that yes I think some surveillance reform is possible. I think if maybe we'll have

another moment like he did with [inaudible 00:53:55] hearing and that we will actually succeed in changing this abc culture. Would I bet on it in the short term? Maybe not. Hopefully in the long-term, change can happen.

Justin Freeman: Ron?

Ron Yokubaitis: I'm just not optimistic that we are going to get any reform in the surveillance and intelligence gathering in the United States [inaudible 00:54:16]. Just sorry, it's got to go through Congress, it's got to be passed on, if you object to it by court, paid by the very U.S. Congress and federal … I think it is up to us, each individual, that's it. I've said for several years that encryption and VPNs are the Second Amendment for the Internet. A lot of people would disagree. The Second Amendment are [inaudible 00:54:47].

I think that folks at Fight for the Future, the political action group that focused on getting the emails on SOPA are a pretty outstanding group of young people. I've been on a panel with one of them South by Southwest. To a man in Massachusetts to be against us gun toten Texans, he knows we are not [inaudible 00:55:13] car jackings in Texas. Because they don't know which one of our wenches have got [inaudible 00:55:17] are you talking about this car?

You've got Massachusetts but nevertheless, they are using that image of the Second Amendment. What is that, that is us, each one of us not counting on government surveillance. I am just [inaudible 00:55:36], we lobby in good faith, both parties. We are bipartisan - slanders and words but still I don't put my family's security in their hands of the government. I am not optimistic about …

I'm trying at a state level, we are working on the ECPA going back to several congresses but we see both parties are entrenched enough that they really don't like it. Only now, only now with this and right now I think we're at 214 signatories sponsored. How many are we at? 216, we need 218. I'm telling you what you could run out of here today and call your influenceable congress critter, whatever party they are.

We need some more Democrats, Lloyd Doggett here, Lloyd he gets it fast. He is one of the Democratic congressman here … The Democratic does the stronghold here in Austin. We don't hold that against him when he snaps. He understands and is willing to listen very quickly on Internet security issues. We very much appreciative … It comes out, he would say it. We have just got to get to him and talk to him.

If you all talk to him, run into somebody somewhere, rather than talk sports or whatever, just say, "Hey what are you doing to protect the privacy of us from national surveillance? Are you protecting your own staff? What about you and your family?" [inaudible 00:57:26] not a congressman, Critter is what we say, it's not Texas talk. I have lots of stuff, like, keep your mitts off my bits. We are just trying to get the ideas going but it's up to you all individually. It's not like somebody's going to take care of your brother, you're going to take care of yourselves and you best take care of your online self and just take simple measures.

For that stuff … I know we do lots of stuff that we don't really care about. I don't care if Google knows what bra I am looking for but there is a lot of stuff that you just need to protect the person at the other end from your loose lips. It's going to sink somebody else's ship. I'm not at all optimistic about our favorite surveillance state.

Scott McCollough: It's a rare government that chooses on its own to limit its own powers and to restrict its activities. It is a common government that thinks it needs more information so that it can then efficiently take care of its subjects. The only way that there is going to be any reform with regards to surveillance is if the people rise up and demand it.

Ron Yokubaitis: That's including geeks.

Scott McCollough: Meanwhile you need to take care of your own privacy through self action. Let me make sure that the audience year understands what the legislation is that's going on in Congress right now because they've kind of been mixed up a little bit. With regards to the NSA reform, the Snowden revelation stuff; there was a bill in Congress called the USA Freedom Act that was originally introduced and largely was a good bill.

We worked with many of the progressive groups and you guys did an extraordinary job on it. We thought we had it coming out of the house but once it was voted out at committee, the powers that be in the dark of the night got together and gutted the bill. One of the people that did that by the way was unelected just a few days ago by his district in Virginia. Sadly, what passed out of house really is not satisfactory in the least. There is an effort now to try and fix it in the Senate. Nothing is going to happen; it's good though so that the folks in the senate have every incentive to protect their underling over there in the executive branch because everybody that's in the Senate … One of these days they are going to be over there running the executive branch. You need to be ringing their phones off and talking to them about an NSA reform bill that actually reforms the NSA.

Second and apart from the so-called Snowden's revelations is the amendments to the electronic communications privacy act. That is the stuff that Scott and I were talking about requiring a warrant for content. The Texas version of the ECPA was what we passed last year. In the federal Congress, we've been trying to get that taken care of for many years. There was a Senate bill that came out of committee, largely a good one from Senator Lackey. It has been hung up not because the NSA wants to look at your stuff, but because the securities and exchange commission, the federal communications commission, the Federal Trade Commission, and all these other administration agencies want to be able to get your content without a warrant by sending a subpoena or something less than a warrant to the service provider. That bill will not come out of the Senate unless somehow or another, the so-called SEC . Don't think it's just the NSA that want your stuff, it's all these regulators with all these letters and after their names, it's not FBI. They want your stuff too and the problem is once an administrative civil agency gets it, then they can turn it over to the FBI without a warrant. It's the same as when a corporation gets your stuff, the government can get it. If one agency gets it, they can freely give it to another government agency. You need to be aware of what this information is, how it's collected, what's it used for, and what happens to it afterwards. On the house side, there is the yoder bill and that's the one where we now have a fairly large number of sponsors. We are three short of the mark.

Ron Yokubaitis: Y-O-D-E-R?

Scott McCollough: Yes, Y-O-D-E-R. If we can get a couple more Democrats to sign on as cosponsors, we will get what's called a supermajority. It can be voted out of the house without having to go through a committee. That is a good bill, that is clean bill. It requires warrant for content. It does not have the so-called SEC carve out.

Ron Yokubaitis: We are not going to let the bureaucrats also protect their power because the bureaucrats want to protect their power. Those are regulatory bureaucrats that he calls administrators, they are regulators. Some people think regulation is the answer. Big companies just hire more lawyers, small companies can't handle it but they do want to give up power - period.

Scott McCollough: I became a lawyer when I got out of the Marine Corps because I figured I needed to know my enemy. Once I got my bar card, I started to do administrative law because I found an even bigger enemy. These administrative agencies are almost as dangerous as the NSA and the FBI. They can ruin your life just as easily.

Scott Henson: After the hearing last year about the cell phone location data bill, the one that said they couldn't look at your historical data, there was this long three-hour hearing in the house … Law enforcement Texas House. Yeah, Texas house, law enforcement said over and over, "Oh well, we don't get this from a subpoena, we always get a warrant or we get these higher standards and reasonable suspicion, whatever."

At the very, very last testimony of the hearing, this poor gal from the department of insurance had no idea what she was stepping into. He walked up and said, "I just wanted you all to know that we access this data all the time in nearly every one of our investigations. We just issue a subpoena, we don't issue a warrant or anything. Just a subpoena, they always send them back—been very promptly. That is the standard here." It's very weird.

Scott McCollough: These were fraud investigations by the way, it just happened to be civil.

Scott Henson: Yeah, yeah, that's why say about the regulatory agencies. It was just very strange because while Texas law seems to… by the way Texas law on this… I've been involved with legislatures since the late 90s, it's the worst written statute I have ever personally been involved with. Five lawyers write seven different pages about what that statute means.

They debate over this…. but nobody really knows what the standard is. It could be a subpoena, there's one reading where you could say it should be a subpoena under Texas state law. There is a reference to EPCA so it could be a standard of EPCA. There is another section that's a very convoluted bit of code that references reasonable suspicion, it could be that.

Some people, some law enforcement agencies says they did not understand themselves of what was required. Were already getting warrants anyway just to have clean papers just because they were confused and didn't really understand.. and just said look, we have a warrant. That is one of the most confusing worst written laws ever. It's because technology has evolved so much more quickly than the statutes.

Scott McCollough: We've got a pretty good start of fixing it here in Texas but now we need to move on to other states and to the federal government.

Brian Hauss: If I can just jump in and talk about one more agency that does this, the DEA. We just had a big case out of Oregon. Oregon passed a law saying, "Listen it's part of our plan to help coordinate medical care in the states. We're going to have this thing where we collect the prescription drug records and put them in a database. We promise you as the state of Oregon that your records will not be disclosed to any law enforcement agency in Oregon without a warrant."

When the legislators propose that law, they built in more protection for the citizens. That was a conditional law being passed. Then the law gets passed and the DA comes in and says "Hey, you've got these prescription drug records, we are interested in seeing if some of these doctors are prescribing things off label or whatever. We're just going to give you a subpoena and we want you to give us all those records." Oregon says, "Well you can't do that." They said, "Well there is a third-party doctrine. Comes right back. These people voluntarily gave this prescription information over to the state. Once they did that, they lost all privacy interest in that information. We don't need a warrant, we're going to give you a subpoena."

We litigate this case in Oregon, we said the governance plan violates the 4th amendment, the District Court agreed with us. We won a big constitutional ruling out there [inaudible 01:07:32] were doing the same thing now I believe in Utah. The government is going to set to appeal itself… [inaudible 01:07:37]. The DA is just one more example of this where … It's not even investigating the patients, it's investigating the Doctor but as a result of them investigating the doctors, all your private prescription information, whether you taking antidepressants, whether you take Viagra, whether you take …

Any kinds of mental health drug or physical drug, your cancer medication, whatever, it will all be available to the government on subpoena on its theory because of the third-party doctrine.

Justin Freeman: Ron would you like to follow through? We are going to save about 20 minutes of questions.

Ron Yokubaitis: Questions is best. I am just going to say this, it's going to pull together what Scott said earlier. The problem you have when you go to the doctor is that you filled all that privacy notice papers.

The first time I was presented with that stuff, several years ago when it first came out to protect our privacy, I sat there in the doctor's room and read every bit of it and started to scratch it off. When I got to the end, I realized what Scott said earlier, that all that document does is ensure that you have wavered any elements of your privacy regarding your medical records. The next time just circled the part that say's he can charge your health insurance on it and scratch all the rest out or don't sign it at all.

Those little ladies out there will tell you it's required and all that SBS. It's a CYA for a doctors ... When he does turn it all over. Just like AT&T, you gave your consent. Believe it or not, just because someone's puts a form and says privacy. Just sign [inaudible 01:09:22]. Read it and then you may not want to sign but it's just [inaudible 01:09:30]. That's how you give it up at the store, at the doctor, everywhere, or online.

Justin Freeman: All right, we've got 20 minutes for questions and we'll start on the left side of the room. Please make your voice pretty loud, otherwise I'll try my best to summarize it.

Male: Yeah, we do have a microphone.

Justin Freeman: You have a microphone?

Male: I do.

Justin Freeman: Beautiful.

Male: Ron earlier mentioned that that the VPN is the second amendment of the Internet age. The second amendment is codified in law is a fundamental problem with avoiding surveillance and maintaining privacy, that the right of privacy that is, who owns the data is not codified in law?

Scott McCollough: I would contend that it is. I would contend that it is contained in the First Amendment, and the Fifth Amendment, the 14th amendment's along with the fourth amendment. I speak because the law is better developed with regard to the fourth amendment and I know Scott is far more of an expert on this then I am. The fourth amendment has been interpreted to include a privacy component. In fact many of the cases that are dealt with that developed the third-party doctrine was based originally on the property notion of trespass to people's property and their houses.

In about the 40s or 50s, the Supreme Court's went from a property-based theory to also add the privacy [inaudible 01:11:12]. Under these interpretations, if someone has a subjective belief that the information is private and it is a belief that society is prepared to accept, then the information is protected. That is how for example in those old phone booths that we used to have on the corners, if you went in the phone booth and closed the door of the phone booth, you had constitutional privacy. It is in the law, it is in the Constitution in addition there are various statutes for its.

The electronic communications privacy act, this outdated act, for example, was originally passed by Congress with the intention of providing more statutory protection than the Supreme Court had allowed for things like PIN registers and traffic trace devices. The Supreme Court then said that law enforcement did not need any kind of authorization in order to obtain your [inaudible 01:12:19] phone numbers or the numbers of the people that called you, that's a traffic trace or a PIN register.

Congress disagreed and said no, we want to propose an intermediate measure of privacy here. You're going to require a warrant

but they did require a very different lower-level of showing but more than what the Supreme Court had granted. This is an area where both legislators can speak and of course we had the judicial backstop. But let me return to one little thing here that I think is extraordinarily important and that is this notion of privacy and the judicial test for it. You have to have your own personal subjective belief and it needs to be one that society believes is reasonable. Society is changing now in what it believes privacy is about and what is reasonable. You need to protect your own subjective expectations of privacy and then you need to work collectively with the rest of your citizens to talk to Congress and to educate yourselves so that we can evolve as a society, so that the courts will then be able to better determine whether this is an expectation which is reasonable.

Male: Aren't you just basically agreeing with my point that there have been interpretations but there isn't anything that specifically says that the creator of the data owns the data, not the party that collects the data?

Ron Yokubaitis: I would like to say something in particular to that. You all know Google Fiber is coming to Austin. Immediately that day they announced, AT&Ts said "me too we are going to give you guys a break". Now they are opening up their Pomona and what their pricing will be. You get a gigabit to your home, the pricing I heard is 99 bucks a month. That is what I understand but if you agree to let them survey your data and keep it, it's $20 less a month.

They realize just like … This is AT&T isn't, the same thing we found with the FTC to [inaudible 01:14:47]. Those folks are rightfully nuts [inaudible 01:14:52] in progressive circles. What you've got is the value of it and I would almost like Scott to talk about your information is privacy … Its property, it's yours. Therefore it is an unconstitutional taking by the government to surveil you under the Fifth Amendment. They are taking your property without due process of law, without your permission.

You've got to act like it's your property, rather than … well that's a third-party, you've got to act like you trying to keep your property, like it's your … saying, "Hey, I've got friends around keep my… [inaudible 01:15:37]." It's like that forever. You take care of your business.

Scott McCollough: Are the definitive rules, no, but what we're trying to communicate to you is that you are an important part of forming those rules and the only way that those rules will be established to your satisfaction is if you are active and seeing to it, as your political representative and the courts do it the way you want because they do not have an incentive to do anything other than to take your rights and liberties and property away.

Justin Freeman: Moving on to the gentleman with the trench coat.

Male: Considering that I was a former submariner, I know a fair bit about intelligence and spying. I was trained by the government to do it. Considering that during the Cold War, this is before … Back during the era of dark men, the earliest versions of the Internet. One of the things that the Russians did was they paid off the people emptying the trash and they were able to figure out what top-secret projects the government was working on by things just as stupid as the metadata of what phone numbers you are calling and for how long.

Considering the fact that most recently the NSA and CIA, some of their higher ups have admitted that metadata has been used in determinations of who they are going to kill and assassinate, could a legal argument be made, that meta data is maybe actually far more important than just property. It's a determination of life and everything worthwhile.

Brian Hauss: Well I think certainly meta data goes to your free expression rights. But the metadata you give of when you speak at stuff like that and that enables the governments to target people, identify who it wants to surveil further. That's partly a function of your expression, rights?

When you speak, how you choose to speak, what time do you speak, those are all connected in some way to your expression. Now it's not legally protected that way but when the government targets people on a basis of metadata, it implicates both the Fourth Amendment because as you said, it directly implicates the privacy interests. It also negates the First Amendment because it's tied to the way the way they are expressing themselves.

It will come about more specifically when it comes to metadata related, say your Twitter account. If the government wants to subpoena Twitter and get your IP address information from Twitter because it wants to figure out where you were when you posted that anti-government message to see if you are part of a particular rally or something like that. That definitely implicates your First Amendment expression in addition to your privacy interests. As opposed to let's say, the government wants to know where you were when you were driving on the freeway at 3 o'clock in the morning, that is not directly tied to your expression interests.

It's more [inaudible 01:18:31] privacy interests. I think both the First Amendment and the fourth amendment are implicated when the government looks at your metadata, specifically when it looks at your metadata on social media.

Justin Freeman: You are up.

Ron Yokubaitis: In response to your [inaudible 01:18:42] desiccated property to the extent that this is more important than property. You write a song, it's your expression—the lyrics, this and that, this and that. The bottom line is that it's your property. We have a pretty elaborate system of constitutional law and developed law which protects your property from people taking it from you without your permission.

We're [inaudible 01:19:10] see all the cyber stuff, we're all involved in—and the fast rate of that.. It's hard to explain some of the changes that people in this room that are all actualized. We all are still working it out but when you see... [inaudible 01:19:28] AT&T will give you a 20 buck a month discount, then you give them your property, you sell them your property. They understand it, you need to understand it and start acting like [inaudible 01:19:43].

Would you pay 99 or would you take the deal for 20 bucks less? Now Scott says Ron doesn't take the 20 bucks less, let them surveillance it, just use the VPN and encrypt it and take the money and give them the [inaudible 01:20:03]. You have got to start acting like you want somebody. What I do is important to start acting like it like the free North American SOB and get away with it.

Justin Freeman: I think we're got one last question here. You [inaudible 01:20:22]. Since you have to run it around I think it's fair if you get to choose as well.

Male: I appreciate that. I just had a basic question back on what the gentlemen spoke ... You all said it so eloquently that this is your property, they don't have a right to take it from you and look to it. I'm curious to know, recently the Supreme Court was backing police to seize your cell phone and look through it, is that real? Do they have the right to do that?

Scott McCollough: We're still waiting on that decision.

Male: I use my phone for work and I've got company information and I try really hard to get rid of it, keep it clean so that when I do lose my phone...

Scott McCollough: One way to slow them down at least is to at least require a keypad entry to encrypt the information that's on it.

Male: Then right now as I drive home right now, I get pulled over and the guy says give me your phone, I want to look to it. And my...

Scott McCollough: I can say they can't do that, there are others on law enforcement who say they can and the Supreme Court should be deciding that in a couple of weeks.

Brian Hauss: What the government is relying on there is called the search incident to arrest exception to the warrant requirement which is the idea that when they arrest you, they pat you down, look for weapons, do that kind of stuff. Now they say because you could somehow away from your cell phone and delete everything and erase all the evidence that they might want to take from your cell phone, that they also need to be able to look at your cell phone immediately so that that way they can get that evidence before you deleted remotely.

In fact there are lots of ways government can prevent people from doing that. There are special boxes that they can put in to make sure the phone can't be accessed remotely and have all the information deleted. There are a lot of the specific, what they call evident circumstances [inaudible 01:22:04] which is the idea that the evidence will magically disappear if they don't get it right away.

That is what they are using to argue that they need to be able to look at your phone right away without having time to go to a judge and ask for a warrant. Also I want to talk about a different circumstance where the government can do exactly the same thing which is at the international border.

If you're crossing the international border, the law in most Circuits, except the Ninth Circuit is at the government can just take your laptop, take your phone, do whatever it wants, look at it, keep it, hold on to it for as long as it needs to, run a forensic search on the device, look at all the files on it, do whatever it wants without any reasonable suspicion, no basis for suspecting you for anything just doesn't like the look of you.

They can take your stuff, keep it, analyze it, build a case against you, do whatever it wants without ever going to a judge or even having to justify its decision after the fact. This is what's called the border search exception. The idea is that when you go through the border, you have no expectation of privacy of anything you bring with you. This was created back at the beginning of the Republic and was really the idea that they didn't want people smuggling drugs, opium, what have you, into the country.

It was never intended to cover the vast amounts of information that you can just store on your phone or on your laptop; especially in a world we know you basically have to take those things with you in order to function as a professional who is traveling across borders. The government knows how useful this is because you've seen in cases like David House was a program in Massachusetts who was involved with Bradley Manning's support network. He was not specifically involved with Bradley Manning; he was just involved with supporting his legal defense. The government wanted to know if David House had any connection to Bradley Manning. What they did was they put an alert in the system. We want to know the next time David House leaves the country. Because they have a system that lets them know whenever somebody's got an international flight going out, they knew that David House could go to Mexico and then use it to come back to Chicago.

So what they did was they sent customs and border patrol and immigration and customs enforcement officers to Chicago and the second he landed, they pulled him off the plane, they took his devices, they analyze everything on those devices, and ultimately they completed that they didn't have any basis to suspect them in the first place because he didn't do anything wrong. In the meantime, they got a look at all the data and they got to completely invade the normal fourth amendment protections that would've prevented them from doing that in the country. They said no connection to the borders, they had no reason to believe that he was can it bring in, smuggling back into the United States. They just wanted it and they knew they couldn't get a

judge to sign off on it so they found a special loophole that they used.

The Ninth Circuit has just come out with the decision last year called the United States vs Cotterman—when the government wants to do a forensic investigation of your laptop, it needs reasonable suspicion. That means when you go to the airport in the open up your laptop, they can turn it on, they can look around the desktop but if you have any password … if your desktop is password protected. If they need to use some sort of software to actually get into the files and open them, or if you have deleted files that you've hidden away somewhere, if they want to look at that stuff, now they need reasonable suspicion. You need heightened suspicion; they need reason to believe you've broken the law related to customs enforcement. They have to justify that to a judge after the fact.

Justin Freeman: So what major airports are in the Ninth Circuit's ruling?

Brian Hauss: LAX, SFO, I don't know the code for the Portland airport but the Ninth Circuit covers basically the entire Western United States. It's a major ruling. The really important take away point from this is password protect your laptop, the entire laptop, the entire cell phone. If you password protect specific files, the court say that that can provide the government with reasonable suspicion.

Why would you want to password protect this file? That seems awfully weird. In the case at issue, they said well he's coming back from Mexico and he password protected some files so those two things together was enough, that's enough for reasonable suspicion which seems to me kind of crazy, that's watering down a standard. If you password protect your whole laptop, the court said that that can't lead to suspicion, that is just good practice.

My advice to all of you is at least when you're traveling through the Ninth Circuit's and probably when you traveling anywhere, password protect your entire device and that will hopefully give the government some delay before they can get on … Its hands on your private information.

Scott Henson: One more thing on that. I know we were talking about the federal standards and what the Supreme Court's said you can and can't do. Here in Texas, just to be clear, you asked if you got pulled over or [inaudible 01:26:14]. Unless it's a federal agent, the answer is it actually, they could take your cell phone. The Texas Court of criminal appeals but it's very recent. It got widespread play… unanimous decision… [inaudible 01:26:33] said that they can't search your phone, [inaudible 01:26:42] to your arrest. [Inaudible 01:26:46] prosecutors of the case [inaudible 01:26:50]. The court said that a cell phone is not [inaudible 01:27:04]. Texas actually does have that protection for states and local law enforcement. [inaudible 01:27:18], it's not the FBI, they have their own standards, their own rules and that's what's being litigated at the Supreme Court. Now because it is in the constitutional issue, if they rule [inaudible 01:27:36]. Texas have already actually got their own [inaudible 01:27:40] court watchers [inaudible 01:27:44] astonished but they did it.

Scott McCollough: Hallelujah.

Justin Freeman: Henry are we going to do a stop now or do we have time for some more questions?

Henry: We've got time for more questions.

Male: If I could ask Brian since he came all the way down from New York City, yesterday on your way down here, the ACLU and some other folks released their poll that 80% of America supports an update the email privacy act. Who were the other 20% that were… If you could just comment on any conclusions that ACLU has drawn from that or even you are familiar enough with that to comment.

Brian Hauss: Unfortunately … Somehow on the way down here I did not actually get to see that poll so this is actually the first I'm hearing about it but I'm very gratified to hear that 80% of Americans agree with us on this point. Again, I think it shows us two things, one that people are increasingly … As people are becoming increasingly digitally literate, as more and more Americans actually understand at least on a rudimentary level what's going on with their email, people care about this stuff.

They didn't know what was going on and once they found out, it turns out this is actually really important to a lot of people, that's very gratifying. And then I think the second point is again, I think we owe a lot of this sea change of public opinion to Edward Snowden because he's the person who came forward and actually told us about these secret courts opinions and informing us of all these things the government was doing all these things that we thought the government would never do. We said, "Oh the government would never like do data surveillance and why would they look at me, I'm just an innocent person. Why would they collect my data? They are just going after the bad guys." What Edward Snowden's revelation showed us is no, that's not the case, they are getting everybody's information. They are storing all of it.

They are building these brand-new data center out way in the desert in Utah just so they can hold on to all this information for as long as they want to; once people found that out, the office stations put forth by the federal government quickly collapsed. Now I think people realize that this is something that we really need to fix.

Scott McCollough: Before that were lying when they said they weren't gathering so-called metadata about everybody. They are still lying about whether they are getting your content; they are all getting your content. You need to protect it, you need to act to get the laws changed so that they don't do that anymore.

Justin Freeman: There was a hand in the corner over there….

Male: Right as my hand went up, Brian actually started answering some of the legal portion of my question so I'm going to focus on the practical portion of, I'm traveling out of the country, I've got my laptop, I've done a full disk encryption and some TSA agent pulls me aside and says, "Let me get into this." What can I say at that point that still leaves me with a reasonable chance of getting on the airplane as opposed to spending 24 hours in a small room underneath the spotlight?

Brian Hauss: Unfortunately it is fully within the TSA's power to make your life a living hell. It's unfortunate that they can do that. You can certainly object … You don't have to give them your password and legally they can't throw you in court, they can't throw you in jail for not giving them your password. You are fully within your rights to object. There is actually a lot of debate right now, presumably the government has internal policies regulating the TSA and CDP about how long they can hold you at the border or if it's TSA in your flying domestically, how long they can hold you before your flight … we don't know what those policies are because they won't tell us. The ACLU was trying to foyer this information, we're trying to get it, we are asking … We are demanding that they publish it but in fact the government loves to keep all this stuff under wraps because that provides less accountability, then you can't argue about it with them at the airport or in court.

Male: We can't even prove that they are holding you well over. We know the cops can hold you 24 hours without anything but if they won't publish standards, how do we know if they are keeping us longer than they're supposed to be allowed to.

Brian Hauss: Right, we don't know the statistics. An individual person held for an incredibly long period of time would know but yes, one of the problems is we don't have any statistics, accurate statistics about how long the government is holding people, who it's choosing to hold, stuff like that. In general, they can make you miss your flight. That's the unfortunate part of this.

If you believe that they are targeting you on an ideological basis, something like that, you might have a First Amendment challenge to that point. Certainly, after a certain point, it definitely pays if they hold you for a day at CSA, I think you've got a pretty good false imprisonment case at that point or unreasonable seizure. It was for a few hours, it will be a difficult case in court.

Scott McCollough: I want to follow up on something. Do you notice how he just mentioned how hard the government works to keep its secrets. Shouldn't we be working just as hard?

Male: Not as hard as they are.

Scott McCollough: This turns to another really important point about our society. Who works for whom? Do they work for you or do you work for them? At some point the people are going to have to stand up and demand that the government be responsive to their desires. There is only one way to do that and it's for you to communicate your desires to the government.

They are responsive when enough people do that. We saw that with the SOPA debate. They were fixing the past in an extraordinarily privacy invasive set of legislation, which would've allowed people to look to our emails in order to enforce intellectual property rights. They were pretending they didn't do that but once the secret got out that they were in fact about to invade your privacy in this fashion, there was an uproar.

It was by Fight for the Future folks, bless their souls. All of a sudden Congress was robbed. It was a distributed denial of service attack. They couldn't get any more emails, they couldn't get anymore factors and their phones when out of service. Do you know what happened? They were responsive. This is the sort of thing that is required.

Ron Yokubaitis: That thing was all T'd up with our Congress [inaudible 01:34:23]. The Democrat [inaudible 01:34:28] in Vermont's he was headed back to the [inaudible 01:34:31] Judiciary committee in the senate [inaudible 01:34:36] and you had both those guys with more seniority than God, and you know what, it was going through and everybody in the Congress new it.

It was a [inaudible 01:34:46] done deal [inaudible 01:34:49]. It just took all those emails and it's going to take that ... That's the vote. It's the protest, it's the block the road, it's the ... You're going to have to be Americans.

Scott McCollough: By the way, don't encrypt that email.

Male: You can encrypt it with their key.

Justin Freeman: Any final questions here? The one of the here at the back.

Male: I've heard a lot of people talk about the government and the situation that we're in and how to get out of it but one thing that I haven't heard anyone mention, I was in Representative Hughes hearing. For those who don't know, that is the one that we were talking about the cell phone data. It lasted until like four in the morning. I think it was the longest-running committee hearing ever or at least that I've ever experienced.

The one thing that I didn't hear was a lot of these people like to protect their own data but they were willing to defend the idea of defeating this bill to give up other people's data. They call them criminals, the bad guys, the suspects, they painted a lot of really good fear and that's ultimately what kind of defeated that bill. We all have to remember, most of us supported Patriot Act, most of us supported all these intrusions right after 9/11 and they called those of us who didn't support it, they called us nuts.

One of the things that I haven't heard anyone talk about yet is what are we going to do the next time we have a 9/11. Are we going to say, "Wow," that happened, let's heal, let's get over it, let's find the guy that did it. Show people what happens to him but don't give up our own freedoms, no. I guarantee you the next time everyone in this room, everyone in the city, everyone in this country, the vast majority will be saying, "Let's pass another law, let's give up some more freedoms." Those of us in tech are going to be the one to get those warrants and we're going to be the ones that have to deal with it.

Scott McCollough: Let's hope that's not the case.

Male: That's what we need to focus on, it's what we do the next time. Not just how we get out of the situation we're in.

Male: [inaudible 01:37:05].

Scott McCollough: They were those of us at the time of the USA patriot act who were warning of the extent to which those privacies were being surrendered in the name of protection. There were some.

Male: Now we suddenly have to remind them that we're in this position because we all consented as a democracy, we consented to this mess. Now we have to clean up this mess, it's our mess. We have to own that mess.

Scott McCollough: Fool me once, shame on you, fool me twice, shame on me.

Male: Amen.

Male: [inaudible 01:37:41].

Male: I just want to say something. I'm kind of with him on this. [inaudible 01:37:46] and they all said the same thing, I've got nothing to hide, I don't care, I've got nothing to hide. I can't stand as liberal security, I cannot stand to hear that because you don't know what you have to hide if you don't know what it is. Ultimately in the end you go, "Crap I did have something to hide back then." It's a mess. Everybody, especially our younger generation, when they are all thinking the same thing, that just gives away all of our freedoms and again, we are going to have … All it takes is another 9/11 and in one is going to say, "Look, this is why we need this. We need to be invaded so that we don't have those things."

That is completely wrong thinking. I don't know how but it's going to take to change the habits, the thinking habits of our society who believe that they have nothing to hide. I really don't know where to go with this but just that is something does need to be done.

Scott Henson: Everyone has something to hide in this surveillance state.

Justin Freeman: I would like to put this in a question.

Ron Yokubaitis: Let's get it on.

Justin Freeman: Why should people care about their privacy and what's the best way to defeat the canard that you don't need to worry about your privacy and why you should have something to hide.

Scott Henson: I think the first we're at a different historical moment. If something were to happen again like 9/11, I think the response, some of the things we did last time were stupid and counterproductive. And maybe just started just random wars in places we didn't have to be in... diminishing civil liberties. That didn't really work that well last time and it won't if we continue. I'm not so certain that it will just immediately trigger that. I also think that the attitude... [inaudible 01:39:48] people are always fighting the alliance war. The alliance war in this case [inaudible 01:39:56] collective set of lessons learned [inaudible 01:40:06]. I don't think ... I think [inaudible 01:40:15] Patriot Act, it just seems [inaudible 01:40:20] because it hadn't helped... [inaudible 01:40:23].

Ron Yokubaitis: In Boston...The fact that that was a real event. [Inaudible 01:40:38].

Scott Henson: That's right, it never prevented anything and in fact, the surveillance ironically, [inaudible 01:40:43] it was that crowd source sort of stuff. I'm fairly optimistic about [inaudible 01:40:58] having worked on some of this with folks [inaudible 01:41:03]. You are asking people who are going to consider [inaudible 01:41:09] because you have 30 days into given [inaudible 01:41:22]. They don't have a lot of time. Their gut instinct [inaudible 01:41:32]. I don't blame them for not having been more aggressive [inaudible 01:41:50] a lot to work with. I think it ... I'm a little [inaudible 01:42:00].

Scott McCollough: If they are not united, they get their butts kicked every time.

Scott Henson: My point is though, I think that actually [inaudible 01:42:22] there are actually ready to do [inaudible 01:42:28]. They need [inaudible 01:42:31] to step up and show them what the right thing is [inaudible 01:42:38] without making this worse because it's [inaudible 01:42:43] that state level to [inaudible 01:42:47].

Justin Freeman: Brian.

Brian Hauss: I think I'll make three quick points. The first is that you don't know whether you got nothing to hide or not. You don't know what's going to be of interest to the governments going forward. It wasn't that long ago in this country that James Hoover and the FBI [inaudible 01:43:05] the war in Vietnam, you had some the to hide. Just recently Eric Holder in the speech said that, "Yes it's important to focus on Al Qaeda and these other terrorist, Islamist terrorist groups.

We also have to focus on groups that have antigovernment bias." If you have an antigovernment bias, maybe you've got something to hide. You don't know going forward what's going to be of interest to the government. They might consider you completely innocent within the government things blow this is a red flag and then your whole life... [inaudible 01:43:30] and hopefully you come out of it without a conviction that your life will definitely be changed for having to conform to that process, you're being investigated by the FBI.

You may lose your job, you might lose your friends, who knows. Anything that we do can be misinterpreted by this fast federal bureaucracy and then you just me to hide. My second point is there is lots of stuff that people do that is not illegal but the government has no justifiable interest in getting that they might not want other people to know.

Whether you see a therapist, whether you have a mistress, if you are big drinker, whether you go to church, stuff like that. Again, not something illegal, you haven't committed any crimes, you shouldn't be thrown in jail for it but it is stuff that is private, you don't want other people to know, it's yours. I think that ties with my last point which is that having privacy is about having a little bit of space in this crazy modern world to just be yourself without having to worry about what other people think of you all what they are going to see in it or how they are going to interpret it.

If you constantly know that somebody else is watching ... Even if you know it's just loggings in a database that probably no

analyst is ever going to go searching for you. A lot of studies, psychological studies that show that on tests if they just tore little eyes on top of the test, people take the tests differently because just the feeling of someone watching you, knowing that your actions are being recorded will change how you act.

Maybe you'll be just a little less vocal because you don't want someone to misinterpreted your anti-Obama message. Maybe you'll be a little bit less sincere with your loved ones because you don't want … Just in case somebody you know, somebody NSA is looking at it and you might be embarrassed to talk about what you did last night. They might just feel a little bit less human. That's what we need to live in this world, is just a little bit of space knowing that it's just yours and the people you choose to share it with.

Justin Freeman: Ron, any thoughts?

Ron Yokubaitis: Yes, I'd like to say this. I'm going to say, for all of us to have a kind of a civil society, we do need to have police power. We need to have the police do things, do the dirty work with the sewer that runs through our community.

They do have legitimate reasons based on probable cause to get some of the data that we as service providers but you got to make sure they cross their T's and not just because he's sloppy. They will ask for a kitchen sink, you got to learn how to say no. It is okay to say no when they are got two FBI agents at your office. You can say no, no, we're just not going to do it that way. They are not going to arrest you on the spot. You might feel the threat to your freedom but you can say no but you are going to narrow it down and that's part of what you got to do … come to Linux… [inaudible 01:46:36] for just being a resident of this country but nevertheless, a lot of us, some of us have to operate a server or something online or have somebody else's stuff. You can say no but they do have… once they present proper stuff. Go out the back door and ask a criminal defense lawyer or someone that knows online stuff. Still, I won't say, stuff is going to get given up to law-enforcement, just not the broad surveillance, no cause, no particular reasons to judge. That's why we've got a search warrant.

They have to go talk to a judge, and this FISA judge is kangaroo court. We all studied in law school about the Star Chamber in England where there are secret indictments, a lot of the U.S. Constitution is a reaction to that. Here we are getting it. This to me is our court. This is a secret court and the other side doesn't get to show up and until that Clappert decision a few months ago you couldn't even say you got served a search warrant.

I think personally, I just think each of us acting as individuals right; providing that leadership with Brian Hughes and that geo-location legislation. We were all involved with that law enforcement at that time. We got to cooperate with prosecutors on the email, not resistant back when.. [inaudible 01:48:34] they want to surveil on us. They want to be able to go by the cell towers, grabbing stuff they want and just get it all, all the time. They see that, we give up [inaudible 01:48:42].

We want your cell phones, your mobile because its tracking us even when it's off and all that jazz. I encourage you to speak up. It's you, it's the individual, it's not the government. The government is the problem. When the Constitution was established and Jefferson said, "tie the government down", to change the Constitution. I would say it's not tied down right now.

Scott McCollough: Those of ya'll who are service providers, and you do get paper. It is intimidating. Ron says yes, you can say no on occasion but you don't have to get to know immediately. One of the things that you can do as a service provider is take advantage of the thing that you know. That quite often the law enforcement agent who is coming doesn't know. That is the technology.

I strongly suspect that most of the warrants or the other subpoenas that you all are receiving … Trust me I believe you; have some technical requirements in them. They require you to take specific steps. While you're trying to find the phone number for

the lawyer that your going to call and sadly have to pay for it.

Why don't you sit there and talk to that guy and say, "Wait a minute, I don't understand this. After all, I'm part of the Linux here and this is Microsoft. I don't have that kind of server. What is it you want?" Use your own knowledge to pick apart what they have given you until you can buy some time to find a lawyer. Put them on your own turf.

I do suspect if you actually look at what they show you, on many occasions, you will be able to fairly quickly see that the thing they're asking you to do, you may not be able to do, and they have to go back and rewrite it; or you may not be able to do it the way that they want you to do it or it requires certain steps.

Another thing, then he give you another lawyer tip. If you are served with a paper of this, most of the statutes involved allow you to charge the government for your reasonable time and cost of compliance. Why don't you start negotiating with them about how much you're going to get paid for it before you apply?

That will buy you a day or two. There are any number of ways … Of course I'm not suggesting that you should do this in bad favor. There are some steps to this however that are legitimate and are built into the statutes. They will try to intimidate you to skip over everything that you have rights to do and not do, and to do everything that they want you to do on their timeline and in the way that they want.

That is not even the way it works under this regime. So read the paper, make sure you understand it, ask questions and one of them is, how much are you going to pay me and when am I going to get paid?

Justin Freeman: Do we have time for another question?

Male: One more.

Justin Freeman: One final question for the gentlemen.

Male: I have one question. Who is the constituency of the NSA? Who is keeping the NSA with its power? Both section of the borders are going to know to vote for candidates that are in favor of the surveillance state. Where is the political power that keeps this thing going? I don't understand that question. I don't think there is any power there at all except bureaucrats.

Ron Yokubaitis: I agree. It's asleep, not voting, not caring thinking the other guys taking care of it or that the government is going to. That's the constituency… is apathy. It's just, the other guy [inaudible 01:53:02]. Someone else does that. That is how it happens. Yeah, it's the acquiescence in the large Defense Department bill buried in there. It's our acquiescence to this.

I would say also to you, it's not the social welfare state; it's tremendously demeaning and intrusive. "I'm from the government I'm here to help" … but what a person that's got request benefits from the government besides being a VA vet and waiting in line every year. Social welfare State just has a tremendous amount of stuff that you've got to trade them for access to government services and then they continually surveil you to make sure you staying with it or not. You're giving … We have all that bureaucracy and legislative stuff, collective and reserved in protect their ability to do so that we've actually … I would say we've been doing this stuff for about 10 years and I mean even earlier today talking to people here, that's a hard question. They are just having a hard time believing…

Justin Freeman: Brian real quick and then we're going to [inaudible 01:54:23].

Brian Hauss: Just to add, one group that I do think provides a strong constituency is the defense contractors: Booz Allen, Northrop Grumann; Boeing is another one… [inaudible 01:54:31]. These are major… Lockheed Martin, thank you… these are major companies.

Male: Excuse me. If they didn't have the power to have warrants or automatic surveillance, then doing what they would do would be more expensive not less expensive, that would leave more money for defense contractors, not less.

Brian Hauss: They would be able to do less with it than they are now if they had to get warrants. Right now they can do it on a massive scale because they don't need warrants. If they had to get warrants, they would have to pay the DOJ lawyers who are ready on government retainer. They wouldn't need to mess up the defense contractors.

If you're paying them less, there would be a lot less data for this contract is to analyze, to collect, store and analyze. It's the fact that the widespread nation of surveillance is of any interest to the contractors because they are the ones developing the algorithms, they are the ones running the scans, they are the ones doing all the intelligence work on this. A lot of the NSA work is contracted out to [inaudible 01:55:28].

Ron Yokubaitis: Snowden worked for a military contractor.

Justin Freeman: All rights, I want to thank the panelists, warm welcome