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

Is There Any Online Privacy Left? What Does The Future Hold?

An expert panel on what every Internet user should know

"Online Privacy" and "Internet Freedom" are the hot button issues of our generation gaining support worldwide following revelations of government spying, mass surveillance and data collection by corporations. We all leave footprints online that can be tracked, and governments can now learn more about us through a digital search than through a physical search of our homes. This expert panel will examine the current state of online privacy in the U.S. and worldwide, the conflict between government surveillance and national security, and the future of online privacy.

SPEAKERS

Kevin Bankston

Kevin Bankston is the Policy Director of the New America Foundation's Open Technology Institute, where he works in the public interest for a stronger and more open Internet, with a focus on issues of Internet surveillance and censorship.

Evan Greer

Evan is the Campaign Manager at Fight for the Future, an organization that's building a grassroots movement to ensure everyone can access the Internet affordably, free of interference or censorship and with full privacy.

Ali Sternburg

Ali Sternburg is Policy Counsel at the Computer & Communications Industry Association, a 40-yr-old international non-profit representing Internet and telecom companies, dedicated to promoting innovation and competition.

Rep. Bryan Hughes

Bryan Hughes represents District Five in the Texas House of Representatives. He is a member of the Committee on Appropriations and the Committee on Criminal Jurisprudence.

Ron Yokubaitis

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

PANEL MODERATED BY

Stacey Higginbotham

Stacey has covered technology and finance for 11+ years for publications such as The Deal, the Austin Business Journal, The Bond Buyer and BusinessWeek. At GigaOM, Stacey covers broadband, data center infrastructure, policy and regulation, and entrepreneurs/startups.

Full Transcription

Ron Yokubaitis: Hey everybody, okay if everybody knows - the bar is open, so have at it. My name is Ron Yokubaitis, and I'm Co CEO of Golden Frog, Data Foundry, Giganews, on and on. We're just here to further talk about taking back your internet; it's ours it ain't theirs, it's all of us and us happens to be in all of our 200 plus countries, so we all talk over 200 plus countries. We've opened this stream to our Golden Frog customer base which is in 195 countries and Giganews which is over 200. So when we want to blank out websites and send emails to the congress critters we get German and French folks that say great, we've been looking for a place to have a say.

So this is the place to have a place to have a say ya'll and we've got some neat folks up here who've been playing their part in keeping us free and open on the internet, so I want to welcome you all to Austin and everything that goes on here which goes on when SXSW isn't here too. Anyway, Stacey Higginbotham from GigaOM is going to ride herd on everybody here and keep us in line, keep you all in line; don't get too rowdy but get rowdy. Thank you all... Stacey.

Stacey Higginbotham: Hi ya'll, and if needed I will translate from Texan to everybody else speak, it could happen, I don't know how many of you are local but I do say y'all a lot. I'm just going to let you know that's not an affectation. All right, louder okay. All right, holy cow! I love you guys in the back who are communicating. Can we work the feedback down maybe? Okay you're all good, all right I'm going to introduce everybody real fast; at the very end we have Evan Greer who is with - he brought his fans - he's with Fight for the Future.

Next we have Kevin Bankston and he is with the New America Foundation which is an organization I am a huge fan of. Then we have our host for the evening Ron Yokubaitis, and then we have Representative Bryan Hughes who is, you're from Tyler and Longview Texas. All right and then next to me I have Ali Sternburg all right and she is with Computer and Communication Industry Association. Soon I will not have to consult notes we can just talk so I will not do that. Thank you guys so much for coming and we're going to kick it off really fast with basically everybody talking about in the wake of everything that's going on with the NSA which we're all aware that the ... actually first let's go for a little bit of nuance here just a little bit, privacy is important right?

We're all yay privacy. How many of us enable location on our cell phones? All right how many people surf the web without using any sort of TOR or VPN? You guys, is there a hash tag on twitter? Is it "take back the internet?" I'm going to follow this on my phone and you guys are going to have to tweet stuff - not too much stuff. We're going to have to use Twitter for this you all this is just done. All right so you guys are very serious about privacy with the exception of a few of you who are just like Google track me, Apple track me - whatever.

Let's start with you guys talked about ... they cut my mic. We're going to run down and everybody give me your sense of how privacy is today in terms of people understand the issues and they have access to privacy or not. Both understanding and how much access to privacy the normal person has.

Evan Greer: Well certainly we gained a much greater understanding of the privacy that we do or don't have since June of this past year. I think that one thing that we're seeing is that people have a strong understanding of what's happening with the NSA since that has been a hot button issue with the media. But it's important that we connect that with the other surveillance that has been going on for years and years and recognize that a lot of this isn't new and that we have to really look at the other governmental agencies, corporations and people outside the US that are surveilling us.

That protecting privacy isn't about just fixing one thing that the NSA is doing, it's about changing our entire culture how we think about our data, how we think about the things we put out there in the world and whether it's okay for people to aggregate them and define us based on the patterns in that data. I think there's definitely greater understanding and people are learning about things that they can do, but I think that we have a long way to go to connect this and get everyone to understand the big picture.

Kevin Bankston: Cool, hi I'm Kevin and on a personal note I just want to say I'm really happy to be back here. I live in DC right now but I went to UT, I wasn't born here but as the bumper sticker says I got here as soon as I could and there's really no place I've ever been happier than Austin Texas. Where are we on privacy? I think we're in a bad way but we're actually in a much better way than we have been. I come from a background of, I worked with ACLU, EFF, the center for democracy and technology and now New America so obviously I'm trying to work in all of them. If you found one in Austin let me know because I'd really love to come back.

Working at EFF where we focused a lot on government surveillance and the last time the NSA surveillance programs came to light back in 2005 2006, we spent years and frankly my friends back at EFF are still beating their heads against the walls of secrecy that surrounded NSA surveillance. It was an incredibly frustrating slog and to see the sort of floodgates open up, and for all that stuff that we said was true - like actually the NSA is tapped into our domestic backbone and just sucking everything up and running weird filtering on it. People were like, "Where's your proof, where's your proof?" We finally have the proof. We're seeing a lot more transparency about the company, not only about national security surveillance but about regular law enforcement surveillance. Stuff we've been trying to get reform on for years either on the hill or here in Texas with some success, thank you Texas.

We're seeing finally major mainstream media spending a lot of resources trying to explain these issues to us. For example like the Wall Street Journal, its multiyear "what do they know" series, sort of detailing all the different apps that are leaking information about you. I think we now know enough to know that we're in a really bad spot, and that collective action is necessary to preserve our autonomy and our ability to maintain some level of privacy in our thought, in our action, in our association as we move into a really exciting but kind of horrifying 21st century. That may not sound like a message of hope but it really is, we know more than we've ever known before and we know more than ever before how badly we need to act and act now. So that's where I think we are

Ron Yokubaitis: Thank you Kevin. Kevin and Fred Von Lohman work at EFF, when he was at EFF and his seminal work on freedom, liberty and putting the spotlight on all the shenanigans that are going on. The surveillance of us and of course Evan and Tiffany Chang in Homes from Fight for the Future are the folks that organize all the desperate groups on the net to email bomb Washington. They had no respect for us, they could steamroll or whatever they wanted through SOPA but this rubble rousing got their pitchforks and the shovels out in the street. Things are getting more better because we all are getting more aware and focusing the light.

Of course Representative Hughes from Texas we've worked with on getting Texas to pass the only bill that requires a search warrant for your content, your email. This state contrary to what you may read is really a haven of liberty because it's in the people. Ya'll don't realize but these people here in Texas, we think a little differently and we think we're open and free and we don't want you all getting in our chilies okay? Representative Hughes, [Carona00:10:46], and a few that's the cabal in our legislature and it's Democrats and Republicans this happens we've got both lobbyists that really cranked on this, good Republican and a good Democrat because we've got to get folks talking about it.

There is commonness in all this, but anyway and of course Ali is from CCIA in Washington which is a group we donate to and

work with. They're just public activists that a lot of the issues they put effort behind, we agree with; open internet, these kind of privacy issues so we bring her down we didn't get the big guy or the big lady but we got Ali I'm not depreciating her, but there are some really giants in this organization. I am so happy that Stacey is going run the show and keep me from talking too much.

Stacey Higginbotham: All right, state of privacy. Go for it.

Rep. Bryan Hughes: Thanks. I have some great news for you; the legislature is not in session so relax. Our founders wisely gave us this part time legislature so we come down here for 140 days every two years, I know better if it was two days every 140 years I know. Then we go back home and have to give an account of what happened and so some good things are happening we're encouraged about that. That warrant for content, email and then the amendment of Strickland from the Dallas, Fort Worth area a number of us worked on that and we're very encouraged with that.

There is work to do you were talking about location services, even with your location services turned off, you probably know this but the government can track you by your cell phone. Based on the towers you're lighting up and the repeaters and the phone cell and all those devices out there. They can get that data without a warrant, without probable cause, without you even knowing that they had it or what they're doing with it, so we've got some work to do there. Texas made progress we had a bill in the house with over 100 coauthors, passed the house, didn't quite get through the senate; it takes a while in the senate sometimes we'll get back to them next time.

We are encouraged overall and what you said about Texas heritage; again people tend to kind of broad brush politics in Texas but folks are big on freedom and liberty and I mean that, those aren't just phrases. My friend Scott Henson pointed out to me that Texas was protecting her citizens from wiretaps decades before the feds ever thought about it. Because we believe in privacy and liberty and freedom here so hopefully we can continue to move that way and I'm tickled to be on this panel and honored to be asked. Thank you guys.

Ali Sternburg: My co panelists have done a great job handling out the land, but one other thing I would say is that the companies that we represent here today which include Data Foundry of course and about 20 other companies. I think a lot of companies have been recognizing how much people care about privacy and have been doing a lot more to be transparent and to offer a lot more controls for people's data and other protections. Additionally there's been a lot more new companies coming out and you can really compete over privacy which I think is a really important thing.

That's one other thing that I would add is that there are different companies recognizing that these things are important and people will pay for different kinds of services and features on programs that control their data. I agree with lots of great things being said by the rest of the panel and I'd also like to say that I've never been at an event, even whenever I'm playing music or speaking at a panel where everyone is paying attention so much. It's amazing to see people actually looking; no one is looking at their phones people are actually looking. This is amazing so thanks for your attention, it's great to see that so many people care about privacy.

Stacey Higginbotham: We're going to share the mic down here. Okay so let's get this started with, I'd like to break this up into two thoughts because I think it might be easier and it might be a natural breaking point. One is government surveillance; so your rights under the government with like law enforcements, search and seizure. Then the other thing is consumer surveillance so this concept of apps and data leakage etcetera and yes the government can subpoena and get that information we can talk

about that too. I think that's probably a good framework as you guys are discussing these issues to kind of make that very clear what you're talking about.

With that in mind, I'd love for you guys to actually, maybe two or three of you, so give me a show of eyebrows or something who has a great story. I'd love to get a couple of examples of data leakage and how that affects the consumer from the app side. Give me your eyebrows who's got a good story? Evan's nodding along excitedly so we'll give.....

Evan Greer: I thought Kevin had a good one that's why I was nodding.

Kevin Bankston: I work mostly on government surveillance myself.

Stacey Higginbotham: All right we have no consumer side stories?

Ron Yokubaitis: Let me just say last at the Southwest we've had boosts all up until this year but nevertheless everybody was wanting to. Young kids were coming up to me with their latest social networking app and "Here try it it's free just put it on your I Phone." I said, "I don't want your damn spyware on my phone." They'd look at me quizzically - that was before Snowden. I don't think I would get that quizzical look today from the free lunch bunch I call them. The free lunch on the internet - there's no free lunch on the internet.

It's a surveillance society we have and these apps are surveilling you, so here it's free. Think about free, the price is very high, it's your liberty, it's your property because your information is property and you're giving it away, it's very valuable. I think when the government does it they're taking your property without due process, so we've got a real civil liberties fifth amendment issue here, besides fourth amendment. You've just got to realize how valuable you are, and what you think and what you do - and enough said. South by Southwest is almost dedicated in a way to your privacy leakage so be careful.

Kevin Bankston: I'll just add to that, there's a maxim out there and I think it's very true, 'if you're not paying for the service then you're the product'. Either your eyeballs are being sold or information about you is being sold somehow they're deriving value from what they know about you or what they know you are doing. So when you're getting a free service, it's really critical and I think a lot of the privacy thought right now is focused on ensuring that you actually know, what is the bargain that you are making. Why is this free? Why are they giving me this? What are the permissions that I am giving them when it comes to sharing my information?

One of the challenges we face and I think it's a really long term serious challenge like every developer, the FTC, lawyers everywhere are trying to figure out is, how do we actually effectively notify you the user of what information you're sharing and when, when you're constantly installing new apps. You're clearly not going to read all the terms of services. In fact there's a great study by a professor about like gauging how many hours it would take you to read all the terms of services you agree to. It was something like a third of your waking life, I mean it was freaking insane, and yet at the same time we don't want to say, "You can't make these agreements."

I think one of the biggest challenges we face is how do we ensure that everyone knows what they're agreeing to when they're

agree to it and I don't think anyone has a great answer to it yet. One other thing, another hard issue is the answer can simply be well make it a pay service because then you end up with a digital divide where the poor are giving up their privacy while it's the privileged who get to afford to have privacy and that's not a good answer either.

Stacey Higginbotham: Kevin you just took my point! I was just going to bring up the fact that AT&T in Austin is launching a giga power gigabit eventual gigabit service, and they have a $20 off if you let them watch and monitor your surf habits. I was just informed by … Oh my gosh.

Kevin Bankston: AT&T does not want you to hear what she has to say.

Stacey Higginbotham: That most consumers like over 75% of consumers are apparently choosing the cheaper version. Which you can guess from the advertisements on Kindle and getting $20 off at Kindle that people will do. But that's a really good point is we're moving to an economy where you have to pay for privacy. My question for you guys as panelists thinking about this in Washington and the state legislatures, what kind of reforms do we want to see to make privacy both more of a right but also just to make sure that this isn't something that only wealthy people can afford? How do you write laws around that or regulations?

Rep. Bryan Hughes: Thanks very much. My primary concern has been in the area of the government tracking us, invading our privacy, but this is a legitimate question and I think we're going to find the answer in a - not to just say this because I'm sitting next to him, but what Ron and his companies are doing. I believe there's going to be a free market solution to this because everybody wants privacy and some are willing to pay for it, and some are more able to pay for it. You made a good point we don't want it to be only available to the rich to the wealthy. I bet we have some business people here and we have some folks who understand the free market.

If you want to make a lot of money, make a product or service that the rich folks can afford and you'll make some money because there are a lot of them. But if you want to make a lot a lot a lot of money you make a product or service that regular folks can afford, that they need that they want and you'll get really rich doing that. The market is going to catch up if the government isn't putting barriers in place. Let me just digress for a moment, before I got elected I assumed that the business lobby and by that we could mean a trade association for a certain industry or a certain company's lobbyist. I assumed they would come up to us and say, "Representative we want free markets, we want low taxes, low regulations, you just leave us alone."

Some of them do but many of those folks come to us and they say, "We want you to pass this law making people buy our product, or putting up tax on our competitor, or giving us the subsidy," or asking us to come in to regulate their industry to keep the little guys out. If the government does its job if we don't get in the way, if we keep the market free and open then the free market will respond, but we've got to make sure the government is not screwing it up, that's my view.

Stacey Higginbotham: Any others? Go for it Evan.

Evan Greer: Sure, I think this is a super important question and it's been said that if you want to know the future of

surveillance, look at the past of surveillance on poor communities and communities of color. Because people have been experiencing this for years in extremely tense ways and it has very real consequences. I think that's important too because we can often talk about this in abstractions where it seems like government surveillance is creepy. It's not just creepy, it's tearing families apart it's landing people in jail; it's having real impacts in our communities. We need to recognize that and not just think of it as something that's kind of scary but something that is dangerous.

Now as far as what we can do about it, I definitely think clearly there are some reforms that we can push for that are necessary and they're sort of the rising tide that lifts all boats. If we can raise the bar for privacy that's going to help everyone but it will disproportionately help those who've been more greatly targeted by surveillance. I think we can also work on this with technology in making crypto tools making tools that protect our privacy not only widely accessible and affordable, but also understandable and usable by the general public and not just by people who have a great deal of technical ability.

I myself I'm not a technologist I work as an activist but I've been able to learn this stuff by having people teach it to me. If we make it more accessible, we make it more usable and we make it a collective experience not just that I'm protecting myself but that each of us are protecting each other because there's safety in numbers. The more of us that use this type of tools, the less they can spy on all of us and the safer we all are.

Ron Yokubaitis: Stacey, I'd like to chime in because I'm not going to chime in exactly, I'm not real concerned about the poor and the downtrodden per say. Even though my wife and I were Peace Corp volunteers and did all that at a time. Because what characterizes old Joe six pack or José six pack is they can buy a six pack and you can get a VPN service for the price of a six pack a month. Let's just put this in some kind of relativity and not make a new entitlement to privacy other than the constitutional requirement that we have an expectation of privacy, inherent as human beings from our government.
But not private surveillance by AT&T you don't have that right against private surveillance that's your market there, you don't buy it. Of course we have no choice due to the duopoly but what I'm going to say to you is - for the six pack of beer, or whatever your favorite inebriant is soon to be legalized. Whatever it is it's reachable by everybody. I just don't want to get the conversation distracted by all the worrying about the last person on earth to get it. Let's get the bulk of everybody in this room aware and start spreading from there and maybe you'll find it in your benevolence to help someone out that turn them on. I'm not too real concerned I mean this is pretty cheap stuff it's either beer or privacy - pick your choice.

Kevin Bankston: Ron and I don't agree on everything but we do agree on the need to impress upon people, the importance of spending at least some energy and resources and time on preserving your privacy. You were asking about regulation but in many ways code is law itself, the way that the tools work and the way that we work with the tools defines what can be done to us and what we can do and being cognizant of that is really important. To go back to the original question; I also just want to flag that like several people on the table I come from a simple libertarian perspective and my primary concern is government surveillance. But that means to an extent companies are able to build vast libraries of data about us.
That data is available to the government under some legal standard often a very weak one and that points to if you're concerned about consumer privacy and the data that the companies are collecting about you, you should be especially concerned to the extent that code is not protecting you. That we have law protecting you when the government wants to take that data and building the legal firewall that ensure that even if you decide you want to make that trade with Google or this app or the other to share your personal information with them for a particular use, that, that doesn't give the government carte blanche to come and rifle through it.

Ali Sternburg: Are we back on? Awesome, so I just had a few points to respond to. One thing that was kind of raised by both of my table mates on both sides of me was that, there's a saying they always say which is that 'the future has no lobbyist'. I think a lot of times the incumbents are the only ones that do have lobbyists so it's really important for newer companies and for consumer groups and for other kinds of advocacy groups to be raising these concerns when they might not be heard. The related point is that a lot of these revelations about how much surveillance is going on, in addition to I don't know if this is a transition, but in addition to all of the obvious liberty issues it's also an economic issue and a competitive issue for our companies and for trying to find business here and abroad.

A lot of this industry is based on trust and if people aren't trusting these companies whether or not the companies are actually cooperating with the government, it's hard to tell when there's lack of transparency. But a lot of the revelations that have come out are starting to undermine that trust and it's really an economic issue in addition to a liberty issue. It's one tree of that. Thanks.

Stacey Higginbotham: All right since everybody here is super excited about government surveillance, I think you guys are very excitable, we'll go with that. Let's hit this topic, so I'm trying to think about the best way to hit it but let's talk about transparency reports, so we'll kind of ease in to some of the constitutional issues in a bit. Let's talk about governments who have access to the data that companies are offering or are collecting and a lot of them are trying to put out these transparency reports to indicate, "Hey we've been asked for this data."

I personally think these transparency reports are almost useless; they don't give any sort of granularity. How can companies improve that and should they even be trying to? I mean like how can companies kind of act as an intermediary between one consumer and the government? Should we be expecting that?

Kevin Bankston: Yes, yes we should be expecting that. This is something my organization has been doing a lot of work on, that I did a lot of work on when I was at CT. Google was the first with the transparency report back in 2010 I suppose. We've seen an enormous amount of development. A year ago last week, Google, Twitter, Dropbox that was pretty much it in terms of transparency reporting. And they were only reporting on law enforcement requests although doing a pretty granular job of it and giving us a fairly good idea of the scope of government access to our data in law enforcement investigations at their services.
No one was able to report on national security requests because they were legally forbidden to. A year ago this past Wednesday, Google was the first company to issue a report that talked about how many national security letters they get. These are secret subpoenas from the FBI for subscriber information and they were able to get a deal with the DOJ. The DOJ said, "We won't prosecute you if you choose to publish how many national security letters you get in a range of 1000." They could report that they got 0 to 999 or 1000 to 99 and it sells, Microsoft made a similar deal a month later. This is not all the granularity we want but it did serve a purpose, to me as someone who's been working inter cell issues for over a decade was reassuring.
It was like, "Wow okay they're receiving fewer NSLs than I feared and it's affecting fewer users than I feared." Flash forward to June, Snowden boom goes to dynamite everything is crazy, it is being reported or misreported that the NSA has direct access to all these company servers, untrammeled access to whatever they want. The companies are merely denying saying, "That's not true but we are gagged from telling you more about it." This has started a yearlong fight, the companies and us in civil society pressing the government to let them say more.

We've had some success, some success. The DOJ has finally agreed after litigation, a bunch of legislation being introduced, a bunch of letters being written to let the company say like they said Microsoft and Google how many NSLs they got. But also how

many FISA code orders they get, not to be too wonky but FISA, Foreign Intelligence Surveillance Act is the wall that primarily governs intelligence investigations in this country. The FISA court issues a wide variety of different types of orders, they issue secret wiretaps, secret pen registrars which is tracking who is talking to who and when, access to stored content, access to stored records.

Then the big boogeyman 702 which is the big programmatic wiretapping programs that we really still don't understand the scale of. That's what PRISM is, that's also what tapping into the fiber is. The DOJ agreed to let the company say how many orders they received from the FISA court but not breaking up the type and having to range it in ranges of 1000. That has not given us more of a window into what's going on, and in fact it's been somewhat misleading because the one thing that doesn't include is bulk orders. Because they made the deal whereby and I'm sorry to get too wonky but I hope I'll bring it back.

The government basically loyally worded their words so that what was agreed to was, if you are reporting on the FISA orders you received, you can report on the number that you received and the number of accounts targeted in the orders. Not the number of accounts affected in the order, not the number of accounts whose data you're handing over but the number targeted. AT&T publishes the report following these rules; AT&T who we know is getting bulk record requests that impact every freaking user of AT&T. You know what their report says? That the orders affected less than 2000 people, because it doesn't include the thing we mostly need transparency about, which is; is the government doing bulk untargeted requests for all of our data?

That is not enough transparency, that is not acceptable and we need to keep up the pressure. Civil societies and the companies working together to make them give us more transparency. Both to allow the companies to say more but also to say more directly as the government about what it is doing. Which leads me to another point; we're in a really interesting spot, a bunch of us have a very interesting relationship with the companies. We are pissed off at them about a variety of things but we also are working in line with them on a number of things.

For the first time ever because of Snowden, we have the big internet companies working with us on national security, first on transparency and now in the past few months promoting reforms in the form of the USA freedom act. The White House's response to that, has not been to give us the reform we're demanding, it has been to open a new process to look at the consumer privacy practices of the companies in an attempt to split us.

Stacey Higginbotham: Wait, let me ask you guys because I think this is important but it's also a lot of information to take in. It's good information, but if you are talking to this group of people, so we've got 280 people in this room, what kind of language should they be asking companies for? What should they be asking for from their representative or congressman? Because that's what lobbyists in DC do, they write the legal language to get what they want and it's very hard to understand the implication, that's what your job is.

Kevin Bankston: I can tell you, so go to 'we need to know.info' that's a page run by the center for democracy and technology where I worked this past summer on this project. That is where the companies answerable societies got together to lay out very specifically in a letter exactly what they want. What exactly we all want is the right to say the specific number of requests we've received under every specific legal authority - please don't make us bucket them into one bucket. And the number of users affected by each of those and the type of data requested. That is what we're asking for that's our ultimate goal, anything that does not get to that goal is not enough.

We have practically every major internet company and every major civil society group, free speech group, privacy group on record saying that is what we need for us to have an accountable democracy.

Ron Yokubaitis: I'm a recovered lawyer so I started an internet company 20 years ago and so law just kind of.....but I didn't forget the experience and I'm still a civil libertarian around ISPs. With access to a lot of data and who has to answer and I'm the one, and Phil here does the geeking on it and Carmen who's not here on spring break handles, Carmen Garcia handles all the to and from. We get law enforcement requests, yes I have law enforcements from around the world contacting us for investigating it's criminal stuff. Let me say it's just not all civil libertarian stuff there's some dirty actors on the internet stealing stuff from you.

It's not all really clear when you're a service provider and have to deal with law enforcement subpoenas, court orders, FISA court orders. You see this stuff and you are required to keep your mouth shut because it's an ongoing investigation and you can't tell the people they're surveilling or getting the information on that they're investigating them for criminal case. This is the reality of the companies that is just broadly mentioned here. We're service providers on the internet; we have millions of customers globally. That is another issue but we have to constantly make those decisions and we're not allowed to disclose it.
Its interesting work but the criminal investigation they don't want us to say peep to our customers. If it's copyright that's another thing, that's civil we send the customer a notice that we've received a copyright complaint and that will go civilly. But I wanted to say in this we're all talking about the government surveillance and what started us was in 05, 06 was AT&T's surveillance of everybody. You remember the brouhaha when the Snowden of AT&T disclosed that AT&T had let NSA into their San Francisco central office and installed equipment, deep packet inspection equipment.

And oh there's a big brouhaha and everybody including Senator Obama were aghast, "We're going to do something about it." When it came to vote he voted for immunity for AT&T from us suing them for doing that kind of stuff under the civil rights act. So what the rhetoric is and what happens in congress, but the private companies are surveilling you and what we found with the FCC in 06 was about AT&T you all have consented when you signed on for the duopoly service to let AT&T surveil you, with deep packet inspection.

Now you've got to be a lawyer like Bankston to decipher what you consciously agreed to. You have no choice you're really going to get Tweedledee AT&T in Austin or Tweedledum Time Warner who have the same terms. But we found with the FCC, hired a couple of lawyers that are here today, great lawyers, and to try and alert the FCC that this ongoing surveillance is going on, and it was a dull thud. Now the Republicans were running the FCC then so new shot with Obama same deal - there's not a dime's worth of difference there, because they're all afraid of the telephone companies will get mad.

But they're surveilling you and the crime of it is you gave consent and you didn't know it. So whenever you want to confront them that they're taking your privacy, "well hell yeah fool you gave us consent." Just like you're going to give them consent for 20 bucks off to let them surveil you and get your....so the choice is in your hands, everybody, your choice not ours your choice.

Stacey Higginbotham: Before we lambast Washington too much, let's get Bryan's opinion.

Rep. Bryan Hughes: Thanks - briefly on that Nodus question... it's so fundamental I think we understand that, but when we try to make laws we try to make policies about this well the response we get is, "Well there aren't that many requests is this really a problem?" Of course we don't know. They know but they won't tell us. It's interesting for historical antecedent and I was talking about wiretaps in Texas and of course wiretap doesn't require a literal wire but it's listening to your phone conversation. You know In Texas, if you've been the subject of a wiretap or whether it was your phone that was tapped or whether you had a conversation with that person.

After the wiretap is over, when it's all over, the investigation is closed, everyone who was affected by that gets a certified letter notifying them what happened and when they were listened to. Man that sounds like a great model don't you think for electronic privacy as well?

Kevin Bankston: It's actually true for the federal law as well.

Rep. Bryan Hughes: There you go I think they got that from us but thanks. The good stuff they usually do, they really did get it from us you're right Scott. The point is why not apply that same notice on this breach of privacy which is so much more intrusive so much more common. On the notice when we were working on the cell phone location data, part of that bill required that every prosecutor and every judge report to us each year how many of these requests were made, how many were granted, what was the result of the investigation. We also had every carrier tell us how many requests did you get, how many did you grant, of course not people's names but so we know what we're dealing with.

It probably won't surprise you, we got a lot of push back from the carriers on that but that's okay there's nothing more fundamental than notice. I just want to aim at what you said, we have to know how much this is happening so we can deal with it... we have a right to know.

Kevin Bankston: Denied! By AT&T again because I was about to say something nice about Verizon their competitor. Verizon's new transparency report actually does have numbers of how many times they get location requests which is actually a really good development. Like that's information we didn't have before and we still don't have from AT&T I don't think.

Stacey Higginbotham: Sorry, I'm going to go to a new question, I know it you're so tolerant over there. All right so someone asked - this is actually an important thing and we can start talking about kind of constitutional rights here which everybody loves. Somebody asked are there laws that you can sue under to take back your privacy? That's a really broad question, maybe we want to start with fourth amendment search and seizure rights, maybe we want to talk about laws, but I'm going to open it up to you guys because you're all experts on this. Let's talk about what laws we have that are supposed to protect us possibly but maybe are being re interpreted to not protect us and kind of where those threats are for us. Evan, do you want to start with that since I cut you off?

Evan Greer: Sure, so one thing I think is that when we talk about privacy obviously there's an immediate attraction to the fourth amendment right? It's very clearly directly related, search and seizure has very clear roots in the origin of our country being upset about a practice of breach surveillance, and it's something that people can relate to. I think it's also really important that we talk about the first amendment right? Privacy is not about whether you have something to hide, it's about your right to be yourself and express yourself without the fear that someone is looking over your shoulder and that you might be punished by the government for being yourself, whatever that may be.

I think there's definitely been court cases and I'm sure Kevin can speak more of this, EFF has worked on it, ACLU has worked on it but absolutely this type of surveillance is killing our ability to freely express ourselves. It's killing free speech, it's killing journalism

and so absolutely we should definitely be tackling this from a first amendment perspective as well as a fourth amendment perspective.

Ron Yokubaitis: I totally agree, it's a first amendment issue, fourth amendment issue, fifth amendment they're stealing your property, but you're going to have to distinguish between when the government does it and when a private business does it. Because we don't have we have our constitutional rights first, fourth and fifth against government violations of our civil rights not private corporations. The remedies against AT&T are different than the remedies against the government, so we just can keep you know when you give it up by giving them permission you've waived it and that's what's going to be the first thing.

Of course you didn't give it up that permission to the government you're not giving that consent so we're going to have to have - I liked the idea having to send the letters on the civilian surveillance. I really like that I think that's going to have a chilling effect on them.

Kevin Bankston: Let me jump back to 2006 when what Ron called the Snowden of 2006, a gentleman named Mark Kline an engineer at AT&T showed up at EFF's doorstep with diagrams showing how the surveillance machine was wired in San Francisco. That was a big part of the law suit that we brought against AT&T and later against the NSA about the mass surveillance that was happening. We brought this case up for a variety of theories we argued the first amendment we argued the fourth amendment the obstruction and seizure of our communications.

We argued violation of the wiretapping law or ECPA, the electronic communication privacy act and violation of FISA the intelligence law. I think we had strong callable claim for all of those. The biggest challenge we faced was the issue of, in lawyer speak, standing - could we demonstrate that we had a concrete controversy that really affected us such that the court had to hear our case. The government then and the government now has had a really great weapon to use against you when you're trying to establish standing in a mass surveillance case. Which is them saying, "Where is your proof?" "Where is the evidence?" "Can you demonstrate that we actually took your communication or looked at your communication?"

"Wait you have news stories, those are just news stories the actual facts are classified." "What you have these diagrams? Well what the hell it's all classified and hey judge if you try and litigate this, if you try and let them have discovery against us to demonstrate what's happening, you're going to hurt national security, and you're going to make it easier for the terrorists to hurt us." That is the wall we keep hitting when we're trying to assert our rights. Not that we do not have the walls to assert but that they are using secrecy as the bludgeon, as the wall to stop us.

The hope that now my friends at EFF and back at ACLU and other organizations involved in this litigation, our hope is that the Snowden floodgates now have given us enough to convince the courts that we don't need them to give us any new information. We don't need them to declassify anymore, we have enough to be able to say, "Hey if you use Verizon, we know that your records have been handed over. If you use AT&T we know that your data has gone into some government box sitting on the network and we don't need any more information to be able to assert our rights." That remains to be seen.

Evan Greer: Just a very quick point on the constitutionality issue because I think it's not even a debate anymore that what they've been doing is completely unconstitutional. So we should just move forward from that and know that's true, but I think it's important that we look beyond that as well, because look at Golden Frog they have customers in 200 countries right? Those people deserve privacy too and so we have to understand not only is this unconstitutional, it's also violating the human rights of people all over the world and those people deserve privacy as well.

The internet doesn't really make distinctions about borders right? It's a global community and everyone deserves this privacy so we should be talking about this not only as a constitutional issue but as a human rights issue worldwide.

Ali Sternburg: Great points going around, one point on making laws going forward, it's definitely really important for these laws to be technologically neutral. Because it's really hard for regulators to anticipate technologies, that might exist a year from now let alone 25 years from now. It's really important that these laws not prejudice new kinds of technologies that consumers will widely adopt and to make laws hard to enforce or be realistic in the modern age.

Stacey Higginbotham: You guys really learnt a lot of stuff. This is actually an interesting question; are there models right now in other parts of the world for protecting consumer privacy from commercial entities, but also from government surveillance that we should be looking for as good things to emulate?

Ron Yokubaitis: Let me just lead off on that though I'm anxious to hear what Evan and Kevin say. We also operate in Europe and we really use for our customers the European privacy standards because we've got so few in the United States frankly. I would look to the sensitivity of Europeans, Central Europeans too who were under the yoke of the Soviet Union, but we're just talking about the French, the Germans. Those folks are very sensitive to their privacy and us as a service provider likewise and we're under legal restrictions in Europe. The easiest thing is to make Baxter's standard worldwide because that's the best standard we have.

But we Americans need to get some of the individual sensitivity the Europeans have, so we pressure our government to do what they've done in Europe. It starts right here so I'm pretty much street let's do it here and that's how we'll get the government, just like the emails from Fight to the Future getting us to blank our websites. We did it in Giganews and we got that worldwide customer base and we sent them to EFF site so they had all the tools for sending the letters to the congress critters.
Boy we had Germans and Dutch people saying, "Great they send emails too" because they were looking to just express themselves on this privacy issue and know that the United States controls so much of the internet that them getting a vote here affects their privacy in Europe. I say by us looking at them we have examples to replicate in our privacy here.

Kevin Bankston: There is a pretty strict data protection regime in Europe, I think that a lot of these concepts could apply in the US; I think other parts of it could face some first amendment challenge. Ultimately one of the challenges we face in the United States is if we're talking about regulating privacy we're also talking about regulating the true facts about people. Whatever we do, do to regulate privacy needs to be narrowly tailored, it needs to serve a clear, in fact a compelling government purpose. I'm not certain that we could have a restrictive regime in the US that they have in Europe but I do think it's an inspirational model and it's one we should look to.
The fact that the Obama administration itself in the blue print for consumer privacy they issued two years ago, followed in a lot of ways basically implementing what have been called fair information practices. Mostly about ensuring that you have adequate notice, ensuring that you have access to the information that is collected about you and an ability to correct it when it is wrong and that sort of thing. Unfortunately we haven't seen any movement from the administration promoting that blue print or getting it translated into any kind of legislation much less legislation that's going to move.

Right now to jump into an issue I started to talking about earlier, we now have another process that's in place to look at consumer privacy again from the administration. When Obama a few months ago did a speech about the NSA, he talked about

well the importance of protecting our privacy against the government etcetera, etcetera. Then he was like, "Hey look over here, the companies are also collecting a lot of data they can't actually lock you up or render you or anything like that, but you should really be worried about the companies. I'm going to start a new process at the White House to look at the issue of big data and what issues that raises."

I don't want to make light of that, I think that's an issue that is deserving of scrutiny. We need to be looking at how does increase in our ability to crunch big sets of data allow us to derive new information that was never derivable before for useful things and for scary things. I fear that this process has been created to divert our attention from the NSA and to cause the privacy advocates and the companies who have started to team up against the government on this issue to start with each other again. I want to hold the companies to account, I want to make sure what they're doing is fair and that we know what they're doing and that we regulate it reasonably.

I do not think that the cost of that should be us taking our eye off the ball in terms of getting meaningful reform against the NSA. Sorry White House but that's not going to work, we're going to work at this big data process as much as we can we want to see it generate something worthwhile but it's not going to be at the expense of us getting in front of the NSA reforms, sorry guys.

Ali Sternburg: I want to echo Kevin's point that's really important that these two very different privacy issues not be conflicted by anyone. The second thing to add on the international model issue is that sometimes I'm kind of skeptical of whether these other countries models for protecting their citizens privacy are really just kind of national protectionism, in kind of trying to deter competition from US companies. It's definitely something to think about what their interests are in trying to protect their citizens' privacy or whether they're just trying to keep out US companies that are bigger and competition.

Stacey Higginbotham: Okay this is another question from Twitter. This may be a final question I'm not sure what our time frame is, this is kind of a call to action question, so SOPA was defeated by a mass movement, lots of companies, lots of individuals calling their congressmen. What can the public do and what can the people here do to take that kind of mass action and do it effectively? I'm going to start with you because you're the guy we're trying to target.

Rep. Bryan Hughes: Like no other issue this is probably more important citizen engagement it sounds like a cliché I realize, but folks we really need to hear from you. Because this isn't an issue that shuffles the deck, for example talking about these bills for cell phone location data for email privacy. I'm a republican my coauthors on that bill were Representative Lon Burnam one of the most liberal members of the house, Representative Senfronia Thompson a neat lady from Houston the first black female member of the house back in the 70s and some other conservatives, some other tea party folks.

It really cuts across all the lines so that's good for us, that's encouraging that means it's a lot easier to get there. We have to confess that sometimes it depends on who's in charge, back when it was the patriot act the democrats didn't like it and now that it's Obama doing it the Republicans don't like it. We have to get over that we have to be consistent. I remember William F Buckley said back in the 1980s, "If the Democrats introduced a bill to burn down the capital, the Republicans would offer an amendment to phase it in over three years." That's really true in Washington, but the good news is our end people get this.

You were talking about the USA Freedom Act to reign in some of the patriot act excesses. So we got, my goodness we've got Mike Lee supporting that, we've got Paul Ryan with a stronger bill, senator Cruz is looking at that bill, he's looking at it favorably I believe. So there are some encouragements for us to re-shuffle the decks and work across the lines and along those lines I know many of us have heard of a group called ALEC the American legislative Exchange Council. They've gotten a lot of press and

they've been at the piranha whipping bowl or whatever the term is for a lot of issues and they differ along some things. ALEC is really taking the lead on electronic privacy working with Republicans and Democrats. Our friend Alan Macfarlane is here works with Ron and he's been a leader on this getting those guys involved, getting the companies and the reps Republicans and Democrats. The good news is we're right and people get this, I'll say this, when I walked around the floor of the house and I was getting support for these bills I would tell my friends, "Now here is what this bill does, now this limits what law enforcement can do. We're for law enforcement we want them to catch the bad guys, we want them to have all the tools they need, but this does limit what they can do, but that's what the fourth amendment does right?"

We recognize that in an open society so as we strike that balance we have to be prepared for some of our friends in law enforcement may get a little nervous if they think we're taking tools away from them so it's important we engage with them. The bottom line is if your reps, your senators hear from you that this is important to you they're going to get it done because the wind's on our back, things are going our way on this. I'm encouraged with the way things are going so your engagement matters like it has never done before so thank you for doing this.

Evan Greer: Amen to all of that; I think that invoking SOPA here is important and it reminds us of the power that we do have. Everyone believed that SOPA would pass there was no question and then in a day we changed all that. I say we I mean I'm literally talking about the people in this room we made some of the tools that made that happen. But this is also a different situation, it's a lot easier to stop a bad bill or stop a single piece of legislation than it is to build a long term movement that completely shifts our cultural idea around the type of privacy that we deserve. However I do think that we need those moments, those single moments that inspire people and make people understand the power that we do have.

I think that this is going to take a lot, it's going take arguing for reform, it's going to take pushing on congress, it's going to take getting those incremental steps that pushes us in the right direction. It's also going to take not asking for our privacy but taking it back with technology and so Fight for the Future this is something very specific when we talk about call to action but on June 5th the anniversary of the first story that came out from Edward Snowden's whistle blowing, we're organizing something called 'reset the net' and we mean that literally.

We plan to take back the portions of the internet that have been invaded by government surveillance turn them off. Turn them on back again with bulked up new armor, new technology like what Golden Frog and folks out here are doing, that's going to keep the government out of our business. This is something that we can do together because protecting yourself is important but collectively, thousands, hundreds of thousands, millions of people saying, "Heck no I'm done with this and I'm actually going to start doing something that makes this type of surveillance too expensive and too difficult to continue."
That's throwing the wrench in the gears and so we need to keep pushing on the government to stop doing that stuff we need to keep telling them where we stand on it. We can't wait we don't have time to wait; this could take a year for them to pass something and whatever they pass might not get us what we need and so we need to start right now with taking our privacy back and we can't wait any longer for that.

Ron Yokubaitis: Take back your internet.

Kevin Bankston: First of all I just want to add, I mean first off this is going to be a really cool thing and like I said earlier code is law and if you can protect yourself you're basically creating a law for yourself that protects you. But I think it's also important to recognize, there's an old saying in DC particularly in our circles, like it's really hard to get anywhere unless you can team up with the companies against the government or with the government against the companies. It's a fact when you're fighting all the

money in the world you kind of need a heavy hitter to help you out.

I think we not only need to talk to congress directly we need to talk to our companies the companies that serve us directly and say, "We need you to help us on this we are losing trust in you, to regain that trust you need to help us address this ." You are seeing it, you're seeing the companies starting to get pissed off like when the story came out that Yahoo and Google had, had their data links between their servers hacked by the NSA outside the country, they got really pissed off. When they started hearing about all these exploits of Apple staff, Apple kind of got pissed off.

So you have Microsoft starting to call the NSA an advanced persistent threat, like something you usually reserve for like state sponsored hackers which they are. Or apple calling them malicious hackers or frankly several goggle engineers calling them on Google Plus where most Google employees say things. This was not the official word of Google but you had these Google engineers like, "Fuck you NSA, like what are you doing? We are trying to protect our customers and here you are breaking our stuff, screw you." The companies are starting to get pissed with us and that's actually a great opportunity.

The more that they are angry, the more that they are concerned that they're going to lose business here and abroad because of this, the more they're going to be willing to ally with us and make Congress pay attention. I think we can help keep pressure on Congress by keeping the pressure on the companies.

Ron Yokubaitis: Can I throw something in? I'd like to get to yall's questions because that's where I think it will rip. But what you're hearing here is just awesome stuff to me too, of course I know Kevin but it's all on us pressuring Congress and it's the only way it's going to work and Evan and Tiffany and Holmes there at Fight for the Future have given us the conceptual tools just to Rabble-rouse like this but it's a legal framework. You mentioned big companies, you mentioned companies, well there's big companies and then there's us Ma and Pa companies. We're still a Ma and Pa company as is the vast bulk of American business that hires ya'll.

Austin is kind of big company centric because it's a government town, but we're all small companies but the large companies that really can make it then get so invested it's difficult for them to piss off mother nature, the government. We are kind of below the radar; some of the work has got to be with large companies that you all work for. We are just the smaller companies around here working in the open market rather than the big deals, government contract deals this and this; we don't do business with the government. Anyway I just wanted to throw that in there's big and small companies so we're not all in the same scale or effect or a part of the surveillance society.

Stacey Higginbotham: Okay so don't call Ron and tell him to start surveying you. All right so from that I got talk to your Congressman, June 5th reset the net, talk to big companies and now put pressure on big companies that you: A. work for. B. Just do business with. Don't call Ron. Now your questions so I need big hands, we're going to go, guy in front.

John Roland: John Roland, Constitution dot org, all this sounds great but I have sat in the club where agents hang out and listened to them joke among one another about how they were disregarding every law, they were disregarding the Congress, lying to their supervisors, lying to their colleagues and it was a joke for them. Simply passing laws telling them to behave themselves is totally useless, especially useless outside the United States. All those privacy protections are just window dressing, but there's also another problem where this agents also joked about how they had people inside almost every significant organization able to operate clandestinely.

Every organization including yours need to ask yourself, how have you hardened yourself against infiltration? What could an infiltrator discover and reveal to his handlers because there's probably is one and he probably can.

Kevin Bankston: So how do I get into this club? Okay, the Hawkindub okay I'll check that out when I get back to town and listen very closely. I feel you, I think that the challenges we face is that yes people in power will bend or break the law. I think it's ultimately cyclical, we had basically a lawless state in the 60s and 70s an intelligence community that was utterly out of control, completely unchecked, everything done in secret, assassinations, spying, telling him it's okay to kill himself trying to blackmail him.

We passed a new regime of laws, the FISA laws in 1978 and you saw a restriction, and then you saw 9-11 and them starting to break rules again and build a new surveillance apparatus. Then you saw the passage of the 2008 FISA Amendments Act, which mostly ratified what they were doing but placed some restrictions on it such that they contracted a bit, but then you saw that change. I see a cycle of yes they're going to reach beyond bounds and yes we're going to place new bounds and roll them in and then they're going to reach beyond the bounds and then we're going to have to pull them back.

That is the cycle, that is the fight, that is the process we're continually going to go through, there's never going to be a time when we've reined in the government completely, or that they have beat us completely.

Stacey Higginbotham: All right, bearded guy?

Male: You guys are talking a lot about companies collecting information, but I'm curious what your thoughts are about when companies lose that information. For instance with the Target hack, it was reported that they knew about it long before it went out public and they didn't know anything about it because they were just trying to see why they're on air. I'm curious what you guys think about that after this?

Kevin Bankston: There are a lot of states that have data breach laws that I think many of us are very supportive of and that they require companies to disclose to their users when this data is breached; unless it is super encrypted. We have seen some movement on ENDC on the hill to pass a federal data breach law. One of the concerns with that is that they want to preempt the state laws and that's probably to the extent of like we saw this great experimentation in the states to develop these laws. It's actually a good thing that they can do that.

Although we'd love to see a federal standard for this, I think there is concern that doing in the way that would foreclose states from being more aggressive is problematic. All in all I think data breach notification is at this point a standard in many states and many people want us to be a federal standard.

Stacey Higginbotham: Do you have a question? Okay.

Male: First of all a comment. I come from Europe. I'm politically incorrect. Just to make the disclaimer. My company is called Mind Your Privacy but I hate the privacy term. Privacy means nothing. Privacy has no real boundaries. In Europe we call it data protection. The data in Europe belongs to us. Here in the U.S it doesn't belong to the people. It belongs to the companies

that have collected it and that are using it. At the beginning of the panel you were saying that you wanted to speak about the government, the surveillance and the user surveillance. I'm sorry, I've just heard the first parts of the conversation and I think that, okay.

The Snowden effect at Tetra has brought a lot of attention on it but your kind of paranoia somehow looking from the outside. You have the, you know the, "Oh, the State is looking at me." When in reality the fundamental question is that data, the data protection privacy is a fundamental right. That's what you should ask your representatives and that's my question to you representatives. I come from Spain so I won't vote for you, I can't vote for you but what are you guys doing to give to the American citizens the right to have their data as ownership, the owners of the data as their property.

Ron Yokubaitis: Let me jump in ahead of the representative here. First of all we can see that a little differently. They do have to have our permission. That may not be perceived by you but let me say I agree with you too in the clip wrap that nobody reads. Okay, because we filed in '06 with the FCC under our Data Foundry Data Centre company about AT&T deep packet inspection equipment. Giving ongoing surveillance, storing your information as their work product in consideration for a little spam filtering and a few other stuff but they sort permission in the terms of service the clip wrap.

That's it, they know they have to get permission to get around our expectation of privacy, that is fundamental to our inherent rights on the constitution, the fourth amendment. They know that. As a private company they need to ask our permission so they don't get sued but we have no choice. In Europe you've got a lot more choice of providers. Here we get, like our political process we get … we don't have parliamentary multi-parties. We've got Twiddly Dum and Twiddly Dee. For a broadband access here in Austin and any about place you go that's a big city in the country you don't have anything, at our ranch we have nothing. Here we get Twiddle Dumb and Twiddly Dee.

We get Telco monopoly that no other Telco will compete with no matter how big they are. Verizon doesn't put one line in AT&T territory and vice versa. Wink, wink, wink and our government can't see the cartel working. Likewise the cable companies, you know … Pardon Me. Go ahead. Good, I better shut up.

Rep. Bryan Hughes: I would say under the US system obviously there's a distinction between protection from the government and from other people. And so obviously the fourth amendment says that "The people are secure and their persons houses, papers and the fax against unreasonable certain seizure and a warrant has to be based on probable cause for the government to get that data, that information." That's a real problem because that's not happening today. The fourth amendment is not being … Yeah. I'm getting to that. That's on the government side. As far as individuals and the question about database was a very good one.
In the American system, if our system is working right. If it's working right, we have a duty to one another whom we engage in the market place to act reasonably. To keep our word at home, we don't. The answer is a civil lawsuit. A civil lawsuit in America is a scary thing. I don't know if you've ever been sued before but a lot of money is involved, reputation is involved, damages, the punitive damages can come into play. When those companies, when a company or an individual acts in a bad way. In America the tort system, that's private law suits that's supposed to keep us in line and it's also an example of others not to do that again. Now it doesn't always work right and there are inefficiencies but that's how it's supposed to work. Those companies are breaking the rules. If they are breaking these data breach of laws or even basic negligence rules they are supposed to be held accountable that way. Again the problem comes in because the government gets in the way and we protect these companies for doing wrong. That's the real problem. The government needs to get out of the way so the market can work. There is a distinction, you are right. It's the constitutional right.

Ali Sternburg: Yeah. Also I spend most of my time on copyright and so this is another way where our law is different about how we think about our rights in very different ways. I think that your points are important but I think that a lot of our common law system thinks of these rights in different ways which is why our regimes differ.

Stacey Higginbotham: All right. Everybody, I'm going to take two more questions starting with …

Lora Moi: Hi, Lora Moi Public Knowledge. It seems like their some consensus among the panel about government surveillance, compelled disclosure of information. But there's disagreement about corporate surveillance in situations where companies are buying and selling information. I guess I'm curious about situations where the government is buying information from companies which we know happens. Charley Savage wrote an article late last year about AT&T selling the information, selling whole records to the CIA. I'm curious to know what your views are on whether or not regulation is appropriate in those situations.

Kevin Bankston: It's almost like you've recently filed comments with the FCC about this issue Lora.

Rep. Bryan Hughes: It's fundamental, that's fundamental at some point that becomes a government action. They can't say, "Well if we are private companies …" I agree, I think we have to look at that and … Let me just say this and let me a gross generalization. A big government in big business are often working together against the people and against small business and families and real people like us dare I say. This maybe an example that now … Again, I don't how specifically we are going to get in and I bet other panelists could do a better job but I'm a free market guy. When a company is acting in contra with the government like that we can hold them accountable and we can get those protections from the government, like I said same companies. Is that what you are talking about? I totally agree with that.

Stacey Higginbotham: Where do you draw that line?

Ron Yokubaitis: Let me speak for that. We've offered a solution to that and the only piece to open that neutrality but open that legislation. Rather than … I think it's a fool's errand that we are going to get our government to regulate these big companies. The FCC is captured by the telephone companies, the regulated. It doesn't matter whether who's in Austin, the big telephone companies are still the king. It doesn't matter whether which party takes control of the FCC the result is the same. The regulated runs the regulator. You notice on the FCC there's been no big pep walks for the biggest financial fraud in our history. The regulators don't do anything. We propose to give everybody a cause of action when they interfere with your connection. It may be worth two bucks in damages but you aggregate millions and there's some plaintiff lawyers that will take that case on the contingency they win. You put them up the tail pipe of the big company. They don't sweat the regulators because they'll own them; hire them or whatever you want to say. FTC, SCC, FCC all of them together but they sweat plaintiff lawyers on a class action coming up their tailpipe. That will make them change because it's big bucks and each one of us doesn't have much bucks but together it's big bucks.

Now that's not a solution, it's a private market solution not a government solution. It's not one the republicans like but the democrats love regulation and the way we are going to get it is individual rights asserted by all of us, aggregated by some tush

offs taking a percentage of the case and financing the case. Try that.

Stacey Higginbotham: All right, go.

Carl Shwinker: Carl Shwinker, I'm an attorney here in Austin. Unlike Ron, I'm not reformed. I actually have a case that I've filed against some of the companies you've talked about a big privacy case. A lot of problems seem to be that a lot of people talk about privacy in the ether without any real definition context. What does privacy mean to each of you?

Stacey Higginbotham: Keep it short Evan.

Evan Greer: Sure. Super Quick. Privacy is essential to anything that you care about. Whatever your issue is, whatever the thing you want to change in the world. Making change in the world requires challenging entrenched power. If those with entrenched power have the ability to steal our data and use it against us we are not going to be able to challenge them effectively. Whatever you care about you need to care about privacy. It's about your ability to change the world.

Kevin Bankston: Mine is not going to draw applause. I actually hate using the word privacy. It means so many different things to so many different people. I'd rather focus on this or that constitutional right or this very lawyerly answer. This or that constitutional right this or that statutory right but ultimately if I had to come up with some definition of it. It is the power to preserve for yourself some level of autonomy about what you think and what you do and who you associate with. The ability to find that quiet space where it is only you deciding what you believe and no one else deciding it for you.

You can only do that, maybe worth an applause line. You can only do that free from the watchful eye of others. You need to have that space for yourself and ultimately what I want to protect is privacy then that's what I want to protect.

Ron Yokubaitis: I'm going to define privacy as property. In the sense that your information is your property and you are letting someone steal it form you. Now you can let them steal it if you want but if you don't want it's theft. So I would define property, information as property. The government can't take without due process and the private business can't take it without your informed consent. And when you only have Twiddly Dee and Twiddly Dum as a choice you don't really have informed consent but I would approach it as property.

Rep. Bryan Hughes: Thank Ron. Man I wish I had written down your definition and what you said about that. Our founders talked about the concept when they said, "If we are to be secure, we shall be secure in our persons houses, papers and effects." Now persons is pretty obvious, house, my home is my castle whether it's a house or an apartment or a place in a hostel or it's my car. My papers are my papers and now papers are electronic and my effects - my stuff. I think that's constitutionally, I believe that's the concept - you know that - but you have challenged me to come up with a good definition. I think I'm going to plagiarize my co-panelist here.

Ali Sternburg: Lots of great points have been made. I think privacy is essential to being free. It's really important.

Stacey Higginbotham: Okay. I'm going to call this the last question because it's 8:30 but Ron, you've got the mics you can...

Ron Yokubaitis: Listen, it's our party you'll want to talk let's talk. More questions until, it's like Willy Nelson, he'll sign autographs until an hour after everybody doesn't want an autograph. Let's go for it.

Kevin Bankston: If we are going to keep going maybe someone should bring us some drinks.

Evan Greer: Whiskey

Kevin Bankston: Or the half of icing, please thank you.

Speaker 2: All right. My question and maybe some people in this audience aren't aware of what the third party doctrine is but it's an important thing to learn about. My question is how can we strike down the third party doctrine not just at the State level like what we've done with protecting minimal rights of Texas citizens but also at the federal level. I mean that to me is very important.

Kevin Bankston: We might want to say what the third party doctrine is. It will take a minute or two. Much of this debate hinges on this basic legal theory that arose from some Supreme Court ruling in the 70s. In the 70s there were a couple of cases. A case about bank records and a case about your dialing information when you call people. And the Supreme Court held that when you transact with a bank or when you dial a phone number that's transmitted to the phone company to connect your call; you are sharing that information with that third party voluntarily exposing that information to that third party. In doing so, you are assuming the risk that that party is going to share that information with the government.

Such that you do not have a reasonable expectation of privacy in that information but it is a reasonable expectation of privacy that defines whether you have a fourth amendment right such that getting the information requires a warrant. Right now for example the government is saying - Well. Yeah we are getting the records of everyone who everyone is calling but under this case in the 70s about a little device that was literally attached to an individual phone line and printed out a paper tape of the electrical signals of when you dialed a phone number and Didn't even tell you if the call was completed much less how long it was or anything like that.

That that somehow comparable to them getting comprehensive laws for years at a time of any phone call made in the country. That's the third party doctrine that this young lady is speaking about and that at this point is so pernicious when applied to new technologies that have nothing to do with what we saw before. I actually wrote a paper with a friend of mine Ashcan Soltani who is a technologist who's also been the technologist doing all the technology side of the Washington Post reporting on the NSA thing. We chatted how the cost of surveillance has been dropping over the decades.

One could have applied this logic to this kind of surveillance but we applied it to location tracking. We compared how much it cost to like follow a guy covertly in some cars with some agent. Compare that to attaching a beeper to their car to attaching a GPS device to their car to tracking their cell phone. You literally go from it costs thousands of dollars a day to it costs pennies a day. When you see that massive shift in the capability of what the government can do. To be hinging our decision based on how technology worked in the 19 freaking 70s is insane and is basically a recipe for us giving away all of our privacy however you define it.

How do we overturn it? There's a really hopeful sign. There was a case about location tracking that the Supreme Court decided a couple of years ago, USB Jones. It involved GPS devices that are attached to cars. The court had held before that you've exposed yourself when you travel on the public roads such that tracking you didn't file an expectation of privacy. But five Justices of the Supreme Court said we think this is different from those cases in the 80s about location tracking under that technology. And that

we don't know exactly what the line is but we think that being able to comprehensively track your location for 28 days without ever being even close to you but simply pressing a button is different. It does violate your expectation of privacy.
I think the Supreme Court has opened the door to revisiting of the third party doctrine. Open the door that hasn't been opened, this is our first huge chance to really overtake this. I've talked far too much.

Rep. Bryan Hughes: No. It's tremendous, allow me to make one distinction about the third party doctrine - that has do with what the Supreme Court says the fourth amendment means, right? If we get rid of the third party doctrine then the Supreme Court could very well rule that the fourth amendment requires a level of protection we are talking about and I hope that happens. But even if that doesn't happen, even if the Supreme Court says the fourth amendment does not protect this stuff that nothing is stopping Congress from passing laws to do what we need to do. That's the good news.

I hope we can see the third party doctrine thrown out but even if it doesn't happen we can still win. I think Congress; bless their hearts I think they are trying. If you look over history in 1934 they outlawed wiretaps. I keep talking about wiretaps. They outlawed wiretaps then in 1968 they came back and they allowed wiretaps put rules on them and they also included the sort of cutting edge electronic communication, more than just wiretaps. Then in 1986 they tried to update that law and they tried to include emails and all the technology at the time.

They did a pretty good job but if you go back and look at that they are trying to give us the protection we need. They just haven't done it since 1986. I hope the third party doctrine goes away but even if it doesn't we can still win. I think that's supportive.

Kevin Bankston: I'll just add to that and perhaps Ali wants to as well. Right now there's a year's long fight that is culminating in Capital Hill to do what ya'll done in Texas which is regardless of what the courts say about the fourth amendment, the government should have to get a warrant if it wants your private communication, whether it's stored in your house or in the cloud. There are several like reform bills out there. There's a big coalition the Digital Due Process Coalition that's been fighting for it and still fighting for it and could definitely use your support.

Stacey Higginbotham: We are losing that half so I'm like do I see questions? I see no questions. Going twice, oh, there's a question.

Speaker 3: I'm just curious to hear what work you all are doing on the ground to organize and mobilize people to speak up for these kinds of protections and rights?

Kevin Bankston: Perhaps the activist?

Evan Greer: Oh, me the token activist, no. This is a super exiting time to be involved and I seriously encourage. When I said earlier we evoke SOPA a lot around this and SOPA as an epic fight. But this needs to be even more epic because stopping a bill is significantly easier than shifting our entire culture and creating a whole new set of both policies and technology that can protect us. This movement has been growing incredibly quickly, Fight For The Future, Demand Progress, EFF. There's dozens of organizations out there working on this and I encourage you to get on their email list, get active and get involved. Sometimes it's as simple as clicking and emailing your congress person or calling. Sometimes there really are concrete ways that we can laser focus on one bill or one thing that gets us what we need.

But more importantly is that we need momentum and we need involvement from as many people as possible. One thing that we did recently this past year, we crowd funded a video. You can find it at nsavideo.com. We didn't just throw it up online. We wanted to show that people care about this enough to get out in the streets.

We projected it onto the side of a huge building in Manhattan and brought out about 300 people that spilled out into the street to show that they're not just going to take this sitting down. I think it's … And then a few weeks later, we turned out 3,000 people in D.C at the Stop Watching Us protest, people from across the political spectrum. I have never stood on a stage with such political diversity. It's pretty astounding, right?

You have Dennis Kucinich and Representative Amash speaking back to back. You know what I mean? That's serious. That's the type of unity that we need to fight this. I strongly encourage everyone to get involved and to stay involved that this isn't just one thing that we can fix in a day. It's something we're going to stay up on probably for years.

Ron Yokubaitis: Let me jump - exactly. That's a longer … Our results when we filed with the FCC in '06 about the deep packet inspection and we mentioned the third party doctrine is … The problem is nothing was going to happen on that time frame. That's what? Eight years ago, this a little more mature. Rather than get mad at the political process, get even. We're technologists. We will create some tools to protect our privacy. There are tools. You can encrypt whatever the NSA got it, it's a bunch of gibberish or they may have to go 10 years before they get enough processing power to decrypt you.
You can take it upon yourself. Yes, we started a service to do that. We found global demand for this. There is a lot of countries far more surveillance than ours, you know? I don't need to mention them, but our second largest customer base is in China. Nevertheless, you've got encryption here, Phil Zimmerman, PGP. We just don't use them. We just say, "For twenty bucks off." Or as I've said for years, Americans will sell their privacy for two coupons and a buck stop.

And that's cheap deal we're doing. You've got to think better of yourself. You've got to realize you're a free born American SOB and work to get away with it and encrypt yourself and frustrate the government on an individual basis. We wait for the Mass Movement, the guys that fight for the future and girls. They're going to help to give you direction and a framework to express it politically. And Kevin is going to belabor as many others are, including us, to give you a legal framework and fight the tremendous lawsuits they have.

It's just ultimate respect for EFF that people don't know started here in Austin. When the Secret Service invaded our own customers, the Jackson brothers, Steve Jackson Games, and walked in and took all their servers because they were looking for one guy. Every … all the innocent people I would give to you Megaupload too, all the innocent people using their service. Hello Kim? Come see us the text. No, we can't. We'll have go to see you at the zoo. But you know they were taking it. So you got to take an individual step while at the same time working massively to get the government on our side with data protection. Thanks you all.

Rep Bryan Hughes: Amen. Thanks Ron. We've said this … I'm so glad you asked that question. We always … politicians talk about building coalitions. Well it's real. We have the ACLUs and we have to conservative coalition and Tea Party. They're all together on this. Thank you. They're all together on this and there is a reason for because it's not just a cliché in America.
The government really does work for the people. It's still true. Aren't you glad that's still true in America? Aren't you thankful for that? I am. I really am. I hope so too. You know what? I don't trust the Republicans with this power and I don't trust the Democrats with this kind of power. When you call your congressman and your senator, talk to them about the USA Freedom Act. Congressman Sensenbrenner who wrote the Patriot Act, he realizes it went too far.

He is out with the USA Freedom Act. Please remember that for your senator and congressman is the biggest blow we can strike right now into this surveillance thing. It doesn't go far enough, but it helps. We don't not trust anybody with this power because we are all fallen sinners, you don't want to give that power either. We're thankful to have a system where the government has to listen to us. If they don't listen to you, you can run against them or vote them out now. Before you run against me, talk to me. Give me a chance. But your activism really does matter. It really works. I can attest it works. Thank you guys for being here.

Stacey Higginbotham: I've got orders here. All right, thank you guys so much. Thank you panelists.

Rep Bryan Hughes: To USA freedom in all senses of the word.

Stacey Higginbotham: And everybody, a toast to privacy.

Kevin Bankston: Thanks guys. I did. I don't know, what was that? Thank you everyone.