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

LinuxFest 2014—Golden Frog's Fight for a Private and Open Internet

Video Details:

Michael Douglass, Co-CTO of Golden Frog
Discusses what Golden Frog is doing to preserve a private and open Internet.

Michael spoke as part of Golden Frog's Online Privacy Discussion at Texas Linux Fest 2014.

Full Transcription

Michael Douglass: Please continue to partake of the drink and the small fingery food items. I think the schedule has me talking for half an hour. If I talk that long, it'll be amazing. I think we will plan for half an hour, and I will talk through it so fast 10, 15 minutes. Most of them have left already, but I do want to thank the panelists. I think two of them just walked out. A couple of them traveled here, one from out of state, one down from San Antonio, so we definitely appreciate them coming and helping us spread the word of the state of the net and privacy.

A brief background about myself. I am Co-CTO at Golden Frog. I share that role with the gentleman who was in the back of the room earlier as well.... as well. Under me, I manage and direct all the software management. He handles all the operations, hardware and all that fun stuff on that side. From the other side of the house, we are a very agile shop, very open shop [inaudible 00:01:12] started the company for 20 years. It'll be 20 years this December, worked for this family, and it's been very interesting.

I hope today that you either discover or you reconfirm or you found the truth that privacy and security is not something that we as citizens of this nation, the world, whatever country you're from; it's not something that we delegate to the government to take care of and protect us from. It's something that we have to own for ourselves.

When I was preparing this presentation, I had no idea what you guys were going to talk about or exactly what they were going to say. I knew the overall topic, so I was very pleased that I heard several of them say "you need to own this." This is in your hands, because the truth is governments are not going to do it. They're not going to do it universally. You may come from a government from a country where you have the strongest laws and the surveillance, privacy laws, but the truth of the matter is that you live in a world where the internet doesn't exist inside the boundaries of one set of laws.

Really, till Snowden came out... I've always been skeptical about what the government is and isn't doing, but Snowden showed us the worst case scenario that I will I admit I did not allow myself to believe that it was as bad as it really was, that they are trapping all the information, that they are storing all the information and keeping it forever. These are the things that were behind how we got where we are today.

Really briefly, I just want to go over who Golden Frog is. Who is Golden Frog? We started live in 1994. This is actually when I started working for the family, as Texas.net, a small dialup ISP down in San Antonio, Texas. Over the years it grew to include Austin, Houston, Dallas / Ft. Worth. As part of that, back in those days, if you remember, one of the services that you received from your internet service provider was Usenet access, and we ran Usenets for a while. The other ISPs came to us and said, "we

hate running Usenet servers. Can we just pay you to provide Usenet?"

In 1998, we formed Giganews and began reselling our Usenet servers that we were already running for our customers to other ISPs, and global customer base. Then at some point, I'm not sure exactly what year we started doing it, but we started selling direct consumers Usenet access. Now that your ISP service no longer comes with Usenet, if you still want to have Usenet, you have to come to Giganews or another one of the Usenet providers in the world.

This is coming to some of the stuff that we're talking about here in this panel. Coming up to 2000, we realized that being a dialup ISP was not going to survive. The incumbent, monopolistic style of telecos and cablecos were not going to let us be an ISP. The independent ISP was going away. We had AT&T, who were Southwestern Bell at that time, were buying POI lines so we could provide DSL to our customers. We order, they say two weeks. Two weeks comes, they say, it's another two weeks. Literally, two weeks came, and they said another two weeks. It was obvious that if we wanted to continue to be a viable business, we had to find other lines.

So with Data Foundry, we moved into providing data center colocation services. We have had several data centers over the years. Today we own and operate two here in Austin. We have one in Houston, and we just broke ground on a purpose-built data center that we are building from the ground up in Houston, replicating what we did a couple years back here in Austin with our flagship data center.

Fast forward to 2008, we formed Golden Frog. Golden Frog is not incorporation, if you noticed. We are actually out of a European country, somewhat for privacy concerns. Again, just like the Data Foundry was formed because of the real aspect of the incumbent, monopolistic, government protected ISPs that were coming up, Golden Frog was formed for the very reasons and things you heard here.

We have spent a decade plus going to Washington, going to the state governments and rallying and just trying to get them to pass laws to protect your privacy, to protect your security, to allow you to have privacy in your home, in your stuff, in your materials, data and metadata both. It was clear they weren't going to listen. The panelists even said - now that Snowden's come out, suddenly these people are listening, and they're passing bills. The Texas laws, we could have passed both if Snowden had come out one month earlier.

Briefly, some of our advocacy highlights of what we have done over the years. Back in 2000, we advocated for doing a Time Warner / AOL merger to get open access to the independent ISPs to the Time Warner network. It was passed as a requirement of the merger. Time Warner never actually did it, at least not for us. We knocked on the door many, many times, but then by 2002, the FCC reversed the decision, and the network was closed anyway.

In 2005, we were very involved in the FCC's policy statement on net neutrality, including making sure that you had access to lawful content of your choice. You could run applications and services of your choice, connect your choice of devices, and to have competition among network providers, application providers and content providers that you could choose from.

Net neutrality was not a name that we actually picked on all this stuff. It's what people turned a lot of what we were saying about consumer choice, which is still a term we much more prefer over net neutrality. Because what is net neutrality? I don't know what that is. If you tell me consumer choice, that tells me something. That tells me that you're letting me choose who and how.

In 2006, we began filing formal comments with the FCC on all their broadband proceedings, and we have done so every time since then that they've come out with.. "hey, we want comments from you on some ruling that we're preparing to do." Again, it's all around the open access, the protect the customer choice, protect privacy, requiring true consent before any monitoring

occurs and not what we have today.

The panelists talked about this. We live in a world where if you have broadband service through Time Warner or AT&T here in Austin, you have signed away, in the terms of service the right to monitor what you do. AT&T specifically says that the data that you transfer on my network is my business record, so if you're not encrypting it, it's mine. That's what AT&T is saying in their terms of service. It's stuff that we have been saying for a long time. We're very happy that suddenly now people are listening.

The end-all of this is to say that this is where we come from. We come from a background of advocating for your rights, for your privacy, for your right of choice. Golden Frog was formed because we were growing very tired of waiting for the government to actually take action.

Last year, Ron Yokubaitis, who was the second gentleman here on the panel and is our co-CEO, he authored a vision paper that I actually took from here because I love the vision paper and I thought that it rung really true with what we were talking about. The realities that we live in are that, worldwide, freedom is challenged by those who think they know better than us. That's the government. They think they know better than us, so they're going to do what they need to do, what they feel they need to do, and in doing so, continue to challenge our freedoms.

Again, this is Ron's paper, so here it is. Encryption is the Second Amendment of the internet. In this digital age, encryption is the only tool we have available to us to protect our privacy, and the right to have secure communications in any society, be it the internet age society or societies before the internet, it's essential for freedom that you're able to communicate in privacy.

The false promise of net neutrality - so we lived for quite a time under this open internet order of the FCC, but it's now defunct, and we don't really have any true hope that it's going to get revived with anything that has any teeth in it. Our response to this deafness of Congress and the FCC and the Federal Trade Commission to all the unwarranted surveillance, again, I've already said this and I'm probably going to say it again a few more times, this is the catalyst behind Golden Frog. This is why we do what we do, why we got involved, to create encryption and private storage solutions and network access solutions for the consumer.

I can't remember who this quote is actually taken from. It's in the paper, and I didn't write it down in my notes, but innovation is the answer. I think it is very important, just as it is with any Internet Age business. If you stop innovating, you die. Privacy and security on the internet is no different. If we don't continue to innovate, if we don't continue to make is easier and more secure, then we might as well not do it.

Briefly, and I promise we're almost done with the who we are background, and we'll get into what we do a little bit here. Our core beliefs, own it. We own and operate our own gear, own networks. We run our own switches. In some cases, if we have our equipment in a Data Foundry facility, we own the dirt, and we own the building, and we own everything in that building, so there isn't some third party is having access to my servers that can let the FBI in and go take stuff without us knowing it, so own it is important to us.

Encrypt it. We encrypt as much data as we can, site-to-site, local storage, encrypt it. Minimize it. If there isn't a business reason to keep it, and I think this was said possibly by someone out in the audience and up here. If there isn't a business reason to keep it, don't keep it, and if you do have to keep it for a business reason, get rid of it when it no longer matters.

Open it. We do our best, and we actually have several internal efforts right now to be even more transparent with our privacy policies, our data retention policies of how we treat your private information.

Lastly, simplify it. User experience is so important in these things because as said up here on the panel and has been alluded to

by a lot of people talking about security encryption is it's hard for the average person. We are here to make it easy.

That's who we are, where we came from. Now we'll learn about what we do. The Dump Truck was one of the first projects that we came out with, and it is an online private storage platform. Part of the problems that we're trying to solve for when we jumped into this - It wasn't this crowded as it is today when we jumped into it, but at the time, one of the problems we saw was that a lot of people, Dropbox being a very big product that went out there, were using other people's hardware, were storing your data with other people. I can't, as a provider, give you any assurance in privacy if I'm literally storing it on somebody else's hard drives.

The second problem we saw was through the use of data de-duplication, and the problems that we saw with data de-duplication is that the associations that it makes between you and another person is not because you actually know that person but because you have the same file. Or depending on how people are doing the storage, if they're chinking things up in intelligent ways to really get the best use of the storage, if you have similar files. There might be five of you that don't know each other, but you're all an advocate for this same common principle, and you've got this white paper that you're reading. You might not know that you have an association with four other people in a room, but these providers who de-duplicate your data can make those associations.

The solutions, I think, for these two things are obvious. You own the storage. You won the network. You own the data center. You own the land. I'm not storing your stuff on somebody else's hardware, on somebody else's solution. And don't de-duplicate the data. Sounds like an expensive proposition, but the reality is if you don't want to make those dangerous associations, that some government can walk in and just abscond with, you can't go down the route of de-duplicating your data with somebody else's data and form those associations.

This was actually brought to light someone with the Kim DotCom where they were talking about "oh well you gave this to me, so you should know that these are the five or ten people because we de-duplicate the data, but they're all having the file as well." It was made very clear that, yes, this is a problem, and people are seeing it and using it out there.

VyprVPN, for anybody who doesn't know, is a consumer VPN product where you can travel, be at home, be at the coffee shop and connect to any of our POPs worldwide to protect yourself, to encrypt your data so that the people around you aren't snooping on you. Your ISPs not snooping on you. AT&T, the business record thing, VyprVPN says, AT&T, you can have business records of a whole bunch of garbage that you can't read. Among several other of these cases for having a VPN, being able to geolocate yourself somewhere else in the world, again, privatizing yourself.

The problems that we're looking at VyprVPN solving around some of the topics that we talked about here are the anti-snooping, the problem being that the ISP and the government's snooping on you. I don't really think I need to add anything more to that today. I think you guys have heard it enough, but another real-life issue is a guy in a coffee shop. You're here on a public Wi-Fi. I don't … actually; I do know that guy over there, but do you know whether everybody in this room on this same network. I think I left my Wi-Fi on.

The solution here, that's where we're bringing in VyprVPN, using these tested and encrypted algorithms, using that the highest we can. Really, the way I look at it, the way we look at it is you're moving your point of trust from your ISP, your network point, to a Golden Frog data center presence where we are putting forth ourselves and telling you this is what we are. This is what we do with your data. This is how long we're going to keep your data, and by the way, if that changes, we're going to let you know.

Throttling is another issue that you find with a lot of home networks anymore, and it's pretty prevalent. I don't know if it's on purpose sometimes. Sometimes I think it's just shotty practices - ISPs throttling your video or any other traffic. I know here in Time Warner I've always had problems getting YouTube when I first moved to Time Warner. Watching YouTube was a practice in

we normally hit pause, and then go to do something else, come back, now I can hit play and I can watch it. Otherwise, it's going to stutter, pause and whatever because Time Warner is sending me through some crappy caching systems they have that's destroying it.

The more common problem that you hear now is ISPs and their poor peering agreements in associations with large content providers. For us, I look at an ISP as I'm paying you for a service, to provide me access to the internet, the best access to the internet you can. Why is my YouTube horrible? Why can't I watch Netflix at high definition? Oh because they won't pay you too? I thought I was your customer.

So Golden Frog and VyprVPN, A, helps with some of this because it, A, encrypts you, so they can't say you're doing as well as, you're doing YouTube? I can't send you to the caching servers because I don't know you're doing YouTube, so you're going out through our network to get to YouTube. And because we own the infrastructure and we actually care about our customers' experience, we do proper network management. We make sure we have the bandwidth to your ISP so you can get to us, and we make sure we have bandwidth to Netflix and to all these different content providers so that you don't have these problems. We're not going to Netflix and going, and saying "hey you need to pay me if you want my customers to reach you." That's not what we are.

We're starting to coin a phrase that we're envisioning VyprVPN being your virtual ISP. It's moving your ISP from where you are physically to us, so you take your ISP with you. Go home, have your ISP. You can travel abroad, have your ISP. It's a known entity, known quantity.

Another issue that VyprVPN helps with is anti-censorship. There are many, many different types of censorships around the world, and VyprVPN is really helping a lot of people. I've heard people talk to me about, I was traveling in China. Actually, a guy who used to work with us way back in the Texas.Net days I saw here today, and he mentioned that he was in Iraq, watching his Netflix, which you don't get to do in Iraq. VyprVPN will help you punch through those firewalls.

We are actually taking steps with our Chameleon Protocol to go even further than just a VPN connectivity. They're going further to try to obfuscate it so that the people you're connecting through don't even know that you're doing a VPN because somehow these great firewalls are starting to catch on and say, let's just block VPNs. Every time we find a way a VPN's coming through, we're going to block a VPN. So with Chameleon, we are essentially looking to how can we play the race game of continuing to stay ahead of how oppressive regimes and other people who want to censor what it is you're doing.

The opposite side is, once you're connected to us, we're not going to censor it. We have our own DNS servers. We're not going to block your access to things via DNS. We're not going to firewall it through any other way. We're taking the ISP world back to more of a common carrier in a legal sense. It's a pipe. It's your pipe. You're paying for that pipe. Use it as you wish.

If innovation is the answer, it can't be stopping there and being happy with what we have. We have to be thinking about what we're doing next. On March 10th of this year, at South by Southwest, Edward Snowden, bouncing through several proxy servers around the world, spoke at a South by Southwest interview with two gentlemen from the ACLU. This is a statement that Snowden made in that interview. I want to play a short video clip here for you of Chris from ACLU who I'm not even going to try to pronounce the last name because I didn't check it before coming, what his response to this was. Of course that would happen. I know exactly why that happened. I muted it earlier when the email was dinging at you during the panel.

Male: By the way, he was actually one of several people who had TED talks a couple of months ago, all talking about internet privacy issues that our government has created. There are at least three of them.

Michael Douglass: I saw the robot in a picture the other day.

Christopher Soghoian:[Video] Now that doesn't mean that small developers cannot play a role. There are going to be hot, new communications tools. WhatsApp basically came out of nowhere a few years ago. What I want is for the next WhatsApp or the next Twitter to be using encrypted, end-to-end communications. This can be made easy to use. This can be made usable, but you need to put a team of user experience developers on this. You need to optimize. You need to make it easy for the average person.

If you're a startup and you're working on something, bear in mind that it's going to be more difficult for the incumbents to deliver secure communications to their users because their business models are built around advertising exploited services. You can more effectively and more easily deploy these services than they can. If you're looking for an angle here, I think we're slowly getting to the point where telling your customers, $5 a month for encrypted communications, no one can watch you. I think that's something that many consumers might be willing to pay for. [/Video]

Michael Douglass: Meet Cyphr. We were actually quite well under way of developing our own end-to-end encrypted communication application. Mobile is where we're starting. When the South by Southwest interview went live, and I was sitting in my office listening to this, and I'm just going, keep talking, guys. He keeps saying exactly what we're thinking, what we're saying, what we're doing. Just a couple of points he made was he wants the next one to be an encrypted communication. That's a key core to what Cyphr is. Cyphr is private key encryption. You own and control the key. We can't read your key. We can't see your key. We can't decrypt your data. I don't know what you're talking about. I, as a provider, don't have access to your information.

Make it easier to use. There goes the email again. Make it easy to use. That's what we do. VyprVPN is a very clear understanding of what it is we do in terms of making it easy. We have in-house UI/UX people who help us keep things easy, keep things understandable, keep them clear to the end user. VyprVPN, VPNs are not easy to set up. For people in this room, VPNs are probably really trivial to set up, but imagine calling your mom and saying, "okay mom, I want you to download the VPN. You've got to get the CRA. No, no, stop."

Through VyprVPN, that's really how we have is user applications and all the platforms we support is we make it easy. What I would do is, mom, I want you to go to GoldenFrog.com. I want you to sign up, download the application, and install it. You've just got to use a username and password. Then just click connect. That's all you need to do. We're bringing that same type of desire, making things easy to use. It's not clunky. If you go out and look at the world of private communications today, the apps are just frustrating, and we are taking very seriously this call of making it easy to use.

Another things Chris said is that he thinks this may be something that you're willing to pay for. I heard several people on the panel today say that same thing. People are going to be willing to pay for services that keep their communications private, keep them secure. We certainly hope that's true because part of why we do Cyphr is so that we can continue to do these types of developments, and developers are not, by the way, cheap. It takes a lot of money to produce these types of applications, and we want to keep doing it.

I have just a couple of more things. I want to talk a little bit since I am at LinuxFest with a whole bunch of computer people here, to talk about, a little bit, of the technology that we use at Golden Frog. Did you all know that we own our hardware? I'm not sure you do yet. Again, it's part of who we are. We control our destiny. We control our privacy, your privacy.

We're longtime UNIX geeks and longtime fans of Linux, and we utilize all sorts of open source projects in Linux to run our services and provide what we do provide. Owning it also brings upon the need to hire and staff our networking folks, system administration, our devops, so we have very robust teams doing that within the organization, and we're always hiring if

anybody's looking.

We do all of our own native development on Windows, Mac, iOS, Android, Linux and other platforms, Objective-C, Pearl, Python, C, C Sharp, Scala. You name it, we pretty much do it. The last point here, we're an agile development shop. We are very agile, very open in our development methodologies. It's nice working at a shop where agile is truly from the top to the bottom. Executive staff gets it. They work with it, all the way through to the guys doing QA, the guys in support. It's all worked in the process.

It's very nice for me, having worked in this company for 20 years, to actually see us adopt and take on something. We actually hired a lady to come help us do that, and it has been game changing for us internally of how fast we can produce and do work and whatnot, so thank you very much. That's all I have to say today, so thank you.

Male: Have you guys been involved in any Restore the Fourth movements?

Michael Douglass: Restore the which?

Male: The Fourth, Restore the Fourth.

Michael Douglass: Ron, have we been involved in any Restore the Fourth movements?

Ron Yokubaitis: I couldn't hear the question. I'm sorry.

Michael Douglass: Have we been involved in any of the Restore the Fourth movements?

Ron Yokubaitis: Not me. I don't understand the movement, Store the Fourth?

Male: It's a movement to restore the Fourth Amendment.

Ron Yokubaitis: Oh, restore, sorry. Yes, absolutely, and we worked federally on the ECPA, but we were one of the groups that hired lobbyists to lobby the Texas legislature to pass Restore the Fourth that never technically existed for email and content on the internet in Texas. We can't speak for all kangaroos, but for all of you all, this is a freer state to be in. It's a much more libertarian state. We don't like the government.

Male: Anti-federalist?

Ron Yokubaitis: Well we think politicians, basically, are up to no good, if you give them much time to stay together and you give them much money, so we only let the legislature meet every two years for 120, 140 days, and don't give them much tax money. I was a Peace Corps volunteer 40-something years ago, and people are just aghast that we don't. It's so important. We let our state legislature meet all the time. They just conspire against you, take your money and use it against you, so at least we can get some necessary business done than we did the last time.

I'm saying both parties here. In Texas, both parties talk to each other, and you work out stuff for the common good. When we go to Washington, its the crips and the bloods. Here, I'm happy to say you're freer here in this state than over in one of your more enlightened states. There's not a bunch of yayhoos down here in our flat desert with no trees as you see.

No, it's essential. The Fourth Amendment is key. The war on drugs has been the biggest boondoggle for carving the Fourth Amendment to where it's hard to hear. Of course, now pedophilia has been the new stalking horse to take our stuff away. It's one of the exceptions in the Patriot Act, that they cannot have a warrant if they mumble the magic words, pedophilia, pedophilia.

I'm not saying there's not a problem because we see it. I asked too long... yes, we've worked on it. It's all of us. You've got to say no, mostly. You're an operator, and I'll set it up there, and you've got to learn to say no. It's the most important word to stay free is, no, I'm not going to do that. You show me why I have to do it. Make them show rather than assume you've got to do stuff.

That's too long an answer. I'm hogging. I'd like to pass the microphone to you all. I couldn't hear your question. Mike, can you do that?

Michael Douglass: Yeah, questions.

Male: I have a quick comment. The thing about every two years Texas legislature meets, the reason I support the legislature and I got so tired when I couldn't be in that building anymore. The one little bit of humor is the reason that they meet every two years instead of every year is the tanks can't get across Texas on a horse to get to the capitol. So we can't get from El Paso to Austin every year. It's too much of a pain.

Ron Yokubaitis: Well we don't pay them anything. They have to have separate reservations. We don't want them to be professional politicians. We want them to be more citizen politicians.

Male: I do value what you said. I don't want to downplay that. I just thought that little piece of trivia...

Ron Yokubaitis: Well our family ranches the country almost to El Paso, and it's not that hard to get off in El Paso. We're about 250 miles this side of El Paso, but once you get past West Austin, it's just all ...

Male: I've heard Sierra Blanca, he hates coming to the capital.

Ron Yokubaitis: He just loves Sierra Blanca and nothing. He didn't say that - Road stops and drugs.

Male: Recently I did some research on VPNs and stuff for my own purposes. What is your guys' response to the VPN providers that don't keep logs, so, therefore, as you receive subpoenas or whatever you get from the government, you must comply, that's understandable, but a lot of VPN providers now are not keeping blogs at all.

Michael Douglass: I think we just did a piece on this. Did we not?

Michael Douglass: Or have we not released that yet?

Michael Douglass: We have a piece coming out about the myths of VPN provider, and we have factual proof of this, that it's a lie. It's just a lie. There's a provider. I believe it's HideMyAss who, "I don't keep logs. I help hide your ass." Pardon my French. That didn't work out for a guy who the cops actually came and hauled off, so we don't believe them. That's our response.

Austin Green: It's also doesn't account for people that use 3rd party hosting solutions because a VPN provider, they not keep logs because of the hosting provider they are being stored on...

Ron Yokubaitis: That's a very good discussion. We drafted what we call the seven myths, and that's one of them. Don't keep logs. You listen to their marketing or some affiliate marketing site, famous though it may be, are getting paid for referring business to the people they're evaluating. What they're doing is they have to keep logs. If you're renting somebody else's service, they're keeping logs. You don't keep any logs, but you go to the hoster and get whatever you want. Then you look in their terms of service. You'll see - we logged the IP address. We make a record of your IP address you signed up from, when you connected, how many bytes you passed through, when you disconnected. Well that's all we logged, so we need it, and we log it for 30 days

because we need to go back and service the customer that's having trouble. We have customers in 170 countries, so our tech support's got to see what it is from what ISP and country, so you've got to have something.

Those routers are all throwing flow stats wherever they are. It's just a question of what you store and how long you store it. But if you want to fix your router, you need to know what's happening, and you've got to record some logs. The no logging is "hi I'm from the government" one of the three great lies. One of them is "hi from the government, I'm here to help you" - but no logs is another big one. We see it pegged around, and we can't say that we do log. That's what we log. We log when you connect, from the IP you connect, what you transfer because we calculated....

Michael Douglass: Bytes, byte count.

Male: So how do you troubleshoot not having logs?

Michael Douglass: Exactly. Some of this... I did say in my presentation, which is what happens when I stop looking at my notes. With Cyphr, one of the things, and I think this will bring true to Scott McCollough is we are taking a very, very serious approach at programming from the metadata perspective. Every interaction inside Cyphr, we are looking at what data, what content, how that content's encrypted and what metadata do we know about that content. Where do we know that metadata? Is there stuff that we know about during transmission that we don't know after transmission? And document it and being very vigilant at keeping that minimized. If there's a decision that we make that is going to increase the metadata, we take that decisions very seriously because well we have worked with Scott for a couple decades now and you can't underestimate the power of the metadata.

Male: Let me understand this. Both two parties want to communicate securely. First of all, I think both ends are going to have to [inaudible 00:40:44] because you can't trust anything you can't see the source from, so they're probably going to get it from a Linux distribution. They're going to communicate over some communication channel, and they're going to negotiate a symmetric-key, and from that point on, it's going to be encrypted, right? After the communication is done, the symmetric-key is going to be destroyed so nobody can come after asking questions later. Where do you come in to this? What do we need you for?

Michael Douglass: What do you need us for? That is actually why I had the slide in there and part of Chris's discussion from the video snippet is making it easy to use. Are we going to go to our mothers and grandmothers and fathers and grandfathers and say, I want you to go install Linux and open this PGP. I want you to set up a key so we can communicate securely and privately. It's hard. Where we come in is saying, it's time. As other people are saying too, it's time to make it not hard to do.

Female: The reality is that it never should have been hard to begin with. When it comes down to using PGP, it's very easy to add on just a little bit of user interface to make key management easy. Then there's almost no email application that will actually integrate it. There's almost no application that will actually let you run your email through an encryption layer before you send it off to somebody else. I'm able to use it because I'm actually willing to get down and use Mutt. And there's maybe a small fraction of people in this room.

There's no way I will ever get my friends to get encryption, at least with the way email clients currently handle it. And for that matter, most of them have gone to Gmail where it's impossible, and I'm not even going to try. They've already given everything away. They can't encrypt it, and I'm not even going to pretend that they could do otherwise. The whole point is it's got to become easy, or it's just not going to happen ever. It doesn't matter how important it is or how dangerous it is to have everything you're communicating just going out into the wild for everyone to look at. It's not going to get encrypted unless it's easy.

Male: Wait a second. Gmail has that IMAP server, and they have STMP servers, so if you send them a message

encrypted with PCP, it'll go through like grease through a goose. They won't be able to see what's in there.

Female: I would wager that less than 1 percent of all people on the internet are willing to go to the effort of setting up an IMAP client when the Gmail webmail is available right there.

Female: Okay, you're right.

Male: Open source software is bein shunned by recent events, but open source software is no more or less capable at secure encryption than closed source software. Open source software has 5 various..

Male: Wait a second. Closed source software cannot be secure. There may be difficulties with open source.

Female: Apparently, open source software can't be secured either.

Male: If it's close source, it absolutely cannot be secure, so the only chance you have is open source software. Maybe you'll fail. Maybe you won't be secure, but you will not be fair. You will not succeed with close source. There's absolutely no way. It's purely impossible.

Philip Molter: So the issue on the closed source versus the open source software is one of trust and auditability. Closed source software can be auditable. Companies go through audits all the time. Open source software has the benefit that if anybody wants to perform an audit on it, they have the capability of doing so. Closed source software can be audited as well. The important part of the whole discussion is not whether open source software can or cannot be secure or closed source software can or cannot be secure, it's one of trust. People have blindly put their trust in open source software.

When I say people, I mean Golden Frog as well. Golden Frog uses open SSL technology, and parts of our infrastructure were burned by the CCS injection bug as well. The fact is, we trust that software to be secure, and when it's not, we are as bitten as anybody who's using closed source software who trusted closed source software was secure. You get down to the point of trust. At some layer there's going to be trust. You asked where Golden Frog comes into it. Golden Frog wants to position itself as a trusted software platform and as a trusted network security platform, certainly more trusted than the other options that are out there.

We had an option abut logs earlier and no-log VPNs. It comes back to that question of trust and being able to trust in your vendor. When people are making extreme statements like, we don't do any logging at all, you're anonymous when you use our servers. When you're making statements that border or actually are physically impossible in the sense of how the internet operates today, you undermine that trust not just for the specific companies themselves but of the entire industry. If I come out to you and I say, we're using open source software. Therefore, you can trust everything that we do, and then at the same time I'm saying, we have to patch all of our servers for the Heartbleed bug, I'm not accurately representing what our capabilities are for giving our service to you.

I want to address open source versus closed source. It's really a question of trust. If you trust open source software more than closed source software, fantastic, we do. We use a lot of open source software in our stacks. For all of our encryption stuff, we're using open source software. But at the level of one being better than the other, really it's about who you trust, and Golden Frog wants to position itself as the company, that it can be trusted.

Michael Douglass: Two things. One, neither of them are related.This is Phillip Molter my fellow co-CTO is handling all the operations side of Golden Frog, and in further response reopens to the closed source. I don't know, but a lot of it they didn't

show us exactly what they were running, but they sure seemed to be somebody that, in the end, was trustworthy. He shattered his company to protect the privacy of his customers, so I think the argument is... yeah. It's not a differentiator.

Male: I have a comment more than a question. I don't think I have to convince anybody here about the problem of privacy, but if you have a problem discussing this with anybody, tell them to go to Epic.org and look up the Fusion Center button. In there you will find the information they've gathered about the Fusion Center and all the kinds of things that they are targeting. After you get this Walt Disney stuff, you will run across what they are saying are the goals of the Fusion Center. One of the goals of the Fusion Center is to regulate non-criminal conduct. I'd like everybody to think about that because that's what they do in North Korea. If you have any problem convincing somebody that Edward Snowden and the federal government ... Well, they're really not doing all of this stuff. Try looking at what the Fusion Center itself said about that.

Female: I just want to get back to a Golden Frog product you were talking about. You were talking about Cyphr, and you were saying that you want to use it for secure communications. Are you looking into video communications or just text? Because one of the issues that I see a lot is a lot of people who want to do work remotely and handle that, that they need to have it very secure, and there's nothing out there right now that handles that.

Michael Douglass: I will answer the question, but first that the South by Southwest video was funny because they make a comment about how they are using Google hangouts to have this conversation. Yes, so not initially out the door. That is something that we are setting our sights on doing. One of the things we do with our adjunct development is we do very rapid development. We release servers often. If you're a customer you probably knew that because your like, okay two weeks go by and we're sending you another email to you, so we're taking the same tact with Cyphr of saying, what's the bare minimum that we need to have a viable product, and let's do that. Then let's create that. Let's add the next feature. Let's build as we go, and video is one of the things we have talked about.

Male: This is not meant as an "I got you." Just coming back to the trust thing. Assuming I'm some regular citizen who's not very technical, why should I trust Golden Frog over anyone else, over Microsoft, if I have no concept of any of this stuff?

Michael Douglass: That's our job. That's our job, to convince you to trust us. You look at us as your virtual ISP. Why do we want to be your virtual ISP? Because we don't believe the ISPs you have are trustworthy. It is definitely one of the things. Part of this man's job here as PR is to get people to trust us, and I think it's through our actions. It's through what we do, the transparency that we provide. At the end of the day, it is still the word trust. There is that matter of you have to decide whether or not you want to trust us. It's coming from history, coming from our behaviors. I don't know if you want to add anything, Phil.

Male: Mark Wood has worked with us in the past. I think he's working with us now, right?

Male: Now part-time, yeah.

Philip Molter: Part-time. Mark is one of our software developers, very, very capable software developer. I was talking to him about PGP earlier. They still haven't figured out trust in PGP to perfect satisfaction. They've got nice systems in place that are mostly trustworthy, but one that people seem to have centered as the best solution is the web of trust, which is effectively that if I want to trust Mike, that he's who he says he is, there are five, 10 or 15 or 50 other people who have already trusted that Mike is who he says he is and then take that as the community word on it. Some of that is true for Golden Frog. We get out there, and we get people working with us. The more people come to trust Golden Frog and pass that on to friends, the more we become a trusted provider. Some of it is how we represent ourselves.

When you have people out there making outlandish claims about VPNs, or maybe not outlandish claims but conducting

themselves in certain ways, handing over customer information without a court warrant, going under, getting blocked by larger internet service providers because they're allowing malicious activity to come through the network because they don't want to put any controls on their network, and we want a responsible network. When we don't do those things, we become more trustworthy as a provider. We become more responsible for that, or those actions represent ourselves.

Ultimately, one of the things that we're going to be looking at is looking where, in the key areas of our company, we can have outside, independent people come in and audit us, audit our processes, audit our code, audit our systems and provide independent reports of what we do. Are we're doing what we say we're doing? If I say I only grab a very small subset of your information and I keep it for a very short amount of time and it's for this purpose, is that actually the case? Some outside company that specializes in this stuff that has a track record for doing this comes in, does the audit, and publishes an independent report that says everything. That helps to establish trust.

I don't know of any providers out there that operate with that kind of mindset, and that's the kind of mindset that we're approaching to it. It's not just that you take our word at it, but how can we start getting other people to prove that we're doing it this way. Getting back to open source software. Open source software makes it available so that anybody can go in and do that, but not everybody can go in and look at our logging stems. We're not going to let the world come in and look at our log systems, so how would I prove that I actually do what I say I do in our privacy policy? We're looking at those kinds of things right now.

When it came to TrueCypt, which is an open-source dislocation. What did they do? They went through a company called I-sec, crowd funded it. They went with a company called I-Sec, and they said audit our code. You find out if it's doing the right thing. Make sure nobody interjected anything bad in it because even though it's open source, no one's really validated that it works the right way. That's what they're doing with open SSL now. That's what we want to do with ourselves as a company. I think ultimately that's going to be the best that we establish that kind of trust, to be able to say you can trust us. It's going to be, here, these other people say so. It's not just word of mouth, but its actual companies that are trained in doing this stuff and are independent from us.

Michael Douglass: I think that's such an important distinction. Even though open ended software should be free, and we place trust in these products. Is it really open to where everybody can invest in it? Can all your family go in and look at the source code and see, I trust this. I see they are doing all the right things.

Philip Molter: Trust is not an absolute. It's not like I'm 100 percent trusted or I'm 0 percent trusted. Trust is a sliding scale. Even if someone went in and said all the algorithms are operating properly. All the code's written properly. All the logarithms are written properly. Underlying all of the encryption that we use to protect people's data or to store our information securely, underlying all of that mathematical algorithms that have not been absolutely verifiably proven to be unbreakable. In fact, as processing power improves and as mathematical proofs are done, some of these algorithms are found not to be. Until we get to that point, nobody's going to be able to say with 100 percent certainty that everything is safe, but we put our faith is certain people with certain reports, with certain analysis and certain software, and that's about the best that we can do as a company. Externally, we want to be able to provide external relationships that you guys can make your own decisions on that are independent from just the words of our excellent, excellent working staff.

Male: As far as you as a service provider, if you a warrant, what are your obligations? Are all the warrants the same, like, give us the data? What are you allowed to tell the customer about that?

Michael Douglass: Right, that's a big question. I wish Ron hadn't left the room, so Phillip can probably answer that.

Philip Molter: I actually service most of the legal requests that come in for Golden Frog customer data. I wouldn't say

it's a large amount, but first off, every request that comes in is going to be reviewed by a lawyer first, usually on house counsel. If it's particularly problematic, we'll go to external counsel. It depends on the kind of request that comes in. On a civil lawsuit, we're going to have to be ordered by a court of competent jurisdiction to provide that information. Competent jurisdiction is going to depend heavily on the attributed information being requested, where the customer resides, where the case has been filed, what sort of actions are being taken. So it's hard to say that there's a one answer on that stuff, but there's a general rule.

In court competent jurisdiction, ordered by the court, the customer has the right to be notified about the information. They will be notified about the information disclosure, including what information is being disclosed, and we give them a chance to challenge that disclosure in the court of law that it's requested. Because we're a worldwide operator, things are a little muggy in terms of exactly what you have to do, but the vast majority of our requests come from the United States, so in the United States, that's the drill.

Civil requests are generally not the kinds of requests we get. Most of them are going to be coming from actual law enforcement agencies. First thing, we make sure that they're going through the process of dotting their I's and crossing their T's and everything, make sure they sent it to the right company. They have to get an actual warrant or court order subpoena to get access to the information. It has to be for the right company. If it's too broad, we challenge them on it.

Ron was talking about the Fourth Amendment. The first thing you've got to do is you've got to say no. If the information request looks too broad, the information request is incomplete or the information request is not an information request but it's a request to do something that's not going to result in the retrieval of customer information, our answer is going to be no on that until the court shows us the court write says that says we have to.

Really, it doesn't ever reach that point. Law enforcement is looking for certain information. They will get to the point where they either get that information or not, the specific information that they're looking for. Once they have a proper warrant or court subpoena in place, again, this comes back to court competent jurisdiction stuff. Ron's a little bit better on that stuff than I am.

Once lawyers determine that this is a valid request, we have to provide the information, it's done appropriately, it is an appropriate request, we have very little information to give, but we will hand that information over. If the court orders that we are not allowed to disclose that information, we are not allowed to disclose that information so that it doesn't threaten an ongoing investigation. If we are allowed to disclose it, we will disclose the fact that we're disclosing it to the customer. Again, it's on a very, very case by case basis, depending on the nature of the request. Most of the times what they're looking for is they're looking for subscriber information on who used a connection at a particular point in time, and law enforcement doesn't move fast, so most of the times their request can't be serviced. Does that answer your question?

Male: Yeah, for the most part. I was just wondering if you're allowed to tell your customer, and then does that give them time to remove the data?

Philip Molter: In a civil case. Absolutely, in this country we are. Again, internationally, we haven't run into a situation where we've gotten a civil subpoena, so I can't answer that. I don't know. We would make every case for actually disclosing that on the criminal kind. It just depends on the request being made. We will always fight to be able to disclose it to our customer, but in some cases, the laws have already been set about how it works.

Michael Douglass: Thank you for joining us. We definitely appreciate you coming out here. Thank you.