2013-04-04_schneier

[0:00:00]

Speaker1: You are listening to the Berkman Audio Fishbowl from the Berkman Center for Internet and Society at Harvard University. Each of these conversations with leading Cyber scholars, entrepreneurs, activists, and the policy makers as they explore the leading edge in the Internet & Technology to mark a safe law in society. For more information on the Berkman Center and for more programs like this visit www.cyber.law.harvard.edu.

Jonathan Zittrain**:** Well, good evening. Oh, is that loud?

Bruce Schneier: There are official people here who are in charge of volume.

Jonathan Zittrain: **[Laughter 00:00:38]** There it is. There is the volume and there is another person in charge of quality. So we have both things covered. Okay, then. My name is Jonathan Zittrain and I am so pleased to be in conversation tonight with Bruce Schneier. Bruce is kind of a really good person to introduce in the sense that he is extremely well known but not for trait reasons. **[Laughter 00:01:00]** It is actually hard to put a bumper sticker on Bruce. Not simply because he is security conscious. I think the closest thing would be, he is extremely well known for his attitudes and common sense around TSA. I believe that you actually coined the phrase "Security Theater".

Bruce Schneier: "Security Theater" is mine.

Jonathan Zittrain: That is a great phrase. You can't help but enjoy every episode of "Security Theater" encountering now **[Laughter 00:01:32]** on the way and it has also been really interesting to see Bruce's evolution from somebody writing economical text and applied cryptography, kind of has the technical chops then really thinking more systemically including human factors about security and again in his explanations being lucid but not reducing in ways that make good guys and bad guys and sort of simplistic slogans and yet still again popular enough that I believe that you are an internet name, are you not?

Bruce Schneier: Hardly enough, yes.

Jonathan Zittrain: There is an internet name about, look up Bruce Schneier.

Bruce Schneier: Bruce Schneier Facts, I have nothing to do with him.

Jonathan Zittrain: Exactly.

Bruce Schneier: Or just not now.

Jonathan Zittrain **:** **[Laughter 00:02:14]** Now it is too late.

Bruce Schneier: Do you guys put these rooms in Faraday Cage?

Jonathan Zittrain : That would be an MIT thing to do.

Bruce Schneier: Oh, okay.

Jonathan Zittrain : Yet not, because then they would hack the Faraday Cage but we just rely on law to keep people honest and it doesn't work. **[Laughter 00:02:30]** So that is a deeper problem than the ones' we are going to probably talk about tonight. The last time Bruce and I shared a stage, I believe it was 2010 and it was for the "Intelligence Squared Debate" resolved the "Cyber War Threat has been gravely exaggerated".

Bruce Schneier: Grossly exaggerated.

Jonathan Zittrain : Grossly exaggerated.

Bruce Schneier: It was kind of interesting. It was I and Mark Rotenberg on one side. We were the side that said, "Yes, it is grossly exaggerated". On the other side was Mike McConnell who used to run the NSA now a big exec at **[Inaudible 00:03:05]**. One of the people who grossly exaggerates Cyber War for a living **[Laughter 00:03:09]** and you.

Jonathan Zittrain : It seems only fitting to be on that side of the debate.

Bruce Schneier: I actually thought it was pretty easy to present a list of gross exaggerations, we'd all vote and then we'd go home. It was more complicated. I actually lost that debate. It really surprised me. But at the end of the hour and a half or something and the vote was they polled the audience in the beginning and polled the audience in the end. So you could think about how to gain the system. Let us assume people didn't. But more people are convinced that Cyber War was a real threat then was grossly exaggerated. It really was thinking about that loss that really

got me to understand the Cyber War debate. Now why I lost? Lot of it was definitional. We spent most of the time arguing on the definition of Cyber War. I think that is in a lot of ways is the policy problems is in today that we don't know when Cyber War starts, when it ends, what it looks like when it is going on. It is not just the debaters or researchers. It is, you know the policy people who don't have good definitions. So it is real hard to discuss whether the threat is exaggerated because you know what the is, is. I am not going in a little bit. It used to be in the real world you would judge the threat by the weaponry. When you saw a tank driving at you, you knew it was war because only Governments could afford tanks. The problem in Cyber Space is everyone is using the same weaponry.

[0:05:00]

Everyone is using DDoS attacks. Everyone is using Exploits. Everyone is using Exfiltration. They are all doing the same thing. You can't look at the weaponry or you can't look at the tactics and figure out who you are fighting. This is a problem because when you are being attacked in Cyberspace you are being attacked in general. There are a lot of people you can call. You can call the police, you can call the military, you can call home land security, you can call your lawyers, I guess we are here, right. The regime in which your defense operates depends on exactly 2 things – Who is attacking you? And Why? When you are attacked in Cyberspace the exact 2 things you don't know are who is attacking you and why. So we are seeing the military use a very expansive definition because they want to capture the whole gamut of the attacks where I argue very strongly for a much narrower definition. That is why I lost that debate. You never heard that. You think because you debated better than I did?

Jonathan Zittrain : No.

Bruce Schneier: In fact you didn't.

Jonathan Zittrain : I was hot. **[Laughter 00:06:12]** I was going to say that you lost because we hacked the vote **[Laughter 00:06:15]** whereby proving our side.

Bruce Schneier: More of McConnell's friends were in the audience. That is in the question, they voted no in the start. I assume that they played fair.

Jonathan Zittrain : Indeed. Well, this isn't a debate in the sense that we often I think share more views than we disagree upon. It is also not a debate in the sense that I think we are wanting to structure this conversation and the one we

will put out to the entire room before too long as thinking aloud more than advancing some particular view and asking people to hammer upon it. This really is, especially given the collective brain trust I already see in this room. This is like a group study exercise more than it is a delivery of an academic paper or a thesis that we are then supposed to be up upon. By way of framing though I think it is interesting first just from the remarks that you were getting into substance, tolerance. You already hear using words like weapon. Which already seems to me to be conceding a big part of the frame of the debate something that you see at the likes of the Anonymous I think ironically deploy when they talk about the low orbit ion cannon which is I think is life imitating art, art imitating life because the low orbit ion cannon is itself not a real cannon. I think also I hope we will get a chance to talk about what I perceive that there is a trajectory in your own thinking from the beyond fear phase which captured a lot of your thinking about, look it is complicated, it is not like there aren't real threats, but we are often focused on exactly the wrong stuff to our detriment and so let's get beyond fear. So what I think is shaping up to be maybe your next book which you haven't named it yet but at the best I can tell the title might be "Be afraid. Be very afraid." **[Laughter 00:08:15]** and it is about asymmetric threats very generally from technology, not even limited to cyber. Again, I am characterizing this because feel free to correct my characterization any moment but I know you have a lot of worries about the asymmetries between off-ends and deep-ends and the prospect that as time goes on our normal ways of handling things and including normal is how reasonable technically oriented people would handle them may fall short and thereby leave us with a real dilemma about how to secure ourselves. That is the least I think where you are at on the current puzzle. So we can start there with that or start at the beginning and work forward?

Bruce Schneier: That is a good piece of it. It is a small piece but it is something I've been wondering about for a while and I wrote it down. Some of the comments that I got was, "Wow! You must have had a really bad day". Very generally we accept a certain amount of bad actions society. The price of freedom is the possibility of crime. We recognize that. That in order to be a free society we deliberately limit what the police can do. We do a bunch of things to make crime possible and there is a crime rate that we accept. The murder rate is not 0 and we wouldn't want it to be 0. There are a whole lot of reasons why that would be bad. We have some natural

Jonathan Zittrain : We might want it to be 0 but we realize that what would take to make it so it is not what the society wants.

Bruce Schneier: We want to be all facts, right? There are too many false arrests. There are a whole lot of reasons why we wouldn't want that. If you think about this, the amount of damage a bad actor can do is vaguely a function of technology.

[0:10:00]

The terrorists can kill 'X' people that as a function of technology 1, 10, 100, or 1000 as the weaponry gets better. A bank robber they can steal more money or steal more accounts. As the amount of damage an individual bad actor can do increases the fewer bad actors we will tolerate. It is assuming that effect is constant. We want a murder rate of 'X'. The murderers murder 10 times many people as before then we want 1/10th of them to keep that number. This is very **[Inaudible 00:10:34]** way. **[Laughter 00:10:34]**

Jonathan Zittrain : This is just in, Bruce will never be running for elective office, ever. **[Laughter 00:10:40]**

Bruce Schneier: Oh, God no.

Jonathan Zittrain : In fact, appointed office is now seriously in question. **[Laughter 00:10:44]**

Bruce Schneier: A whole lot of reasons for that.

Jonathan Zittrain : It will be legalized soon.

Bruce Schneier: As the amount of **[Laughter 00:10:53]** as the amount of damage increases the number of bad actors we want to tolerate decreases. In theory you can imagine to get to the point where even one is bad, even one is too much. This is the weapons of mass destruction debate. The terrorists can do so much freaking damage that we must rewrite every, all of our laws to make sure we catch them before they do their bad thing. No more after the fact the action response that works for murder and lot of other crimes. This must be predictive, police saying this must be arresting people on conspiracy. All of those reasons why you have these very invasive investigative tools.

Jonathan Zittrain : Which is to say what used to be a spectrum on a dial of enforcement to try to scale to the nature of the problem becomes a binary choice between doom from terrorists or doom from police state.

Bruce Schneier: Kind of. My worry is now.

Jonathan Zittrain : Doing my best on the bumper sticker.

Bruce Schneier: That is good. **[Laughter 00:11:56]**, and eventually I will do a bumper section. I like them too. Eventually you get to the point where technology becomes so great and I am wanting this like a general rule of civilization that can apply around the galaxy. If there comes a point in any species technological advancement where the amount of damage one lone actor can do is so devastating that it destroys society. If that is the case and I am partialating that destroying is easier than preventing destruction. There will be a window in technological advancements where one lone actor or a group of actors can destroy a society.

So now what is the chance that such a society can get beyond that? I am not sure I am optimistic about the chances. It is, we tend to run a pretty wide cover around our species. So that is in general the worry. Now what is that need? I am not sure. Is it true? A lot of things I wrote to see if people can refute that. Well, maybe unless arguing. Last book I spent a whole chapter arguing on this notion that the attackers have an inherited advantage because they are first movers and they can react quicker.

Let us give an example. Someone invents a motor car and the police say, “What a great idea” and they have a committee to study the use of a car. They produce an RFP. They get bids. They buy a car. They have a training program if you got to use it. Meanwhile the bank robber says, “Oh, look a new getaway vehicle”. We saw this on the internet. Misuse of the internet. Peers use it and we suddenly have a new breed of cyber criminals like emerges organically and figures out how to commit crime in the internet. Meanwhile the police who have been too trained on Agatha Christie novels **[Laughter 00:14:02]** took them like 10 years to figure out how to defend. I will argue in general there will be this temporal gap as society increases, I mean as technology increases where the bad actors, the lone actors, the fringe actors are more agile.

Jonathan Zittrain : It is interesting though your story is basically good cops and bad robbers are on a similar baseline and then the robbers adopt enabling technology

sooner. It may also be a little bit the good cops or just cops are very well resourced and use that to have an advantage so they might not have unsure numbers but use the technology to leverage it. I can listen in on a conversation that you can't and then the technology has a democratizing effect that levels the playing field but makes it so that the cops no longer will have the multiplayer they were allowed.

[0:15:00]

Bruce Schneier: I may have other thoughts where we are seeing power used technologies to effects that we didn't imagine before and there are exceptions. Finger print technology is an easy exception. This is the technology that benefited the police and didn't benefit the criminals at all. Or really the thing that advanced policing most probably in the last 1000 years is invention of the radio. That fundamentally changed the way that police work. No longer is the policeman lone actor in the community. He was able to radio for backup and that just changed everything. You can argue that and I think it is also true while the fringe actors are more nimble, the state actors, the powerful actors have a greater multiplier. They can make use of technology not faster but once they figure it out it is a greater effect. We are seeing that now in the Government of Syria using Face Book to spy on people or using internet technologies for surveillance whereas 5 years ago the only people using them effectively were the dissidents. Now it is not clear where the new balance is.

Jonathan Zittrain: Well, so I want to just look back a little bit as we go because we can put a few ideas on the table and then have a larger conversation. So one idea on the table is what I kind of called "Be very afraid" another way of describing the asymmetry between offense and defense.

Bruce Schneier: I am an inherent optimist so it is weird to just sort of have this dystopian essay under my belt.

Jonathan Zittrain: Well especially because it is not just dystopian it runs in a very different flow from a lot of your other works such as your work on "Digital Feudalism" there is a loaded term for you, in which you worry a lot about centralization of certain technological functionalities either with private actors, the Googles, and Apples and whoever of the world or public authorities, the Syrians of our world. That is the kind of thing for which it

is exactly those kind of folks that would want to do that and encourage the centralization that would benefit from fanning the fears of the first topic. If you want to be protected from these asymmetries come shelter your website under Amazon Web Services, come do your email through Gmail and let us filter your spam and **[Inaudible 00:17:37]**. By the way, I think Bruce and me maybe the only people in the room still using Eudora. Any other Eudora users? It wasn't a my email client is older than yours, it is a challenge. **[Laughter 00:17:51]** I knew they would be five users. I was just that, there is one moment in history where we both tend to.

Bruce Schneier: It is going to be sad but we have to give up. Eudora, there is nothing else like it.

Jonathan Zittrain: I keep clicking as many batter ads as possible just to keep it afloat **[Laughter 00:18:03]** but anyway there is a second cluster of thinking that you have recently is around this sort of digital fuse. I want to give you a little space to kind of map that out and say, "Welcome to the club" with people worrying about this.

Bruce Schneier: This does echo the stuff that was in your book which actually had to re-look at after forgetting it and re-remembering it.

Jonathan Zittrain: That is a blurb you are putting up there. **[Laughter 00:18:30]** the book is so nice I read it twice after I forgot it the first time. **[Laughter 00:18:32]**

Bruce Schneier: You are not that bad. **[Laughter 00:18:35]**

Jonathan Zittrain: The book or the blurb?

Bruce Schneier: The blurb. I have been thinking a lot about power and power asymmetry. I see increasingly where we are living in a computing world that I liken to feudalism and the idea being if you pledge your allegiance to Apple and give them your email and your calendar and your address book and your photographs your life is easy. They in turn, I guess they promise to protect you. You can pledge your allegiance to Google. Lot of us pledge some of our allegiance to Face Book, to Amazon. I mean all these companies that are increasingly controlling our data as we move them onto these platforms and controlling our end-user devices. The era of general purpose computing seems to be fading. Apple controls what is allowed to be on your IPHONE and IPAD. Amazon controls what can be in

your Kindle. Last year they forcibly removed the book. It happened in 1984 which was couldn't write that stuff. **[Laughter 00:19:53]**

Jonathan Zittrain: You couldn't write that stuff. **[Laughter 00:19:56]**

Bruce Schneier: I like the feudal metaphor because in a lot of ways we are pawns.

[0:20:02]

For example, I found this out recently that Google and Apple are 2 feudal lords fighting and what are the effects is I can run Google Maps on my IPHONE but not my IPAD. Google and Face Book are fighting and one of the effects is that Google readers disappear. These things are happening. These companies, they are protecting us but they are also selling us, they are using us. Feudalism is kind of half history and half gamatrons here. I really mean it as a metaphor and not an exact

Jonathan Zittrain: We are members of no house here.

Bruce Schneier: We are the peasantry. We are collateral damage. Dropping Google readers is collateral damage. In fact that I can't get the maps on my IPAD is collateral damage. If you read about historical feudalism it ended with the rise of the nation states. Things like the Magna Carta. What basically happened is a larger Government said to the feudal lords, "Look you have all of these rights, you now have to have responsibilities. That having just one is fun for you guys but no fun for everybody else". I want that metaphor to guide what we need to do on the internet.

Jonathan Zittrain: So what is the piece of West Failure?

Bruce Schneier: I am not that detailed. What I think we need.

Jonathan Zittrain: One second, the next book is "West Failure" it is not "Just for Ham"

Bruce Schneier: Yeah, I know. But nobody would buy that.

Jonathan Zittrain: Or the people would buy expecting something very different.

Bruce Schneier: I think we need to recognize that these corporations are de-facto states

Jonathan Zittrain: Which now sounds like Mark Zuckerburg on atleast that one day he woke up and decided that was an interesting thing to say. I don't know how much he stands behind it.

Bruce Schneier: I know but I want to regulate him. He is not going to like where I am going. That we need to rein them in. on the internet there is no such thing as a public space or privately owned but we treat these spaces as public. We treat these as infrastructure not as corporations. It is more obscured by the fact that the basic market model which is I buy something, you sell it to me and we have this capitalistic chains that really is the base of the system fails because we are not customers of these things we use. We are users, we are product reviewers and you got to call us. So a lot of this is obscured.

Jonathan Zittrain: So we are laying down our markers here. As we are laying down these markers roughly by your label on the round of digital feudalism let me just mention the kinds of push back that come to this kind of argument that I am well familiar with since I **[Laughter 00:23:27]** argued similar things without the same terminology in my words.

Bruce Schneier: It is the bumper sticker.

Jonathan Zittrain: It is. It is also from a futilism. So it has a nice double **[Inaudible 00:23:41]** going on which appear in almost any book cover don't blame me. But the push back includes I will channel folks like the **[Inaudible 00:23:50]** Center or name your favorite libertarian. The first objection to that is, give me a break you are a communist or you can pass that. Second is, we have more technological affordances today than we had yesterday, than we had last year. Isn't most of your worry front loaded to some future that hasn't atleast arrived yet. So there is a quality of "Chicken Little" because I know I can't get Google Maps on my incredible IPAD Mini that didn't exist three years ago talk about the glass being one-millionth.

Bruce Schneier: It is a lot more than that. We know that Google collects this data. I am worried a lot about Government-Corporate interaction. We know that Google collects this data and we know that the Government asks them for it. I read an article, I mean talking about the crazy libertarians about Gun Control.

Jonathan Zittrain: You said crazy?

Bruce Schneier: I will say it again and I will definitely prove it if I have to. The reason we oppose registering Gun Owners is because there will be list of Gun Owners which Government will use to confiscate guns.

[0:25:05]

That is the argument. I am really thinking, why does the Government need to get a list. Why don't they just ask Google? Why don't they ask **[Inaudible 00:25:12]**? I think we are seeing more. Remember when.

Jonathan Zittrain: How does Google know how many gun owners there are?

Bruce Schneier: I am sure in Googles' database, if you ask Google who owns guns? I am sure they will give you decent list.

Jonathan Zittrain: Really!

Bruce Schneier: Based on searched terms, based on topics discussed, based on purchasing history. It depends who you ask. The question is, if not now when will it happen? I bet soon. When will the corporates fear just in the data that they are collecting about our actions have that list. We know that the TSA when they were trying to do, it was "Secure Flight" it was called in '05 and '06. They wanted to use corporate data to differentially screen passengers. They recognized that the data that we are willingly giving these companies they could use for differential law enforcement in this case. I wonder if the era of the Government needs to know data from us is ending. I can imagine the IRS saying, "How to figure out who to audit? We are going to go to a credit bureau. We are going to ask them to run a differential base of what they think your income is, what you said your income is and we are going to audit people who mismatch"

Jonathan Zittrain: This is a good idea or a bad idea?

Bruce Schneier: It might be an effective idea but I don't think it is a good idea. It is an idea that we should discuss the possibility of before they go decide to do it without telling us. So getting to sort of the question that if things are looking really good why are we worried? We are at a point, and lot of that is the opt out answer. You don't like it don't do it. But I know that is not really possible. We can't not have a credit card. We actually really can't not have a cell phone.

Jonathan Zittrain: Can you not have an IPAD?

Bruce Schneier: You could not have an IPAD. But your choices are few and if the two choices don't compete on the future you are pissed about you are stuck. When you can't fly more secure airways that run background check on everybody or a less secure airways that hand you a knife when you get on

board. **[Laughter 00:27:27]** you don't have that ability. All cell phone plans are.

Jonathan Zittrain: The market has not spoken. **[Laughter 00:27:34]**

Bruce Schneier: Or atleast the few sellers in the market have decided not to speak on that issue.

Jonathan Zittrain: It might just be some one time flyers.

Bruce Schneier: There isn't a Face Book that won't collect your data.

Jonathan Zittrain: Which is an interesting puzzle by the way. Why? I don't know, maybe we must just do a quick market test although there is obviously selection buyers who have chose to come tonight but how many people would be, how many people are Face Book users? But the record shows there is a lot. How many people are a little queasy about Face Book? The record shows more. **[Laughter 00:28:10]** How many people will be okay with paying $5 a month and in exchange Face Book will do zip with any data it collects, it expunges it has and it offers you 6 bucks. We are going to run an auction now? **[Laughter 00:28:29]** Just 5 bucks. How many people pay 5? I will say maybe 20% of the hands went up.

Bruce Schneier: Because you asked the question wrong. The question is, how many of you are willing to pay 5 bucks to be a non-user of Face Book when all of your other friends are on Face Book? That is the problem. It is the network effect. You are not on Face Book, you don't get invited to parties, you don't get dates, and you don't get **[Cross-Talk 00:28:56]**

Jonathan Zittrain: These folks are all on Face Book and they are not wanting to pay the 5 bucks. Whether they are on it because they feel they have to be on it or they are on it because they like it. Either way they are not willing to pay the 5 bucks for the most part.

Bruce Schneier: Some are and some aren't. The problem is and they probably have it in a lot of these systems is they are creeks. We are on Face Book, I happen not to be but I am the Eudora using freak.

Jonathan Zittrain: Wait, who am I friends with then? They are all like you? **[Laughter 00:29:19]**

Bruce Schneier: Honestly I get **[Cross-Talk 00:29:20]**

Jonathan Zittrain: It turned out to be Chuck Norris.

Bruce Schneier: I get email from people thanking me for finding them on Twitter and I am not Twitter. I don't know who you are friends with. **[Laughter 00:29:29]**

Jonathan Zittrain: This does seem poor security, doesn't it? With all the spoofing.

Bruce Schneier: It is only so much I can do.

Jonathan Zittrain: But now this leads to the other I think the main objection although we may hear more shortly. On this rife of Mark doesn't like what I have to say because I say, "I want to regulate them". A big part of your objection to these loci of concentrations of data is that it is very easy for the Government to get it and yet here you are saying let's have the Government come in and regulate these guys.

[0:30:00]

When is the last time the Government came in, in this space and did something you thought to improve the situation.

Bruce Schneier: In this space, you have to take a long term view. This is the only.

Jonathan Zittrain: We shouldn't tell the senators to get a bill about the internet until the very end. **[Laughter 00:30:18]**

Bruce Schneier: Longer term. This is the quote that lets me survive in this world is, Martin Luther King, "The arc of history is long but it bends towards justice". Might be a 100 years ago half of us in this room couldn't vote. 200 years ago a bunch of us were slaves. I mean in the long term assuming my dystopian vision doesn't happen, Governments will do the right thing.

Jonathan Zittrain: How long do we have to wait to do the Face Book regulation you want to do?

Bruce Schneier: You might have to wait 20 years. You might have to wait a generation. You might have to wait 2 decades.

Jonathan Zittrain: We haven't regulated any friends yet but it is like just coupon and lets' see how this thing shapes up.

Bruce Schneier: Short term I was actually very pessimistic but I don't think Government can pass a good law at this point.

Jonathan Zittrain: So you are about to testify Mr. Schneier, "Should we get into the business of protecting the defenseless American public from these economic engines that are called Face Book and Google and everything? Should we get into this or should we just keep on walking for 20 years? What is your answer?"

Bruce Schneier: You guys, you money grubbing senatorial morons, you shouldn't do anything.

Jonathan Zittrain: Definitely not conformable. **[Laughter 00:31:27]**

Bruce Schneier: We are living in a world where there is a very dysfunctional Government and this is another one of my threats that power is now using itself to increase power. So, while in the near term I have actually no hope for, I think the update on the Computer Forum on Abuse Act would be a disaster because I can't imagine them making it better. I love them to make it better but I can't imagine it happening. I am terrified they will forget their **[Cross-Talk 00:31:56]**.

Jonathan Zittrain: That is okay. I just want to pin you down for a moment here.

Bruce Schneier: I am slippery.

Jonathan Zittrain: I know it. So you have a feel radical answer that says, "There ought to be some regulatory muscle that could be but not always is flexed. That answers is just something other than a market. That answer is to a quality that deals with certain market failures you've identified but in the real world atleast for the next 19 ½ years or it is going to kick in the wrong direction. In which case what should we do right now?

Bruce Schneier: I don't know. I don't know if there is an answer. In a lot of ways, well you are screwed. What do we do? What do we do in the face off a Government, a US Government that doesn't even follow its own law with respect to data collection, data retention, and data use? That carves exceptions into its laws. We have learnt recently that the FBI has been for the past, over the decade running fake cell towers for surveillance almost certainly against law. It says eves dropping. We are pretty sure that the DHS has collected the financial records of everybody under the National Security Letter. These things that are happening are sends pretty abhorrent. On the other hand, all we can do is keep up, keep fighting. Last week, a few people I have talked two of them one is Glenn

Greenwald. He wrote a really nice essay on Gay marriage. Where he said, it was one of the uplifting things I have read in years. He said, “Look at what has gone on. We have for years been fighting an issue that we had no hope of winning and in the space of 3 months what the hell happened, it all turned around. Whereas now it seems that winning is inevitable. Look, don’t give up”. Which was his moral. Which is more general, his moral was about that and Guantanamo and all the other things he argues about. I don’t know. I have to believe that sooner or later. We’ve got people working. Once Larry Lasik solves the money problem, I am in. so I am just counting on him to be like a month ahead with this issue. As long as that happens we are good.

Jonathan Zittrain: Internet??? Lasik profits. **[Laughter 00:34:38]** Somebody needs to alert him but this is progress. Now you mentioned Glenn Greenwald, that is not a bad segway because Glenn was one of the people who had been identified as an ally of sources.

Bruce Schneier: Conspirator. Ally.

Jonathan Zittrain: Wickedly into something and Anonymous in turn managed to hack HB Gary Federal, one of the “Be afraid. Be very afraid. Write us a cheque profit”. Question mark there.

[0:35:14]

Anonymous was able to completely own them, get all of their internal corporate email including PowerPoint texts where they made their sales pitches to the likes of Bank of America and where they proposed a dirty tricks campaign against Glenn Greenwald.

Bruce Schneier: They did yes.

Jonathan Zittrain: And other. I am just curious. I am curious, I know that you have thoughts about leaks and their value to society. But I am curious to really think about the function of something like Anonymous. It feels like a powerful entity that has the future of not being honest to traditional forces. That maybe not great but it is also not honest. What do you think about that?

Bruce Schneier: There is a lot to be said about that. About non-state actors. There is a lot to be said about their whole escapade. We are living in a world where a bunch of hackers can drop a company. A few months later, this made the

news less, Anonymous told NATO not to mess with it. We are living in a world where a bunch of guys can threaten NATO. That is kind of freaky.

Jonathan Zittrain: I find it interesting because they have also did it against North Korea that your time has come. **[Laughter 00:36:36]** I thought you were going to bring up that Anonymous had a war within itself. There was a moment, if you went to one of Anonymous's main pages. It said, "There is a guy who used to be us, who compromised our server. Until further notice don't visit our website anymore. You might get owned". At that point I was just like that the center cannot hold. I don't know who the falcon and the falconer is.

Bruce Schneier: Anonymous is like a lot of movements that are given. We as a species like organization so we tend to assume our enemy is organized. Reminds me the way that the Black Panthers were treated in the '60s, the way Al-Qaeda was treated 10 years ago. That we assumed that there was this organization with roles and higher **[Inaudible 00:37:27]** and armed chart. He drew a salary and got benefits. In all those cases it tends to be random people who pick up the banner and say, "I am AL-Qaeda. I am Anonymous. I am this." And maybe they are loosely connected, maybe they are ideologically connected, maybe they are just using the name. it is a lot more diffuse. So there really isn't an Anonymous. There are the people who today have done things and said, "Hey, look we are Anonymous".

Jonathan Zittrain: What is your thinking around that phenomenon?

Bruce Schneier: I think the rise of non-state actors is really interesting that they can do real damage. This will be called the next Cyber War but it is not. It is a bunch of guys. There is another thought that came out of my head. It was the non-state actors, it is their power not being tied to a population makes them much more random.

Jonathan Zittrain: I will just share some of my thinking about it. There is a paper that talks about an arrangement reached in the American Antebellum North and South between political elites about a very contentious issue at the time of return of fugitive slaves. The North agreed to return fugitive slaves in order to keep the larger peace. It turned out that the North couldn't deliver because there wasn't professionalized law enforcement the way there is today and in order to get pretty much anything done in the law

enforcement context like the return of fugitive slaves you has to convene a passé. Which is to say that as a citizenry you need to compel and the citizenry was going to be shampooing the cat that day. They were not interested in doing that. It was an interesting way of applying a template that perhaps subsists or persists only now in the tradition of the jury, where before you can just put somebody away until you get 12 citizens good and true than many and have them be the last ones to weigh in on this. That is less and less needed as enforcement becomes more push button we see it from anything ranging from You Tube take downs to surveillance, such that we don't need the passé anymore.

[0:40:00]

I am wondering is the rise of something like Anonymous and many counterparts. A reintroduction of actually having to get a good portion of the quality in line with something for it actually happened in the world or is it something else.

Bruce Schneier: I think that they are one of the first examples that we have seen of what civil disobedience looks like in the internet age, what it means to protest, what a sit-in looks like, what a picket line looks like.

Jonathan Zittrain: And you have a view by the way on DDoS? Is it sit-in and should it be treated as **[Inaudible 00:40:41]** or is it blocking information?

Bruce Schneier: Remember what I said in the beginning. It used to be, you can tell by the weaponry, now you can't. So DDoS is either it has been used for extortion. It tends to happen most on fringe industries offshore. Online gambling, online gaming, online porn. There is DDoS extortion. It is used for causing damage. It is used as protest. It is used because it scores out on reward. So it is used for all of those things. Actually there are cases, a few years ago the Victoria Secret website it went down not because of the DDoS attack but because of a lot of people wanting to see the pictures but you couldn't tell the difference.

Jonathan Zittrain: Not exactly. This is just in. **[Laughter 00:41:32]**

Bruce Schneier: But you can't tell the difference. If you are on the receiving end you can't tell the difference. So Anonymous largely I believe engaged in legitimate civil disobedience and should be treated that way. Less because of what they did and because of who they are and why they did it. This is hard. In the real world we tend to have not different laws but different

expectations around civil disobedience. So you know that you will get arrested and you will be thrown in jail and this is all part of what we do.

Jonathan Zittrain: but of course Anonymous if it is true to its name wants the impact of civil disobedience without the part of civil disobedience where you go to jail. All fairness going to jail for 40 years for something wasn't in the cards of counter sit-in.

Bruce Schneier: Right. Because in the US atleast we are and I think we are doing this because of corporate pressure classifying all of this as these horrible crimes against the internet and we are really exaggerating what these are. So I would also want to remain Anonymous too. We really don't have an agreement among all of us of what a valid protest is. It maybe defacing a website. It could easily be. Remember Green Peace, the way they throw a banner on a smoke stack that is the equivalent of defacing a website. You make a public statement that, or as a picket line you make a statement that says, "Those who are going to whatever it is you are protesting have to see, have to interact". But if you do it on the net you are a cyber criminal and you get really exaggerated sentence. There are a bunches of example.

Jonathan Zittrain: Those views are, I just want to go on this for one moment. If somebody manages online to disrupt things not just in an expressive kind of way, vandalism is almost the easiest case for online protesting, the graffiti kind of way but manages to do so on a way that PayPal or Master Card, not just the brochure front page but the actual functionality, the API is not working for a while and a bunch of commerce grinds to a halt. You are saying in your view the motive of such an attack is immaterial to you in wanting to figure out how to treat it?

Bruce Schneier: That feels in line with the way law works. We do look at motive, accidental homicide versus murder.

Jonathan Zittrain: Well, in this case it is intentional homicide but one was for a cause and the other was for money.

Bruce Schneier: Okay, I think motive actually does matter. I think it matters in all crimes. I have always wondered why you can be tried for murder of a year with these penalties whereas **[Inaudible 00:44:42]** with fewer penalties based on something as weird as how good your aim is. **[Laughter 00:44:48]** Makes no sense to me. It seems like that if that is what you wanted to do,

or maybe how much the wind was blowing or how lucky. Why should your penalty be based on fact that which has nothing to do with intent?

[0:45:06]

Now, I am not an attorney. So it is probably good reason certainly it is easier to measure the effects than the intent. So, my guess is that as we invent law we can do the hard thing but it is very easier to do the easy thing and just totally **[Cross-Talk 00:45:26]**

Jonathan Zittrain: It is funny that it puzzles you on the negative. I wonder how much it puzzles you on the positive. Should we give a Nobel prize for an effort like Frankenstein, I am sorry it didn't pan out but there was a lot of work to it and that was pretty genius, it just wasn't true.

Bruce Schneier: But there is a difference there. Because there you are actually awarding a result and you are not awarding, you are not passing.

Jonathan Zittrain: It will be funny if somebody accidentally cured cancer and won the Nobel Prize and the **[Inaudible 00:45:57]** is like "It can happen to you to" **[Laughter 00:46:00]**

Bruce Schneier: It is something like the Beverly Hillbillies of Science.

Jonathan Zittrain: That is right. Black DNA gold.

Bruce Schneier: That would make it. That would make a great sitcom, faculty at Harvard.

Jonathan Zittrain: **[Inaudible 00:46:12]**

Bruce Schneier: That would make a great sitcom because now he is faculty at Harvard. He doesn't know a thing and he has got to teach. Wow! **[Laughter 00:46:16]**

Jonathan Zittrain: A less unusual situation than you would think. **[Laughter 00:46:19]** So I feel like we should open it up. To do so and it is being recorded I think. It is not going on Live but it will be reproduced what you are hearing. **[Laughter 00:46:35]** We should see, is there atleast one hand held so there won't be the annoying phenomenon of questions are asked but the multitudes who watch it later don't. So let's just let these hand helds find repose and I guess my only suggestion is aside from the usual "Try not to speak unduly long" is "I am happy to conduct a conversation more than a ping-pong back and forth" so we will weigh in when we are moved but

let's have a conversation. So, here is a hand, here is a hand, here are mikes. Also feel free to say who you are.

Bruce Schneier: Or not because this is being recorded.

Daniel Dern: I have seen enough scenarios here that we don't have a week to talk about it. On one hand, Bruce you go to a restaurant, you got write your hamburger comments and then the guy at the register says, "I am sorry Mr. Schneier, but the restaurant computer refuses to sell you another hamburger this week because your medical records say that it is all you are allowed until next Thursday". On the other hand, somewhere in the basement of the FBI there is a big master switch that says, "All cars except ours stop. Cruise to say a stop and don't move".

Jonathan Zittrain: Which is the more terrifying scenario? **[Laughter 00:47:54]**

Daniel Dern: Or even United or even the Government says, "All network routing devices must use our code, etc. and we are not telling you what is in it".

Bruce Schneier: Like China is trying to do. That is not even theoretical. I have to choose.

Daniel Dern: I am not talking about scenarios **[Inaudible 00:48:15]**

Jonathan Zittrain: I have got to say that Bruce does run a semi-annual movie plot contest. So you already have got 2 entries going there. As I understand the rules, it is to come up with as scary and yet a realistic plot as possible but one for which there is no cognizable specific policy that the Government can do that it would be responsible.

Bruce Schneier: The phrase movie plot threat, I coin to be. And you are serious these overly specific scare stories you will hear in an effort to make you afraid.

Jonathan Zittrain: That sounds like a great show time series. Overly specific scare stories.

Bruce Schneier: But you remember that **[Laughter 00:48:54]**. Remember the terrorist that Scooby **[Inaudible 00:48:55]**, "The terrorists of Almanacs" all those make great movie plots. But you don't want to craft policy around that yet those are and when I first did the contest I got email from saying, "Oh my God, how could you give the terrorists ideas". **[Laughter 00:49:14]** Like people actually thought that the hard part of terrorism was the idea. **[Laughter 00:49:17]** thought you told them, look you can bomb a dam

and they would say, “God why didn’t I think of that” and run off and do it. **[Laughter 00:49:24]**

Jonathan Zittrain: So, I just want to know one point for a moment. I don’t know how many people remember this but back in the day there was that movie “Independence Day”.

Bruce Schneier: They are making a sequel.

Jonathan Zittrain: Harbor Day. **[Laughter 00:49:38]** way it is going down, the whole Federal Holiday Calendar **[Laughter 00:49:40]** and the British Internationalized counterpart “Bank Holiday” **[Laughter 00:49:46]** “Bank Holiday II”. Anyhow, I am now confusing myself with what my question was. “Independence Day”, the trailer came out and that trailer featured the White House being blown to bits.

[0:50:00]

I don’t know how many people happened to have remembered being in the theater the first time, you saw that trailer. I atleast remember feeling like “Wow, that was intense”. The reaction of the rest of the theater was kind of a stunned silence even though there have been plenty of ‘B’ movies that show Godzilla tearing cities apart. Even within the cycle of that trailer, by the time it was getting stale, people were laughing at it and of course now I think there are 2 movies being released this week which is like “White House blows up even more” **[Laughter 00:50:36]** and there is maybe something I wonder about making certain things more thinkable not by a contest run on a blog but by making mainstream certain acts.

Bruce Schneier: I think so. Want to address the original question, the hamburger. Basically what we are was saying is, “Do we want the Government to regulate our choices”? That is the question. We do all the time, by the pharmaceuticals you can buy, that hamburger can’t have more than there some amount of bug parts that are allowed and some that are too much **[Inaudible 00:51:17]**.

Jonathan Zittrain: Seems awfully hard to buy if people can’t sell it.

Bruce Schneier: I am not sure there is but there might be. On the drugs, on the prescription side, some people can buy this pharmaceutical and rest of us can’t because there is a mechanism by which you can get it. We as a

society, I mean there is a long rife here. I think that we can make a reasonable argument that modern advertising is an unfair trade practice. That it is no longer a seller informing a potential buyer the virtues of his product and it is now deliberate psychological manipulation.

Jonathan Zittrain: I can't think of any other reason I am buying most of the stuff I buy. **[Laughter 00:52:04]** So working backwards, I can't be to blame.

Bruce Schneier: Along with my rife on libertarism completely wrong is the notion that, and there is a lot of psychological stories to back this up that the point of sale is a terrible place to gauge preferences. That on the long term people want to eat better, on the short term "Man, that hamburger looks good". I got one of those damn Chex Mix bags when I came in here. I would have been way happy if.

Jonathan Zittrain: This session is sponsored by Chex. **[Laughter 00:52:36]**

Bruce Schneier: I would have been way happy. This is why we have adopted termlets. Please pass a law to prevent me from exercising my preferences. That is a truly whacky thing.

Jonathan Zittrain: Let me interject here because this so nicely fits into your earlier rife about Face Book and Google and kind of you can't just say it is market they are kind of having an advantage and that is why Government should come in. so the analogy here would be one reason they might not sell you the hamburger is because you signed up ahead of time and said, "No matter what I do don't sell me **[Cross-talk 00:53:10]**". The other reason might be some bloombergians, some **[Inaudible 00:53:15]** nudge or something where they are actually doing their best to remind you of the kind of commitments you want or the burgers have to be served with blue buns and they make a less esculent value or whatever it is. But that is an example of the Government intervening to save us from the market. Who is worse in this circumstance, Bloomberg or Big **[Inaudible 00:53:38]**?

Bruce Schneier: These manipulations are happening. In your grocery store, products are paying for eye level placement. Ones that don't pay get high or low. Those big gulps were designed for you to **[Cross-talk 00:53:52]**

Jonathan Zittrain: So if the Government intervenes.

Bruce Schneier: Someone is intervening. Intervention is happening. We can either say no intervention which maybe we can do or we can try and this is where I have trouble with solutions. But solutions, my guess is that solutions will be the multiple, distrustful parties each keeping each other on check. So do we want Government intervention to limit corporate intervention? I think some solution will have a corporate component, a Government component, a NGO component that everybody will sort of be keeping an eye on everybody else. Of course, this could fail. I thought this was the way the US Government was supposed to work but post 9/11 everybody fell down on the job. The Congress wouldn't keep the President on check. The courts said, "I don't know, you can keep me out of this". But in theory that is the sort of system I want to work.

Jonathan Zittrain: But at the very least one can retreat to, "We really need a self conscious dialogue about what kinds of forces" it is not much but it is something

[0:55:05]

Bruce Schneier: I am a big fan of this sustained nudges because

Jonathan Zittrain: Even though they are manipulation.

Bruce Schneier: But the manipulation is happening anyway. This is my unfair trade practices argument that we are being manipulated for profit. Maybe it is not that bad if we are manipulated for benevolence. Now the question is of course who decides what benevolence is? There is a lot of devil in the details but there is a whole lot of devil if you don't do these details.

Jonathan Zittrain: As was promised, this is a weeks' worth of stuff. Is there anything you want to say about the FBI turning off all our cars which when I put it that way makes it sound absurd but in fact the more the devices are tethered the more the Government can ask. You want to say something about that before we move on?

Bruce Schneier: And then we've seen requests for that. Any event of terrorism and the Government can shut off the internet. This is being asked. If cars is going to be driverless cars, high speed chase we need ability to turn off cars on the highway for the safety of everybody. You can see how that could make sense. Or atleast how that would be requested. But internet kill

switch has been debated. It may be fundamentally crazy for lot of other reasons.

Jonathan Zittrain: I should say in fairness at the time it was debated the senators pushing the bill that was said to contain it said, “This bill doesn’t contain that”. In fact the Government has long since had that authority to make some amendments to the Communications Act made in the wake of Pearl Harbor. So there is I think

Bruce Schneier: I missed the internet provision that was passed in the ‘40s. **[Laughter 00:56:37]**

Jonathan Zittrain: So we should keep the conversation going if the mike has found another home. How about over here? Got someone there.

Audience: So this is not my opinion in particular but I’ve been exposed to the opinion by people in the computer security community that the way in which to deal with these sorts of problems is that, rather than is that everybody should be responsible for their own Information Technology Security. That everybody should learn the skill set in full. If you don’t learn the skill set that it is your own problem.

Jonathan Zittrain: Dan Beard is one of the people who has talked about an internet drivers license.

Bruce Schneier: The problem is, it is not only your problem. We are too interconnected. If you think of DDoS attacks and Bots what security is very directly a function of whether my mother remembers to turn the Firewall back on because if she doesn’t there are more insecure computers being used.

Jonathan Zittrain: But I guess one question here is, how much low hanging fruit is there in trying to get grandma to turn on the firewall? Of all the things that make security hard, is there some space comparatively to try user education?

Bruce Schneier: I am not a big fan of user education. I think user education is a cop out. I think user education is a cop out when computer security people like me design crap systems. You get these warnings, you see them on your computer, “Complex security thing, blah, and blah, blah. Do you want to say Yes or No”. you what you read is “Blah, Blah, Blah. Make this dialogue box go away”. That is what you read and you click.

Jonathan Zittrain: “Would you like to continue with what you are doing?”

Bruce Schneier: Right.

Jonathan Zittrain: "Okay or Cancel".

Bruce Schneier: Would you like me to stop annoying you? **[Laughter 00:58:22]** It is rare that the user can make a better decision.

Jonathan Zittrain: I can't wait for the Firefox plug-in called "Yes Man" **[Laughter 00:58:32]** that just answers all dialogue boxes "Okay". I am having that.

Bruce Schneier: So, I want systems that are robust enough to deal with an uneducated user. We can't legitimately say, you need to pass this skill set to use the internet. It will be real hard to turn it into something like driving a car. I am not sure we want it.

Jonathan Zittrain: So, right now just share with us your best conception of the process of a user checking email from a server whoever the provider might be. What would be the best practice using today's technology so that the email provider can make it as secure as possible without the user having to be anybody other than grandma?

Bruce Schneier: What we have today is mostly good. I like seeing the additional authentication mechanisms. I like seeing the back of the authentication mechanisms improved. It is not a lot.

Jonathan Zittrain: So, you don't see anything out there that isn't already kind of working elsewhere?

Bruce Schneier: This is a surprise. This surprised me from your book. I read your book. You made a really good point that openness is so much better and that a closed system will be rejected. I believe that too. We've got it wrong. People love the IPHONE.

[1:00:00]

IPHONE is giving you more security because they regulate what goes on that platform. It turns out much to my annoyance that people like that. This is the problem with the feudal metaphor. We like these feudal systems because my mother does a way better job with her photos on Flickr. It is really better for her to be on Gmail. Better for her, her calendar and address book. She loses her phone, she purchases a new one, pushes a button it all appears magically. For the average user this feudal trade-off isn't that bad. I'd like it to be worse but it turns out not

to be because the cost my mother is paying is largely invisible, it is largely long term.

Jonathan Zittrain: And also along with security against third party attack it may well be more secure for her.

Bruce Schneier: Almost certainly is. But even against what I am more worried about the third party attack is she making a mistake. You make a mistake and you lose your photos, you lose your email, your hard drive no longer works. It is robust against the naïve user which is really valuable. Because if we want internet to be socially useful it has to be technologically easy.

Ethan Zuckerman: Hi, I wanted to return to the idea of asymmetric attack and the notion that the bad guys get way ahead of the good guys and what this makes us think about open and closed environments. Bruce I was working on my entry for the movie plot and I put together two current events. One current event was this strange little paper where someone claims that they infected a 100,000 cable set top boxes and used them to make a map of the internet. Hard to verify, but a fairly convincing paper suggesting that someone built a little worm that was capable of getting into many, many, many, many set top boxes. Roughly at the same time a really big DDoS attack using DNS amplification which we have all known about for a very long time but swamping spam house our friends and sometimes enemies who try to knock at internet spam under 300 Gigabytes/Sec of traffic. A level that many of us thought was kind of unfeasible for those things. You put the two of those together and you suddenly have a scenario which everyone's cable box compromised, becomes part of a giant DDoS network , hitting DNS and knocking out servers. For the first time.

Bruce Schneier: You haven't broadcast fake news. You've got a really good James Bond plot.

Jonathan Zittrain: I think that has already happened here. **[Laughter 01:02:53]**

Ethan Zuckerman: For the first time **[Laughter 01:02:55]** people would not notice. People might not notice. First time, I found myself looking at this and going "Maybe I am actually scared about this. Maybe I have actually hit the point where these open systems that for years we've known are riddled with holes because we are idiots about security but we are so resilient because we share information very quickly, we adapt so on and so forth. I

find myself wondering if we are hitting a point where not just on the consumer devices, where I think you are absolutely right first the people in many cases are preferring the safer environments whether we are going to hit this point on the actual core net. Do we think that we might be reaching the tipping point on this? Is that part of what is reflected in you writing some of those significantly depressing and the follow-up to this is, is this going to shake Zittrain at all on this who thus far has been really good about sort of coming back and saying, "Yeah, in general we are willing to trade a lot to make sure that we have the openness out there and so far it hasn't been but is this finally the time we get it".

Bruce Schneier: So, I think that is a good example. My worry is, is really that the fear of these things will leave the actuality. This whole webism mass destruction debate is largely a fear debate. The Cyber War debate is largely a fear debate. These are not based on realistic threats but you know 10, 20, 30 years they likely will be. I am afraid you have a point.

Jonathan Zittrain: I find myself wanting to say, especially when I ran into that spam house situation I find myself wanting to say, "Yes, this is exactly what I predicted". because my book wasn't, things are great except people are paranoid and the paranoia is going to destroy us. that was not the theme. The theme was, things maybe great now but the better they get the higher the stakes are for somebody to find value in making it worse and unless we come up with a defense to it that is constructed along the lines of what made it great to begin with, namely a distributed civic defense for a distributed civic network.

[1:05:10]

The most obvious defense when the trolls come is going to be a centralized response, a militarized response and that is bad. So I think that fits the template in the sense of people are a little bit kind of a sweep of the switch or collective action problem. There ought to be ways and there have been ways suggested to secure border gateway protocol, to secure DNS service and the DNS servers because each of those cable boxes contains a DNS resolver, who knew. There is a public proxy, like what? So these are the kinds of things that either an IP Source specific movie plot it is hard to go closing doors after the horse is asleep but this actually has been long anticipated and if the community that has roughly existed to build this distributed, collective hallucination to begin with

could come up with a distributed defense of it. So far the way Wikipedia has managed to do at the content layer. A distributed content generation system that contains its own defense, not just against guarding variety and accuracy but against every page being turned into an ad for a Rolex watch which you can guarantee has been attempted as we speak. That gives me hope. I just worry that the paranoia generated by the very real dangers represented by that incident will have just say, we've got to send the marines somewhere. I agree with the paranoia worry.

Bruce Schneier: Any solution is going to look like some form of resilience and whether it is the Wikipedia distributed type of resilience, whether it is something built into the internet. There will be different aspects of it but in a world where we are seeing people today calling the Cyber Threat an existential threat to humanity. Those words are being used by actual policy makers. That is fundamentally a crazy thing to say but getting past that is going to be a realization that 9/11 the existential threat was not the terrorist attack, was the reaction to it. That if we have a, if we come from not from fear but from endonibility and imagine if that is what President Bush got up and said, "Yes this is horrible. Yes we are going to be after them. Yes we are going to achieve justice but our country is better than this. The things they killed us for are not going to change because they try". Those sorts of ways and I think that rhetoric makes a huge difference.

Jonathan Zittrain: But see upto the minute Bruce Schneier worries about asymmetric offense because we have an existential threat.

Bruce Schneier: We said in the beginning this is not a consistent talk.

Jonathan Zittrain: Yes. **[Laughter 01:08:14]** Well it isn't. It isn't. That is right **[Laughter 01:08:17]** Cheap shot. I am sorry. Are there mikes? Yes, back here.

Gilly: Hi, I am Gilly. I am a senior at the college here and a former Berkman. So it seems that the most pragmatic solution that we have come out thus far is just start a discussion. So I want to ask about how to frame that discussion. I think the role of metaphors has sort of come up here and we talked about wars as a metaphor. It is sort of both a conflation of the threat and the use of notions from National Security. Then another thing that Bruce seems to support to me is the Public Health metaphor in a sense the Bloomberg intervention and that sort of making sure grandma

turns on the Firewall again. Are there any other metaphors we should be considering? Should be aware of these metaphors and what they imply?

Bruce Schneier: I think metaphors are extraordinarily important. Just taking the Cyber War metaphor, when you use the word war you invoke a certain solution space, right? Certain things that wouldn't be considered are reasonable when you are at war. For these type of Cyber attacks I much prefer a Police metaphor. I am actually for terrorism and much for a Police metaphor and I think it is much more accurate. I think that we as the people would make better trade-offs. When it is war and when the NSA goes to you and says, "Can I eavesdrop on every phone call?" When you are at war you say, "Okay, put this stuff on the closet and don't tell anybody". That is because you are thinking is war. So I find the War Metaphor dangerous. I like the Public Health metaphor, actually I think Biological metaphors are in general useful for the internet.

[1:10:07]

There is a lot of analogy not the least of is viruses. We are trying to see that go back. We are trying to see that the term virus came from health. We are trying to see ways that we are thinking about computer viruses going back into the medical community. They are using some of the tools we've developed for computer viruses to look at the spread of actual biological viruses. The metaphor of the internet stateless versus statefull, not from a finance state but from a Government perspective.

The metaphor of the '90s, that the internet is outside of any nation state it is turning out to be not true at all. There is more censorship than ever and now there is a rise that is called the "Cyber Sovereignty Movement" which terrify all of us. where countries are saying, "Look, we all of every piece of the internet is in somebody's border and the ones that are in my border I get to control and you getting involved". A lot of this I think you fight on the level of metaphor. You get the right metaphor, magical things happen. **[Laughter 01:11:28]** It really frames the debates. These debates are hard, they are technical, they are confusing, and the metaphors matter in an enormous amount.

Jonathan Zittrain: What of course the metaphor I am most intrigued by these days is Mutual Aid and if I am in a military environment I will call it a NATO for Cyberspace but elsewhere it is Mutual Aid that tries to push against the idea of "I wrote my cheque, give me internet. If there is a problem with it

that is a customer service issue". Lot of what built it was a form of Mutuality and then maybe useful ways for people to be able to help one another with cycles and bandwidth, with expertise and even at the content layer in terms of real crisis.

That is it a good thing to imagine should something happen now a natural disaster or otherwise my 3G goes down, my WI-FI isn't going anywhere, I am stuck. But what if my phone worked 2-way radio and can talk to every other 2-way radio in the room and what if my Face Book credential were cached and I could then see any of my Face Book friends in this adhoc network and if they are I could send them a message and if there is anybody in the network that has a pre-cached route certificate that says, " I am from the Government and I am here to help because I would like some help". Those are examples to me "Mutual Aid in Action". It is not a solution to every problem but it tends to be overlooked because it isn't all that helpful in many other public safety defense operations that the other metaphors tend to invoke.

Bruce Schneier: Like the Infrastructure metaphors but some had the idea of the internet dial tone and I kind of like that. I think something to be said for us to realize that the internet is a infrastructure, it is a utility. It is not optional. It is like water. It is like power. I think that is valuable. British Telecom had a great slogan a couple of years ago called "Innovation at the speed of life". They meant to me going really fast. I thought of it and said, "Wouldn't it be neat to have a slow down like that".

Jonathan Zittrain: I am thinking about the serial. **[Laughter 01:13:52]** Okay, so why don't we take a few more questions because we only have 14 minutes left.

Bruce Schneier: Wow.

Jonathan Zittrain: So, my suggestion is that we take some thoughts and they are going to pile up and be specific but Bruce has a pen and he is going to write some stuff down. I just want to get some more voices in as we go. So, please.

Audience: I am less concerned about threats from the internet to humans but threats from humans to the internet and if you look at **[Inaudible 01:14:22]** where you had a global scale conflict you saw that **[Inaudible 01:14:29]** are being smuggled across borders and there was some communication possible but it was extremely limited. I am curious what if the internet can exist post a global scale conflict where nations are

rebuilding their networks and whether the internet can exist during a global scale conflict and what your thoughts on that are?

Jonathan Zittrain: Let us take some other questions, wherever the mikes happen to be. This may I realize the favorite people on the periphery but yes.

[1:15:00]

Audience: You mentioned that, speaking about Anonymous that we are going to call that the next Cyber War but it is not. It is just a bunch of random guys. Your emphasis on the asymmetry of attack and defense seems to run against the idea that war can't be about random guys and I would like some comments on that.

Jonathan Zittrain: Got it. I was going to ask you about Government Policy too but well I let you succeed. Where is the other mike, yes?

Audience: I was going to suggest that the reason that you got tempered response to $50 for a less data collecting Face Book is that it would be a less useful Face Book. You would be losing all of the people who like 'X' also like 'Y' suggestions that people actually tend to like getting.

Jonathan Zittrain: Face Book comes back and says, "For you". We will still keep that for your 5 bucks, will that get your hand up? In other words, you think what you hate is also what you like.

Bruce Schneier: In general people tend to like the primary users. Everyone like Amazon's Kindle Books. They like the books they bought. People tend to dislike other secondaries that Amazon then sells and then somebody else propagates that. We tend to be okay with the immediate recommenders systems and the immediate systems.

Jonathan Zittrain: Although it is interesting to imagine that does apply to people suggesting, people will like this, this other person especially in a real environment rather than just Face Book and that is getting really close.

Bruce Schneier: People tend to like this lecture might like to attend a lecture next week.

Jonathan Zittrain: Yeah. Where are the other mikes? Yep.

Audience: On the subject of Anonymous I am just wondering how much you think Anonymous is sort of a reaction to a loss of faith in the Government. For

example, Wiki leaks. People who supported Wiki leaks didn't have really a standard way of hating within the system. It wasn't like the FBI was standing up and saying, "Well, Wiki leaks may not be legal but we are going to hunt down these people who are doing DDoS on Wiki leaks". So, Anonymous is sort of people who said, "Well, our only option is to go DDoS other people and then we can sort of defend".

Jonathan Zittrain: I guess this is the Batman theory, yes. The times call for the person. There is the other mike out there around somewhere? All right. There, sorry.

Hal Hudson: Shall we go back to the Feudal metaphor. My name is Hal Hudson. Lets' go back to the Feudal Metaphor briefly. I guess the feudal system became bad when people started getting hurt and you can kind of imagine. At the beginning it was rather nice. Kind of like at the beginning.

Jonathan Zittrain: Episode 1.

Hal Hudson: Yeah, you can imagine at the beginning Google was rather nice and it was. So what is the internet company equivalent of killing peasants because you are pissed off? What is going to happen? What are the damage equivalents for internet companies of the Feudal **[Cross-Talk 01:17:44]**?

Bruce Schneier: I think the last of the Google Reader is the one we've got right now. **[Laughter 01:17:47]**

Hal Hudson: Google Reader is hardly killing villagers. But what is going to hurt me. Google Reader is just inconvenient. It is not actually going to harm me.

Jonathan Zittrain: You took away my free product. **[Laughter 01:17:56]** How dare you? Ben & Jerry's, I want ice cream every day.

Bruce Schneier: I don't think we will get that kind of harm. It is the internet. It is not the real world. So you are not going to get Face Book.

Jonathan Zittrain: As Captain Kirk would say, "For how long, Mr. Schneier? For how long?"

Bruce Schneier: You are not going to get Face Book spearing its users. It is just not going to happen. **[Laughter 01:18:20]**

Jonathan Zittrain: Atleast it is the silver lining to his pessimism**.[Laughter 01:18:24]** I know we've piled up a lot of questions. You want to, did any of you want to say what has happened so far before we open it up again?

Bruce Schneier: The question that I thought, the notion of can a bunch of guys declare war? They can do something but I think war is a very specific thing and it is something nation states do. I argue that what a bunch of guys do even if it is damaging and there is a lot of history with organized crime I can do a lot of damage. A couple of weeks ago had someone assassinate a prosecutor in Texas. And then lastly, I think this is very much I don't know if it is terrorism. I don't know what to call it but a couple of days ago another prosecutor has stepped of a case prosecuting the Aryan brotherhood because he fears for his life. This is a viral action to change policy. So that is what I would call it. If these things, even though they are bad, even though they kill people they are not war. War to me is nation state versus nation state. Yes, there are these new sorts of asymmetric threats and they are important but is the war metaphor the proper way to deal with it. We screwed this up. We were attacked on 9/11 and in response we invaded a country because that is what militaries do.

[1:20:01]

If the FBI were in-charge we wouldn't have invaded a country because that is not what the FBI does. Now we can argue whether invading a country was the right thing to do but there was no actual debate about it because the war metaphor was immediately invoked.

Jonathan Zittrain: It is funny to think if the President in the wake of 9/11 had said, "We are starting a full criminal investigation. The US Attorney in the Southern District **[Cross-Talk 01:20:29]**

Bruce Schneier: We did with every other terrorist attack to date. That is what we did after Mumbai, not probably. Kenya.

Jonathan Zittrain: That is interesting to see **[Cross-Talk 01:20:46]** nearly a decade later that choice which may well have been sort of by democratic accountability somewhat a forced one to sign. That is no doubt debatable.

Bruce Schneier: It was psychologically the right choice, unfortunately.

Jonathan Zittrain: But it is interesting that choice then persists in the sense that it attempts to down shift into a "Lets try these folks in criminal system mode" still results in a lot of push back

Bruce Schneier: Remember that we were trying to bring one terrorist from Guantanamo to New York to try him and there was actual fear we couldn't put him in a

US jail. I am thinking, "What is he Magnedo?" **[Laughter 01:21:26]** He is just a guy. But there is this fear. I think Obama had the opportunity to change it when he took office. He could have said, "It is perfectly a reasonable reaction that went in here".

Jonathan Zittrain: Congress actually passed a **[Inaudible 01:21:45]** act that prevented it. There is one other quick thought too on your notion about, "When you have prosecutors withdrawing from cases out of fear for their physical safety"

Bruce Schneier: That is what happened in the US. that happens in other countries. **[Cross-Talk 01:22:04]**

Jonathan Zittrain: Where you have judges wearing hoods.

Bruce Schneier: Right. That happens in Mexico.

Jonathan Zittrain: That gets back to the question of – If our own primary institutions are faltering does that push for alternatives? To me it calls to mind a book to be published by Yale University Press called the "Cartoons that shook the World". A very scholarly team of peers reviewed of the Mohammad Cartoons from Denmark and it included not only the cartoons in question but depictions of Mohammad over the centuries and the Yale University Press did a security review prior to going ahead with the publication and concluded that it was not safe to publish and insisted that all of the cartoons and all of the other depictions be removed from the book and the book was still published with the objections of the author was removed. The book was published without them and when Yale responded to assertions that they were kind of giving in to threats of violence kind of thing. They said, "You know you can just get to them on Wikipedia. So why do you need us for it". It is an interesting kind of point that Wikipedia does not even have enough of data ware to decide whether to take the cartoons off that were a click away. In fact there is a discussion, a talk tab on the page about the cartoons on Wikipedia talking about offending sensibilities, not threats of physical violence and they have decided it would be a very small thumbnail and then you could click if you want it. That was the Wikipedians solution for the problem.

Bruce Schneier: But that goes to his point of Anonymous being a loss of **[Cross-Talk 01:24:42]** I think if we sort of look at their activism it is both a frustration

at the institutions who are behaving badly and a belief that the institutions aren't going to follow through with what they should do.

Jonathan Zittrain: So my guess is the mikes are in 2 hands currently are about to be. Let us do the last 2 mikes and then we should wrap. Where they are? Right here, sir.

Audience: You invoked let us say the Gay Marriage flip and the question is how optimistic can we be that the nation state becomes redefined by the internet in time to save us from this debacle.

Bruce Schneier: That is the question. So, the question really is the relative speed of social change, political change and technological change. That is your question. It is a really good one. **[Laughter 01:24:40]**

Jonathan Zittrain: I am detecting a theme in tonight's thoughts.

Audience: I was wondering whether atleast in some cases we don't have to be so afraid that the Government has access to our data. So we talked about them using our Financial Data to decide who to audit.

[1:25:00]

If they are mining through our data everyone is anonymous when they are going through until you are identified as someone likely to have committed tax fraud. Whereas before the internet they would have had to break into your house, look around, serif the pools in the back are not. That seems to me like a much more fundamental invasion of privacy than just seeing your Anonymous data and then pulling out the committers.

Bruce Schneier: A lot of cases you can build. You can build privacy preserving systems. Already we allow the police a remarkable level of intrusion into our lives. We do that willingly. But we put in a security mechanism. The warrant process is meant to be a security mechanism. I will allow the police to intrude my life but they have to first convince a neutral third party that it is in societies best interest to do so. The rules are telling me that they did it after that. There is a whole lot of mechanisms not to limit what the police can do but to limit how they can do it. So that is our trade-off to make that work. Those sort of trade-offs are certainly possible in all of these technological type of surveillances, investigations, data collections. We are not doing any of them. An example is in Full Body Scanners at Airports. You can either see the picture or you can blur out the human

form and see a stylized picture and just the contraband objects you are looking for. They are both technologically the same. Larry Lasik has a great point of the license plate. The police say, “We need to know who is driving the car because the cars are hitting things and people are driving away. That sucks. Our idea is we want everybody’s name on the back of the car”. Someone says, “Wait. Don’t do that. That will lose our anonymity. Put a random number on the back of the car. We will give you, the police the database of random numbers attached to people and that way you can look up cars when you need to”. That is the mechanism that gives the police what they wanted but preserves privacy. There are really clever things we can do to do that. We are just not doing them.

Jonathan Zittrain: Which also tends to raise the question that often divides engineers and lawyers and you kind of gave the lawyers an answer descriptively speaking which is, “Well we can hash it. We will have a table and the Government can consult the table when it has good cause”. And often the engineering answer is, “I never trust them to have good cause. I want a fake license plate or no license plate or something like that”.

Bruce Schneier: There is an argument made to what are the solutions here to know the very invasive police measures is to give the police better tools. The reason, I mean they are just trying to do their job in most cases. It is the job we want done. The reason they have to be so expansive is that we don’t have the surgical tools. If we could design them well the better chance of having them not do the things we don’t want them to do.

Jonathan Zittrain: So speaking of engineers and lawyers this event is co-sponsored by the Center for Research for Computation in Society, The School of Engineering and Applied Sciences and the Brooklyn Center for Engineering Society a part of the University but often identified with Harvard Law School. I think tonight’s conversation has been as kaleidoscopic and freewheeling as it was promised to be. We are still trying to figure out how to make the most of a physical gathering like this, a gathering augmented by the various technologies we know are happening at the moment in the background. We have got a big Twitter feed in the screen behind us. these are threads of conversation I think that show first how hard this stuff is and not reporting to have answers where we don’t yet have them. That also really cause us to ask how many of our solutions can be general type solutions. A sort of approach that I

work from zone to zone to zone or how much of it is trying to fix one week at a time and do so in a way that may feel like your movie plot example which is you just keep closing upon doors. But it provides I think a lot of puzzle that we continue to work on and venues very different from a public lecture. We are very hopeful that Bruce will continue to be in our environments here in Cambridge virtually and we will have chance to continue the kinds of conversations that are happening here.

Bruce Schneier: I actually really appreciate the conversations. This is stuff that I am as you can tell still trying to figure out. I am glad that it has been taped. I wasn't taking notes but I will listen to this again. I said stuff I didn't realize I was going to say. **[Laughter 01:29:59]**

Jonathan Zittrain: And you guys there is a bunch of people tweeting stuff that they were finding you on Face Book now and we have to tell them it ain't you.

[1:30:05]

Bruce Schneier: Okay, there actually is a Face Book account that mirrors my blog and there is a Twitter account that mirrors my blog. I control the Face Book account but not the Twitter account. Someone else set that up. But I never actually visit these sites.

Jonathan Zittrain: All right then. **[Laughter 01:30:21]**

Bruce Schneier: So don't send me stuff on Face Book.

Jonathan Zittrain: So please join me in thanking Bruce Schneier for a very good opportunity. **[Clapping 01:30:30]**

[End of Audio] [01:30:35]