Transcript: EFA Speak Out #3 – Tuesday 11th February 2014

Danny O'Brien – International Director, Electronic Frontier Foundation (EFF)

Sean Rintel (SR): Alright. Well thank you everyone for joining us at the third EFA speak out event on "the day we fight back" in Australia, rather the end of that day in Australia, and the beginning of that day in the United States. So we are very, very pleased to have with us the EFF international director Danny Obrien, who's a very distinguished activist in the field, and who has been coordinating this campaign, and has been doing lots of this stuff for a very long time-for over 15 years- and we're just thrilled to have him and to be able to talk to us about all the details of this globally. The issues as he sees them In Australia and the U.S, and of course globally as well. What we can do practically, what we can do now, what we can do in the future. My name is Dr. Sean Rintel, I'm the chair of Electronic Frontiers Australia, but much more interestingly, we've got Danny O'brien who is the international director of the Electronic Frontier Foundation. So Danny, over to you.

Danny O'Brien (DO): Well thanks Sean. I hope you can hear me OK. Give me a thumbs up if you can

SR: I can.

DO: OK, the technology is working wonderfully. Well, I have such a long space to talk. I have to say that this has already been one of the longest days of my life. I think we spent the last weekend rushing to get everything sorted out. It was great to see Australia coming online. I think we sent the tweet out about your work midday here in San Francisco, which would have been about what, 6am? Yeah, 6am-ish, y'know, generalising across the time zones, and really we've been preparing this whole action for almost a month now. I just actually finished submitting a patch on Github for one of the very last pieces of the code.

One of the things that's made it enormously interesting is that up until now, I think the closest we've got to international campaigns on the web, actually dates back from the very founding days of the Electronic Frontier Foundation and Electronic Frontiers Australia, which was the Blue Ribbon Campaign, which - if I can just use my beard here to go back in time - was a campaign that was about a US piece of legislation 'The Communications Decency Act', but that was due to set a really terrible precedent; which was that the internet should be a system for communication, but a system for communication that governments should be permitted to place essentially a censorship regime over. It was the first attempt to legitimise the blocking of websites. As you can tell from the title it was all about the 'moral majority'- as it was called in the United States - attempting to chill speech on what was then the fledgling internet back in the early nineties - I'm not going to give the date because really it's half past 11 here and I've been up for a very long time - but that was actually an international campaign; people put the blue ribbon on their pages; EFA and EFF and other organisations all joined together to stamp out this particular proposal, and one of the key moments in it was actually Yahoo - this was before Google, this was I think before AltaVista the predecessor to Google - actually turned its front page black and put the blue ribbon in a very prominent position. So this was...that was a very interesting combination of events. What it was a law that was being proposed in the United States that provoked a really international sense of fury because of the standard it was setting, the idea that the internet should be censored. Something that everyone really from the moment they used it and got an idea of how this technology could work and was intended to work objected to, and then people showed their discontent by putting these banners up on their own homepages linking back to the central Blue Ribbon campaign, and then we had, like, companies getting involved and thinking this was important as well.

So, fast forwarding a bit to things that I think are now still in living memory which are the SOPA and PIPA campaigns; again, we have this idea that SOPA and PIPA were primarily United States laws. But everybody realised that the idea of setting this standard for copyright or intellectual property reasons, that the domain

names could be blocked or removed from their rightful was clearly an anathema, and we were incredibly concerned that this was like, the first attempt to establish this as a principle, and as a consequence people united, and also that led to an international movement to make sure that these principles weren't smuggled in-as they really often are-through international standards, and international norms, and in that case that was (...) the anti (..) trade agreement which had very similar principals wired into it, and so an international protest against SOPA and PIPA combined with companies - because, as you remember, Google put something on their front page, Wikipedia stepped forward, many other companies around the world said "this is something that's undermining not just people's human rights but also your commercial ability to communicate over the net"- really set this set of dominoes going, so SOPA and PIPA went down and ACTA went down, and I think we're pretty sure now that any attempts to present this sort of removal of websites through domain names for copyright reasons is going to have to be done in this very, very slow sort of incremental process, and I think a very good example of this sort of approach is what we've seen in Australia, where you try to put forward a censorship plan that's based around blocking IPs or blocking domain names. That's thrown out as being a 'step too far', and then you have this incremental kind of unofficial sort of approach which says "actually governments kind of have this right already, and we're going to go ahead and do it" and as soon as they do, hopefully there's a huge fuss.

To just sort of touch base with SOPA and PIPA, is that after SOPA and PIPA failed and flamed out so spectacularly in the United States, what happened was the authorities said "Oh, well, we have this right anyway", and we've got these individual cases of domain names being seized by the customs services. But at least in those situations it's very, very hard for states to get a strong grip on doing that because they have to fight each individual case, and because there's been a large protest, politicians don't really want to touch this, and judges are increasingly sceptical. There's always a challenge, and this is something that activist groups like EFA - and many other groups like Open Rights Group in the UK - is great at sort of bringing these to a head, but you have to establish the norm first of all. You have to show (that) actually people don't want this kind of censorship or people don't want this kind of domain name blocking, and so you establish in the political culture that this is a hot potato - that this is going to be the 'third rail' of doing something on the internet. And, you know, politicians are very instinctive creatures; if they've been burned once they really don't want to go pass it again. It was amazing to watch with SOPA/PIPA in the United States. Genuinely-and I know people always say this, but I was sort of weirdly on the sidelines in SOPA/PIPA and maybe we can talk a bit about what that was like - but I watched a bunch of politicians and a bunch of lobbyists going from "this is a slam dunk! This is the easiest thing in the world! No one is going to object about this" to genuinely not wanting to go anywhere near anything that had 'internet' or censorship' or anything that could be framed as a politician stopping the internet, or killing the internet, or anything like that could be framed like that.

Which brings us today: so we've faced, since June, a series of revelations by Ed Snowden, and joined with other whistleblowers old and new about what the NSA, and the Five Eyes - the other countries involved in information and controlling resources in this way have been up to, and certainly in the EFF where we've been fighting this battle since 2006 at least, there's a bit of an air of "well, we knew something like this was going on". Well, we knew, and the reason why we got upset is because we could foresee the consequences of this and what Snowden's spelled out in such compelling detail is...he has shown what these ramifications are and really made people think about it. So we're now at the stage where the public is hearing about this for the first time, it's really trying to process it, and the politicians don't have a strong sense of what's going on, and this is true in any country. The instinct at least in the United States was national security; "no one's ever going to stop us from defending our brave surveillance troops at the NSA and no one, you know, once we explain that this is for secret national security reasons" you know, and that's the root password to the constitution as they say. This is not going to change anything, and you know, mostly people believed that at the beginning.

In the United States at least we've now seen opinion polls drop and drop and drop in support of the NSA, and this really started right at the beginning when we were going "Oh my god! Our worst Nightmares are true, all of this is being revealed. What happens if nobody cares?" And then we had a vote in congress - the Americans had a vote, I still have a British accent (...) I can't vote - so congress had a vote to defund the NSA - this was really early on, I think this was I late June or early July, and it almost won; I think it only squeezed through with 4 votes, and that was because the Democratic party actually put the equivalent of a 3 line whip on this-forced their people through. So even in congress, even without this change in public opinion on this, in the United States - which we have to say is not famous right now in this decade for putting civil liberties before national security interests - in the heart of DC people wobbled, people were not sure about this. It's not been true in lots of other countries. I think largely because there's really justified anger at what the NSA is doing, particularly that the American government feels that non-US citizens, or non-US persons as the category is, have absolutely no privacy rights at all. That's at least the assertion being made effectively by the US government. We at EFF think that that's nonsense both in terms of public policy, but also in terms of how things should be interpreted. Nonetheless, that's enough to make everyone annoyed, but everybody - and when I say everybody I guess I mean everybody outside of the United States - has a feeling that something is going on that is sort of horrible (and) invasive but we don't have any control over it; it's in the United States, we don't have a vote.

Well there's a couple of ways this actually plays out: the first one is actually the pressure that the international community places on the United States does have an effect. It's a subtle one, and again I can't really convey because you're never going to get an American politician going "I decided to do this on the basis of a bunch of foreigners being upset" but in DC you can see this starting. Basically what you see is the damage that's being caused to American foreign reputation with their major allies has a knock on effect, right? It basically means you have to negotiate harder for everything else. One of the other things the EFF works with- and we can talk about this if we talk about surveillance - is international trade agreements, and right now there's one being placed between the United States and Europe, and all of those politicians are going in going "Hey, we're going to have do something about this NSA surveillance" and effectively implied "and if we don't you're going to actually have to compromise on a bunch of other things" so it's this sort of like strange, real politic balance that's going on; there's real damage caused by Obama having to sit down and meet the chancellor of Germany when all the newspapers say he's actually been listening to her phone calls for the last few years. It really has a knock on effect. So there's that, and that's kind of in the real politic phase. The other part of that though - and this goes back to the Blue Ribbon campaign and SOPA/PIPA- and this is about international norms of government. Right now, we're in a situation where a certain segment of the American governmental system is insisting that 1) mass surveillance, mass trolling and collection of all the emails, all your text messages, all the meta data about your phone calls - even your location data, even where you are when you're using or just carrying your phone- all of that stuff is fair game and anyone can collect this. Any government can collect this and there's very little oversight that's needed. There doesn't have to be a court order for this kind of collection, there doesn't have to be a court beyond a secret court that's specially created to basically rubber stamp these proposals, and this is just the way it is, and everyone should just accept that and shouldn't even be surprised that this is going on. That's an appalling norm, and I think most of the digital activists already know that; anybody who understands how the internet works, anybody who understands quite how much information about us is being shared on the internet, anyone who really understands anything about how computers mine that information, and learn even more than what we've already discretionarily released; anyone who understands frankly Google's Ad business model, or why Facebook is a multibillion dollar industry; anybody who lives in the 21st century, and thinks about it for a moment, understands the damage of creating a surveillance state like this. The issue is that governments just say "NO this is perfectly normal".

Which brings us to today: right now we have two campaigns effectively, but they're joined together. Within the United States,a la SOPA/PIPA fight, we have a campaign to just call congress people and invite them to support a couple of bills. Now, I have to say that those bills in (...) are in effect the beginning of something good; they have some great things in them, but they really are just the beginning of the solution. We need real investigation about what's going on. We need to find out what the NSA is actually doing, and once we know what they're doing maybe we'll be in a good place for congressmen and politicians to actually craft laws to stop what they're doing. Because otherwise it just turns into an episode of Father Ted, Right? Where you're just going, "whatever you're doing stop that" we disapprove - What is that? I can't remember - I'll come up with the line latter on-but anyway, so we're in that position; urging congress people - like I say 'the congress critters"- in the United States to stand up and start doing that - this is the first step in the United States.

The other part of it is establishing this global norm, and we feel that the thing that everything can unite on is basically no mass surveillance. Surveillance is supposed to be targeted. It's supposed to be aimed at suspected terrorists, or, y'know, James Bond like spies or other people getting up to...y'know, a very narrow range of things. It's not about scooping up information about everybody who uses the internet, and in order to sort of draw that line in the sand, what we have to do is point out to these governments that existing human rights law already forbids this, and that's the tricky bit, right? That's what you have to do. So, that's what we're doing. In the US right now Americans we'll be waking up to "the day we fight back" and they'll be calling their congress people and urging them to pass this law. In the rest of the world what we're urging people to do apart from - and this is kind of my third point - fighting the encroachment of these tools in any other government - because it really isn't just the NSA that's doing this, it's really not just the US - it's really not just their allies like Australia, and the United Kingdom, and Canada, which we find out the same way the Americans find out (through these Snowden leaks). It's anyone that can get their hands on this capabilities...so locally we all have to protest that, but then we have to unite and join together and say "look, human rights law this is the (...) by anyone. Y'know, we really need to have the same level of prohibition as the Geneva Convention prohibits particular uses of weaponry in a war- a prohibition like a landmine prohibition. This stuff is literally - well not literally - but it could be...nuclear, right? It's toxic to open societies; it would burn away the moment any dictator had access to this, or any corrupted official had access to this it would be game over. It's midnight here (laughs) I guess I talked a long time, but this is what we're urging people to do, and I'm sure many people have already done it because we're getting to the end of the day-'the day we fight back' in Australia.

Sign the 13 principles. Sign the principles that we formulated as necessary and proportionate. You can read them if you like. They're fairly detailed. They're very 'lawerly'. They've very - they're not cautious, but they seem just like perfectly sensible things to say to anyone who isn't the NSA, and what those principles, those 13 principals basically spell out is what everybody understands a surveillance law should be. They don't prohibit spying. They don't prohibit criminal investigations of the bad guys, but they do say "you can't spy on everyone and you can't spy on people just because they live in a different country" and if we get those two things out of those thirteen principles then we've done pretty well. There's a lot of other stuff there that your viewers will recognize in particular: protecting encryption, and the tools of encryption and preventing back doors in companies, and technologies and standards and the like. There's stuff about things being limited in there being legitimate oversight and so forth but you can plough through them all, but trust me - me and many other people have ploughed through them - and this is basically what we see again, as the minimum standard going forward. And we can set that minimum standard in the same way we set the minimum standard for how the internet should be a free communications system. That means that politicians hopefully, and intelligence agencies will view this as the third rail of surveillance, and they won't conduct this kind of thing, and if they do they will be held countable in whatever country they try to pursue it. That's it...

Oh I can't hear you I think you're muted.

SR: Yeah, I'm unmuted now. Danny thank you so much, that was absolutely fantastic. There's some questions that we'd like to ask you. I've got a couple. I'm sure David Cake who's our vice chair also has a couple that he'd like to ask you. Maybe I can start out with one and then we'll switch to David. Does that sound OK to you David?

David Cake (DC): Sure

SR: OK. So Danny, one of the things you talked about is making surveillance a hot potato for politicians, so that they don't want to go near it, they don't want to sort of rush into those kinds of bills. This very day, one of our senators, Senator Scott Ludlam who's a long time Green senator who's been fighting for...

DO: Love Senator Ludlam.

SR: Right.

DO: I mean I can't vote in Australia as well (laughs) ...There are many other senators that I admire his senatorial knowledge on these matters

SR: So he today stood up for all Australians in the Australian senate and asked the attorney general George Brandis about these kinds of issues, and ultimately Brandis just sat down and sais "this is national security I don't want to talk about it" and sat down. One of the problems we face with this kind of issue, bringing it to the public's attention so the public gets enraged enough to make this a third rail for politicians -'third rail' by the way for Australian viewers is US slang I guess for the electrified middle rail of the subway system. Although we don't have that, we have an over-head line so I guess...

DO: I'll confess I got it from the West Wing so you know...(laughs)

SR: One of the problems he had is kind of the Habeus Corpus problem, is that when there's actual instance of an actual problem that has led to damage. You know, the things that Snowden-the Snowden revelations are a big deal for the civil rights communities, to the digital communities, to the internet, to the computer science communities, and to the coding and professional communities, but a lot of everyday people fell that they are not seeing many instances of this that they can then in particular. So then in some ways we see this as kind of like akin to the Global Climate Change problem: that is to say, it's been going on, and there's a lot of people that know a lot about it that say "it is really important! It is clearly going on!" but individual people don't seem to see the point at which it affects them, so it can be hard to change some people's mind. Do you know any examples of these sorts of things or ways that we might go looking for these kind of examples to be able provide better, clearer examples of concrete manifest things we can help to do something, and it's bad?

DO: So the Snowden revelations are really not finished yet. There a hundreds of thousands of files as far as we can tell in that repository, and we've been getting here in the United States a headline or two out of that pretty much every one or two weeks since June, which is a pretty incredible record. Like, one of the things that-we're amongst friends here- so I can tell you one of the internal discussions we have with the EFF apart from "Why does Glen Greenwald release these things just when we thought it was going to be a quiet day in the office?" but one of the things that we talked about is first of all fatigue; we worried that people would gradually...it would normalise it rather than make it appear weird, and the second thing is we didn't know what stuff was going to be upsetting and what stuff wasn't. I think that it was really interesting in the first few days. So the first of Glen Greenwald's revelations actually from the Snowden revelations was something that we'd been looking for at EFF or a very long time: basically a smoking gun. It was actually the secret court order that required Verizon (one of the US telephone companies) to hand over all of this meta-data. This was something that we'd been fighting in the courts for years, and that came out in that first one, and we we're

like “Oh My God,” but mostly it got covered in the people who write about our stuff. The second one was the prism revelations, and really that hasn’t stopped, right? People are still weirded out, and freaked out by the idea that the data that they share with companies is being handed over to the American Government, and I sort of think I see this as a sort of A-B testing of what turns people’s attention. I think that most people react to these things - and rightly so - in a very emotional way, and the two key ones to me have been prism. Prism because it’s a breach of trust by somebody, by an organisation that you formally trusted, and then you sort of go back and realize what you’ve said, and what’s been done and how revealing that is. So that’s one part.

The second one is something called “LOVEINT”. So “LOVEINT” is the term used within the NSA for when NSA employees start spying on their spouses, or ex-partners, or prospective partners. The very fact that there’s an internal term for this within the NSA gave a lot of people pause and got a lot of headlines, because it was the first indication of a kind of very human fallibility amongst these people who sort of insisted that they had everything under control, and I think that right now that it’s the nature of the stockpile of information that we’re getting; that it’s the stories that the NSA and GCHQ and others tell to themselves, right? You look at these powerpoint slides, and part of the shock of them is they’re sort of boastful, right? They’re sort of going “a ha! We’ve collected everybody’s text messages” or you know “we’ve come up with a silly name for a system that lets us find out really quite personal things about person from their angry birds advertising patterns” right? This is what was happening; they were collecting data on the ads in angry birds, and those ads - because of advertiser’s own profiling - knew when somebody was married, single or a swinger as it were. So it’s this kind of stuff that changes people’s minds, but right now we’re only seeing a little tiny sample of them. Like, the NSA is never going to do a terrible, awful powerpoint slide boasting about how corrupt it is to itself because these are the stories it tells itself. We have to bear that in mind because there’s a lot more of this and there are many more potential whistleblowers coming out. So the two parts of this are “Yes, I’m pretty sure that that’s” the argument people would say is ”I’m sure that they’re doing the right thing that this information is only about the bad guys” setting the ground for saying “Yeah, but why- what a huge thing to be collecting, and then finding out these things” I mean, It’s a long call, but I think you have to think of it in those terms: set the frame, let everybody understand what’s happening. To give a really strange example which only works if your organization begins with the words ‘electronic’ and ‘frontier’ is...Do you remember the SONY root kit scandal? Right, so this was CDs that deliberately installed malware to prevent you copying them, and ripping them and putting them on your iPod or whatever. So that was a huge water-shed in the fight against DRM. Before that everyone just went “I can kind of theoretically see why this would suck, but It doesn’t affect me and I don’t really see the problem” to people going “Sony did what with the who now?” Right? People understood at that point the idea of copying stuff onto iPods then, and suddenly realised that someone was trying to take this away from them, and they were willing to do really invasive things to their personal computer in order to do it, and it’s that triggering point; where you frame the debate, where you talk about the DRM and all your friends go, ”Please stop! It’s like living with Richard Storeman!” and then at some they see what happens and they go “wait, I now understand what the horror is” and it really only takes one story like that. It really only takes one thing to happen close to you, and the race is to get those stories out, and to get the ideas in people’s heads before it’s too late.

SR: Fantastic! David, would you like to ask Danny a question?

DC: Sure. So, the only...over the years we’ve had SOPA, we’ve had PIPA, we’ve had all of these attempts where essentially the well-organised lobbyists try to charge at us and try and take away our internet rights, and we’re sort of getting better at fending off these grabs though they keep coming- of course the TPP is the current attempt- and of course, I mean, I think the fact that they’re trying to do it via such a closed, and secretive and undemocratic process makes it clear they know they won’t win any more openly. What can we do to not just

actually fight it off, but actually push back to try to shore up our rights for good rather than just keep defending each attack as it comes?

DO: Well, I think there's a number of strategies. One is, to sort of describe the way EFF comes into this, is the stuff that we do domestically, we always frame as bringing your civil liberties into the digital age, and the reason why that's so useful is because it's just a matter of updating some general fencing off that already exists, that people already understand as being essential to an open society, and so I do this - I mean as you can see...talking about the principles necessary, fortunate principles. I think that, like, that kind of 'this far and no further' is really useful, and so I think that it's being really interesting for instance watching, in Brazil, the 'Marco Civil', which is the idea of an internet bill of rights that defines and updates things. I think there are some huge opportunities in doing this. I think there are also some risks, in that we're always really nervous about a new internet law because it's an opportunity for everyone to stick their own restrictions in, and I think there's always a danger that something can be not sufficiently understood. So just to give an example there's a big fight actually happening today on 'the day we fight back' in Brazil where a lot of people are campaigning to make sure that there are true privacy protections in the 'Marco Civil', and there are already plenty of privacy protections in the 'Marco Civil', but there's a couple of interesting sort of tiny bits here: which is that there is a compulsory data retention clause in it, and also there's a long discussion about this idea of keeping personal data local in one country; it's basically companies have to keep their data in Brazil, and these things are still being worked out and argued about, but it's pretty clear to me that both of those particular proposals have some real problems attached to them.

Data retention, we know, is sort of a terrible idea, and that's been thought for a very long time, and really this idea of sort of keeping data locally is, y'know, almost like a first pass at trying to fight off something like the NSA surveillance. I think most people in the tech community or the internet community would go "well, I could see where this could call problems, and I can see where this would make this worse" So, in conclusion- and I'm sorry, the later it gets the longer I talk. I think this sort of Idea of a bill of rights are really good, and sort of an interesting way of solving this in one go, but you have to be really careful; you just drop one amendment in this bill of rights that's kind of not right and you're left with it for, well, what? 200 years around here! So yeah, that's one way. The other way, I think, is diversity: you get a bunch of countries to say "OK, we're not actually going to normalize in the way that the TTP requires us to do. We're not going to all come up with one solution. We're all going to try something different and new and see where that gets us, and let's compete on copyright law, and innovation and ideas like that" Of course you don't want to be in a situation where people don't accept basic human rights principals and say "no, y'know, we're just pursuing our own cultural oddity" but I think that's kind of interesting for this other stuff that doesn't necessarily fall into the category of basic human rights.

SR: Thanks Danny. Danny, do you think this is really kind of a western problem, approached from a western perspective, and done in a very western way and would have very different sort of ramifications in non-western countries? I mean, there are a lot of other sorts of cultures. Are we particularly concerned about it? Are we particularly affected by it? Should we be doing more in fact to help other countries-non-western countries- not get into this sort of situation? What's your sort of feeling sort of internationally about that?

DO: Well I think it's really easy to fall into a sort of orientalism about this sort of thing. Where, I think that often people think of censorship, or surveillance or internet controls as happening somewhere else, and no matter what happens in your own country as long as it's worse somewhere else than you've got nothing to worry about, and also there is also a sort of a sense of trying to export or target other countries with, as you say, sort of a particular viewpoint. I think the solution to this is home-grown digital rights organisations, and we've always really, really supported that at EFF. That really it's amazing how common the ideas are amongst internet users. I don't think there's many things that any EFA member and an EFF member would disagree on,

and frankly I've found that in all the places I've visited. I have an awesome job as the international director of EFF which means I get to go to places like Thailand, Mongolia, Kazakhstan, Brazil and many, many other places. All though Africa...and basically you see the same thing, you see the same groups of people, and the commonality is amazing, and I think that commonality comes from who we are, right? I think we're all in some way technology advocates or enthusiasts or at least interested in the impact of technology. We're all sort of on the leading edge of exploring that sort of thing, and I think we've all been influenced by the possibilities that we see there. So, for instance, I don't think an advocacy for absolute free speech rights is an artefact of the internet being an American thing, although some people try to view it like that. I think that wherever this technology first emerged, and let's face it - it didn't just emerge in the United States - it encourages in you an idea to see uncensored speech as a positive good, and the idea of censorship as actually a kind of technologically limiting and difficult to achieve even. So I guess what I'm saying is that every place that I've been, the internet has been really different. Like, if you look at how the internet grew and evolved in Iran, say compared even to Egypt, from a Westerner's point of view they might sit there going "oh, this is all the same" but it's really not. You go into these environments and it changes radically between cultures and of course up and down cultures as well. But at the core of it is a bunch of values that people recognise as important to keep this technology executing on its promise, and that's where you have this commonality, and that's the reason why we have over 400 organisations all over the world working on 'the day we fight back today'. We all have something in common and we all have some part to play in protecting people's privacy on line wherever we are.

SR: Thank you. David, do you have another question you wanted to ask Danny?

DC: Yeah sure...I don't do quite as much international activism and stuff as you do (laughs) but close! And it's my experience...you defined people who are passionate about the internet and it potential for free speech and so on in every society I've run into at least. This is a huge sort of growing global coalition of webists. I hope we get more organised and more effective. But I actually have another question: besides your EFF and so on role, I know you're also someone involved in the hackerspace movement-as am I (although) not as much as you- and you're very aware that the internet is becoming something that is creeping into more and more of our devices, and more and more of our things, and this idea of the access to not only controlling your own computer but the computers in your air conditioning, your refrigerator, and your every other devices is going to be an emerging issue. DO you think we're going to see that? Is that going to be another whole battle?

DO: No, I think that's incredibly perceptive actually. Like one of the things that's sort of super interesting is that EFF one of the things we have to do is think (about) endless years into the future. Because basically we have to do is convince judges to make the right decisions about things that will only be really public interest in a few years after that. So, in the early history of EFF we we're arguing that email should have the same protections as other documents that are described in the bill of rights, and we had to do this to people who had never seen an email in their life and we're like "why should we extend this to this strange thing?" and of course that seems ridiculous now; everybody understands that email's not only the same as physical letters, but has totally replaced them for many purposes, but you have to kind of sit there and work all this out. So right now - and I guess this is a spoiler if you're interested in what the next 5 to 10 years of politics is going to be, or cyber-politics - we're really interested in this, because the locking down of devices is something falls into that category of 'very hard to explain'. People love their closed devices, and they love their Apple kit, and they love their mobile phones, and these devices are much more controlled than the technology of a generation ago, and we are both simultaneously trying to imagine how to argue for the idea of 'you don't own it until you can open it' and why that's important, and frankly trying to work out how to fend off the worst consequences of a locked down world. So I think really that's going to be the next big battle.

I remember when I first joined EFF in 2005, one of the first meetings I had was sitting down with the GNU radio folks. So for those of you who don't know GNU radio was an early prototype- still going actually, still actually at the heart of this whole thing - of software-defined radio, which is this idea of rather than having a mobile phone or a TV (...)a wifi on your machine, your Bluetooth, all those things...you could reprogram how a device broadcast and receives data just by giving it another program. We were really, really interested in GNU radio, and in fact we represented them at a European Standards Organization who wanted to introduce DRM into TV broadcasts, because you can't put an anti-copying system into a TV that you can just reprogram. Nowadays – those were like about $1000 in 2005 - Nowadays I play around with a software defined radio that's like 15 bucks and you can plug it into a USB socket. The attempt to control devices like that and chase them out of the market and replace them with systems that you can't control; that are controlled by someone else, be it a corporation like a mobile phone company, or controlled directly by the state is I think one of the key battles of the next ten years, particularly when we all we be using mobile phone devices over mobile phone networks to access the internet infinitely more than we are with our semi open PCS and our semi-open internet service providers these days. I hope that doesn't sound depressing (laughs). You know, I'm excited by the possibilities, that you just have to try and anticipate every objection and get there before society makes these mistakes.

SR: Just bouncing off David's question there and you're response, and I guess this could be a little tangential to a (...) discussion, but given the importance of that sort of thing and I guess the way it links into the (..) maker culture and those sorts of things. Do you think that one of the things that might improve the civil society understanding these sorts of things is to potentially do things like insist that coding is taught in schools as another kind of literacy along with language and mathematics and those sorts of things so we set a fundamental principle of technical understanding? Or is that sort of the thing always going to be the province of a small group?

DO: A small technological priesthood in charge of society (laughs)...No, I love the Idea of reading, writing, arithmetic and algorithms - if you can turn that into an 'R' word - and I do think that even if you're not teaching kids JavaScript, the idea of just burning into people's heads what looping and reiteration are so they realise "oh, this is something that can save me time, or this is something that can spiral out of control" It's part of a sort of well-rounded education. I think sometimes there's a part of geek culture that really relishes the whole idea of doing everything from drafting laws, to building our own furniture, to de-soldering our computers, to writing our own to-do list handlers- I feel guilty even mentioning that one - but, y'know, we can't do it all. We do have to in some way have other people do some parts of things for us. The two provisos on that though, is that I do think that it behoves us to kind of teach politicians and people in power to at least talk about these things. One of the things that I think is incredibly powerful for anyone is to do a sort of 'adopt your MP'. Adopt your senator or congressman or whatever. Go and actually talk to them, because the chances are they're more scared of technology and the possibility of doing something wrong right now than they are wanting to grip the iron fist, and everybody I know who's gone into that discussion has either come out of it enlightened about how the political process works, or is doing endless volunteer work for politicians who then make better laws. So maybe it's not a matter of teaching people to code, but teaching people to respect code, and understand the impact of it. Yeah, I forgot my second point so...

SR: That's awesome! David, would you like to ask another question?

DC: Huh! Sorry? You kind of caught me slightly on the hop there! Yeah, I think that's an idea - I know it's been part of the Electronic Frontier's - both the foundation and its offshoots-the idea that we actually have to teach people a unique form of policy process about technical things, and the consequences that are not obvious to politicians who spend all their time learning about privacy chasing parliamentary procedures (...) I guess, how much do you think teaching not so much code, but we also had this idea of the crypto party, and that idea of teaching people cryptography and all these basic privacy techniques is important, and just a part of that seems

to be at the moment the extraordinary demonisation of...y'know...in the reporting of cases like Snowden and Manning we've seen these issues where you know, the reporter's going "they used a tool called 'worketc' " and everyone who's ever done any system administration, who has ever used a command line, is sort of like going "yeah, of course they did! They moved data on the internet" and there seems to be huge gulf. What can we do to address not just politicians but journalists and all of that?

DO: I'm going to talk sort of a little more personally about this. So I actually spent three years away from EFF for a short while around the time of the Arab spring, and I actually worked with an organisation - a great organisation here in the US - called "the Committee to Protect Journalists", and they asked me to join them because clearly more and more of the people they were trying to protect were internet users; actually bloggers or citizen journalists, and they were also being targeted using malware and pretty sophisticated high tech tools. CPJ (Committee to Protect Journalists) works in the same way as, say, Amnesty International does; it seeks to defend individual cases where people have been imprisoned or attacked for pursuing something that that society sees as a good, a public good, and is indeed essential for an open society: prisoners of conscious, reporters for a free press...What became really apparent to me over those three years, and led to me actually coming back to EFF was that out of those categories of people, who aren't better or worse than anybody else in society, but are actually bell-weathers, kind of canaries in the coal mine for an open society, is now technologists. I'd spent time with people in repressive regimes, and increasingly you have activists, and you have human rights defenders, and you have people reporting on it, but you also have the people building the infrastructure that supports them: people smuggling, and converting and uploading to Youtube videos of bombs in Syria (and) of course the people running the power supplies and wifi in Tahrir Square, People building anti-censorship software in and around China and distributing it. And I have to say, here in the United States many of my friends have been pursued as consequences of what they've done technologically. I think Aaron Schwartz' case is the one that comes to mind. Many of the people, as you say, in the hacker community who were suspected of association with the Wikileaks cases found themselves under the kind of gaze that I think most people don't expect to go on in an open society. So the point here is that technologists are one of these targeted groups exactly as you said, and I think one of the things we could do as activists is to think of them in these terms, and highlight them in the same way as Amnesty International highlight prisoners of conscious. CPJ and Reporters Sans Frontiers and other organisations shows you the roll call of people who've died or faced imprisonment in the pursuit of journalism. I think we have to start doing that for our own people really, and EFF does; we now do 'bloggers under fire'. I'm right now working on two cases: the 'Free Alla' case, which is Alla's a blogger whose currently in prison in Egypt, who was one of the founding bloggers of the Arab spring in that country, and "Free Bassel' Bassel was a Syrian open source developer who's still imprisoned in that country, and I think unfortunately we're just going to see more and more cases like that.

SR: That's fantastic Danny. I like the idea of working to push the supporting of those kinds of people, and also the adopt-a-politician idea, for geeks to adopt a politician. That's really cool.

DC: It's really useful for framing discussion; to think of technologists as a targeted group at the moment. Which as you said is certainly true, especially whistleblowers of any kind are in particular the lemming. It's very common to see people who report security records immediately be attacked.

DO: I think we both recognised both Snowden and Chelsea Manning as people that we could work with or could have been in our community, and I mean not in any sort of political way, but just in the same way that when a journalist sees someone with a camera being dragged away in a war zone they have this moment of going "that could have been me"

SR: Absolutely. On my part, I'm careful that time's really getting away and you're going to have to prepare for the 'Day we fight back'.

DO: Yes! Just all the way through this I've just had little text messages appearing "could you go back to 'Github' and just check it out" (laughs) So we will have to go back to the codeface now.

SR: Well look, it's been absolutely spectacular and you've answered a lot of questions and told us lots of great advice. If I could one last very short question, which is in just two minutes- we've had the adopt a politician thing for geeks, and we've had the civil society organisations to really push and protect technologists those who we think of as our own- but to the general public, If you could say just one thing about internet surveillance, what would that be?

DO: Internet surveillance is mass surveillance, it means it's collecting information on all of us simultaneously, and some of the most private information. If you've ever considered what exactly you're typing into a search engine, or what exactly you're typing into a search engine, or the fact that your phone reports exactly where you are at all times, that data is being collected, and if you feel that you've got nothing to hide, you'd be surprised what people can find if they have all of that information, but I guess the question I'd want you to ask yourself is "think of the most vulnerable person you know, or the person who might risk all kinds of danger if that information was made public or used against them, or just fell into the hands of political opponents" that's the kind of information that's being collected and we don't know where that information is going to end up. We have to stop mass surveillance in order to stop that risk.

SR: Thanks so much Danny that's absolutely terrific, and really concise!

DO: Oh believe me, this is a perfect trial for the next 24 hours. We're looking forward to it. Thanks a lot guys.

SR: awesome. Well, thank you so much, and thank you for running the 'day we fight back' campaign and everything that EFF has done up until now and of course the (...) is absolutely spectacular. Thank you so much for being with us in our (...) as well and we hope to have you back in the future.

DO: Thank you. This was literally my first hour of 'the day we fight back'. I can't think of a better way to start it. Thank you very much.

SR: Well that's so nice and we're so proud to have you. So thank you so much Danny and thanks to David Cake, our vice chair, for attending as well.

DC: Thank you very much Danny, really appreciate it.

SR: Alright, well so that's the end of the broadcast. Thank you very much to everybody who has tuned in. We'll be closing down now. We'll have another EFA speak out in March. EFF will probably have one as well I imagine. We'll copy the site.

DO: This is a great idea. We might create a commons (...)

SR: Go for it!

SR: Alright, thank you very much indeed, and goodbye everybody

DO: Thanks a lot.