01:59:46 Chris Roosenraad: The usual suspects, as it were
01:59:56 Glenn McKnight, Foundation for Building Sustainable Communities: Hi Suzanne. Its a wet late Winter day here in Oshawa, Ontario Canada, perfect for this type of thing to do
02:00:01 Holly Raiche: The session is started already'
02:00:04 Maureen Hilyard (ALAC): Technical glitches down under, unfortunately
02:00:13 Rod Rasmussen: Apologies for being a couple minutes late!
02:00:29 Lucien Castex: Hi all
02:01:05 Matthias M. Hudobnik: hello everybody :)
02:01:21 Javier Rúa-Jovet: hello to all!
02:01:21 sergio salinas porto LACRALO: please link audiostreaming in spanish
02:01:34 Lucien Castex: http://stream.icann.org:8000/cun67-costamaya1-es.m3u
02:01:55 sergio salinas porto LACRALO: thanks
02:02:15 claudia.ruiz: Piste audio en français (http://stream.icann.org:8000/cun67-costamaya1-fr.m3u)

Transmisión de audio en español (http://stream.icann.org:8000/cun67-costamaya1-es.m3u)
02:02:36 claudia.ruiz: Paul is not speaking
02:02:45 claudia.ruiz: Do have more than 1 call open
02:06:38 Carlos Raul Gutierrez: Holly !!!!!
02:06:46 Humberto Carrasco: Hello everybody
02:07:45 Olaf Kolkman: I hear it in the faint background too...
02:07:51 Korry Luke: Same here
02:08:00 Julie Hammer: I'm getting a distant voice in my headset too.
02:08:25 Rod Rasmussen: Can we get everyone muted except for the speaker?
02:09:52 Glenn McKnight, Foundation for Building Sustainable Communities: Here is the link as a ebook to Pauls presentation
02:09:53 Glenn McKnight, Foundation for Building Sustainable Communities: http://online.fliphtml5.com/gnel/hsyj/
02:10:00 Jonathan Zuck: "Mediumly brief" Gonna use that!
02:10:14 Paul Hoffman: https://www.icann.org/en/system/files/files/octo-003-en.pdf
02:11:54 Glenn McKnight, Foundation for Building Sustainable Communities: Here is a ebook version of above
02:11:55 Glenn McKnight, Foundation for Building Sustainable Communities: http://online.fliphtml5.com/gnel/duqz/
02:12:18 Ricardo Holmquist: anyone else had problems with Firefox entering Zoom
02:12:37 Ricardo Holmquist: it worked fine 6 hours ago in another ICANN67 meeting
02:12:46 Ricardo Holmquist: now I had to change to Chrome
02:13:07 Ricardo Holmquist: Firefox didn't want to start
02:13:08 Vittorio Bertola: I'm on Firefox and launching the Zoom app worked fine.
02:13:22 Satish Babu: Worked for me too...
02:13:23 Ricardo Holmquist: grazie Vittorio
02:13:23 Dev Anand Teelucksingh: No problem with Firefox - but then I have it configured to open the native Zoom client (Windows)

02:13:26 Judith Hellerstein: i have no issues but I am using the zoom app
02:13:57 Judith Hellerstein: the same with me when i use my computer
02:14:09 Ricardo Holmquist: didn't launch the app, tried to use on windows, but did not start the audio on the computer
02:14:13 Rod Rasmussen: Firefox worked for me - launches the zoom app automagically.
02:15:02 Judith Hellerstein: you can open up zoom and put the meeting I'd in the app
02:15:02 Ricardo Holmquist: @Rod, that is a great start, never here of automagically ;)
02:15:17 sergio salinas porto LACRALO: I can't connect to the Spanish channel, has anyone had problems?
02:15:42 Ricardo Holmquist: *hear
02:16:10 Jonathan Zuck: https://www.dictionary.com/browse/doh?s=t
02:16:26 Yesim Nazlar: @Sergio - we have live streaming only for ES & FR. No ADIGO channels, fyi.
02:17:04 Holly Raiche: Could I have a dial out please
02:17:12 Yesim Nazlar: sure Holly
02:17:40 Thomas de Haan European Commission: Question (for later) why did browser providers choose DoH and not DoT?
02:18:18 claudia.ruiz: @Sergio I just tried the live streaming and was able to connect
02:18:20 sergio salinas porto LACRALO: yes yesim
02:18:56 Barry Leiba: The web browsers already have all the network stuff built into them to handle HTTP connectoins.
02:20:19 Jonathan Zuck: I don't understand why encryption would increase "assurance"
02:20:39 Jonathan Zuck: Oh like man in the middle attacks and such
02:20:51 Jacqueline Morris: <question> Will this presentation be available for later viewing and linking for my ALS members who are unable to attend right now?<question>
02:20:51 Thomas de Haan European Commission: @jonathan: because the resolver is validated
02:21:23 Jonathan Zuck: Can't authentication occur with out encryption?
02:21:48 Glenn McKnight, Foundation for Building Sustainable Communities: Ebook on RFC http://online.fliphtml5.com/gnel/ohtg/
02:21:56 Barrack Otieno: @Thomas, maybe @JZ is looking at it from a Social Engineering angle?
02:21:57 Heidi Ullrich: @Jacueline, the presentation is hyper-linked to the agenda page: https://community.icann.org/display/atlarge/At-Large+Meetings+-+Tuesday%2C+10+March+2020
02:22:43 Dave Kisssoondoyal - ALAC: What is the rationale for encrypting only PARTLY the session i.e between the DNS stub client and the DNS recursive Server.. Why NOT the sessions between the DNS recursive servers and DNS authoritative servers? Is it not partial encryption?
02:23:13 Barrack Otieno: Last point is quite interesting wrt global Cybesecurity efforts

02:23:21 Korry Luke: If you did that, you'd have to get all the different authoritative servers to support
02:23:34 Korry Luke: Which is quite difficult at scale and given DNS's history/age
02:23:48 Gangesh Varma: <question> what has been the responses from law enforcement agencies across different jurisdictions on DoT and DoH? <question>
02:24:28 Joanna Kulesza: < Q > How does the encrypted DNS requirement in local policy fit into the discussion on internet fragmentation? <Q>
02:25:07 Roberto: @Joanna - good question
02:25:08 Alyssa Moore (CIRA): @ Dave K, as mentioned at the beginning of the presentation, the 'risk' to privacy is diminished the further away from the end user in the chain you are. And then every authoritative operator for each zone would have to support DoH.
02:25:13 Jonathan Zuck: At least in theory, it shouldn't impact fragmentation.
02:25:21 Holly Raiche: I am using firefox in Australia and was told about this
02:25:43 Juhani Juselius: Does encryption replace DNSSEC to some extent?
02:26:03 gih: No it does not
02:26:09 Barry Leiba: Not at all. DNSSEC is about authenticating response data, and this is about encryption.
02:26:20 Sarah Wyld: Juhani - I don't think so. DNSSEC makes sure you really are getting the resource you think you're getting, but not that the request/response is encrypted
02:26:22 Gabriel (PSWG): <Q> Does the "unwanted centralization" lead to an increased risk of a large DDoS attack targeting those DNS servers, possibly leading to a large scale WWW outage much like the Oct 2016 Dyn DNS attack? </Q>
02:26:24 john.crain: @ Juhani, No. DNSSEC is more about the integrity of the data
02:26:40 Satish Babu: <Q>Given that the response from the resolver is encrypted and cannot be intercepted, do we still require DNSSEC if we have DOT/DOH</Q>
02:26:50 Dave Kisssoondoyal - ALAC: Thanks @Korry and @Alyssa
02:26:53 gih: channel encryption means that noone else can see what is going on in the channel, but the object being passed to you can still be a fake
02:27:00 Alyssa Moore (CIRA): @Joanna and @Jonathan: Fragmentation exists in the sense that you could circumvent the DNS filtering of your enterprise or ISP's recursive resolver by using a DoH resolver, thereby seeing "a different web"
02:27:09 gih: DNSSEC protects the integrity of the object
02:27:56 Roberto: @Alyssa - that is exactly my worry, we can have a sort of a set of "private" internets
02:28:05 Glenn McKnight, Foundation for Building Sustainable Communities: Link to document?
02:28:15 Barrack Otieno: Was just reading about the Mozzila Containers
02:28:21 Barrack Otieno: good initiative
02:28:30 David Huberman: @Glenn: https://www.icann.org/en/system/files/files/octo-003-en.pdf
02:28:31 Joanna Kulesza: Interesting @Alyssa - my initial understanding was that it would allow to limit the number of queries asked and effectively responses presented to an every day end user in a specific jurisdiction. Guess it works both ways?
02:28:52 Jonathan Zuck: That was Holly getting exited about Windows DOH!

02:28:57 Peter Koch: I'm a bit confused that people seem to believe that 'filtering' was an integral part of the architecture. It's a huge distraction, really.
02:29:00 liz Orembo: what's the difference btn dnsec and encryption? doesn't encryption also protect web/data integrity?
02:29:11 Roberto: @Joanna & @Alyssa - a sort of "virtual fragmentation"
02:29:33 Dev Anand Teelucksingh: Microsoft's announcement re: DNS over HTTPS : https://techcommunity.microsoft.com/t5/networking-blog/windows-will-improve-user-privacy-with-dns-over-https/ba-p/1014229
02:29:33 Satish Babu: <Q>Why would resolvers like Cloudflare provide DOT/DOH service gratis? Is there a revenue model somewhere?</Q>
02:29:37 Gangesh Varma: <Q> On unwanted centralisation, do you see this becoming a geographic centralisation of resolution ? in a sense do you think countries might require resolution within their borders? is this technically feasible? <Q> sorry if this is a technically absurd question but just curious about how national governments could /would respond depending on their interests
02:29:40 nigel hickson: @Paul - Thanks for such an excellent overview and update
02:29:44 Thomas de Haan European Commission: Question: status of Chrome? the l;ast thing we heard is deployment in March 2020!
02:29:45 Justin Mack (MarkMonitor): Network operators can setup a "canary domain" to prevent Firefox from using DoH and choose the local resolver instead.
02:29:57 Paul Hoffman: https://www.icann.org/en/system/files/files/octo-003-en.pdf
02:30:33 Glenn McKnight, Foundation for Building Sustainable Communities: This is the paper that I converted to an ebook
02:30:34 Glenn McKnight, Foundation for Building Sustainable Communities: http://online.fliphtml5.com/gnel/duqz/
02:30:50 Alyssa Moore (CIRA): +1 to @Peter
02:31:00 Joanna Kulesza: +1 @Roberto, also a #plug for tomorrow's session: we'll discuss fragmentation tomorrow but this presentation feeds directly into it. https://community.icann.org/display/atlarge/At-Large+Meetings+-+Wednesday%2C+11+March+2020 Happy to keep this conversation flowing
02:31:18 Glenn McKnight, Foundation for Building Sustainable Communities: breaking up
02:31:18 Justin Mack (MarkMonitor): Canary domain for Firefox: https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet
02:31:29 Korry Luke: I'm having trouble hearing the current speaker
02:32:13 Peter Koch: @Satish: there can be a certain advantage for a CDN provider that also runs a 'centralized' resolver, at least compared to competitors who don't
02:32:31 Korry Luke: https://www.chromium.org/developers/dns-over-https
02:32:42 Korry Luke: Here's Chromium's policy on DoH
02:33:07 Satish Babu: Thanks @Peter.
02:34:22 Dave Kisssoondoyal - ALAC: please read out
02:35:09 Suzanne Woolf: @Peter that hidden centralization means more data in fewer hands. Not that Cloudflare would sell it, they've committed that they won't, but big resolver operators see a large cross-section of internet activity and can learn a lot from it in

aggregated form. I want to emphasize this doesn't have to involve privacy violations or the use of potential PII to be valuable.
02:36:31 Sarah Wyld: +1 Suzanne - this is a really important concern with centralization of DNS resolution
02:37:11 Thomas de Haan European Commission: @korry Thanks!
02:37:18 Jonathan Zuck: Wouldn't that centralization only be temporary as more resolvers can handle encryption?
02:37:31 Peter Koch: @suz the advantage I referred to is for CDNs using 'DNS tricks' and therefore catching two birds with one stone running the resolver (and essentially taking the other bird outr of the game for their competitors)
02:38:13 Vittorio Bertola: @Jonathan - not if the browser (of which there are not that many with significant market share) decides to send all their users' queries to a specific single resolver or a few.
02:38:37 Suzanne Woolf: @Jonathan there still has to be a resolver that sees unencrypted queries so it can answer them. The encryption ewe've been discussing protects the data in flight, but it has to be decrypted at the resolver in order for DNS query-response to happen.
02:38:57 Suzanne Woolf: @Peter also a valid concern IMO
02:39:17 Dave Kisssoondoyal - ALAC: Thanks for answering to my question
02:40:06 Jonathan Zuck: @Suzanne. Thanks. I get that but as the number of available servers goes up, so will the distribution of queries, no?
02:41:22 Vittorio Bertola: @Jonathan - you can have a million DoH resolvers but if a browser decides to send all the traffic to one, it will still be that one that gets all the data.
02:41:35 Satish Babu: <Q>From a scalability perspective, doesn't DOH create a single point of failure? Is there a fallback arrangement?</Q>
02:42:13 Suzanne Woolf: @Jonathan +1 to Vittorio on that, we need both lots of resolvers and good, easy ways to diversify which ones are used
02:42:17 Edmon: but in part its because the browsers are not actively displaying the dnssec check
02:42:44 Edmon: right... the same could be deployed by browser for dnssec?
02:42:57 Justin Mack (MarkMonitor): <question> How does DoT/DoH affect geographical-based answers from authoritative servers when the recursive resolver is centralized? Will users potentially get IP addresses that are "farther away" than they might have when using a local resolver? </question>
02:43:03 Thomas de Haan European Commission: QUESTION Does anyone know more about progress on opening upof DoH resolving to other parties accotding to agreed guidelines (EDDI etc)? Paul told about network operators being more active now
02:43:04 Suzanne Woolf: that's an active area of standards development in fact—allowing applications to obtain a list of trustable resolvers and apply a policy to choosing among them
02:43:54 Judith Hellerstein: hand up
02:44:04 Juhani Juselius: So a key think against centralization is users' freedom to choose DoH resolver?

02:44:16 nigel hickson: Good evening; if possible could we briefly touch on the issue of "user choice" concerening where their DNS queries go? I recall this was touched on at a previous session and how feasible / practical it was?
02:44:33 john.crain: The LE question is maybe a question to PSWG members
02:45:33 Gangesh Varma: I agree it's for law enforcement to answer, but was just asking to get a sense what stakeholders have heard. given that, like someone mentioned some countries require this type of dns encryption for users /citizens.
02:45:49 Gangesh Varma: thanks John. will follow up with GAC :)
02:45:54 Jacqueline Morris: There's the idea that users will choose resolvers that they trust. However, how many end users will really do that? And how many will assume that any web traffic issues are the fault of the ISP, not the browser, or a choice of resolver that was made by an app, or by the person who set up their computer?
02:46:03 Dawn Shackleton Mercer: Comment: DNS traffic becomes managed by the resolvers which in the main would be big tech companies not ISPs who in many countries are regulated. I personally would prefer my data even non-personal data managed by a regulated organisation than an unregulated org. Normal users wouldn't even realise this. Where is the transparency from these Tech companies and how do users know that they can be trusted to have the interests of the user at heart. Tech companies are doing this for commercial reasons.
02:46:18 john.crain: So I work a lot with LE and will say that they have demonstrated nervousness about the ability of “bad people” to use encryption to hide.
02:47:17 john.crain: Also the issue of “breaking” protective filtering systems raises concerns in that area.. but once again the questions should really go to LE folks
02:47:54 Gangesh Varma: ah. expected, are there talks about how they can work around/work with it? can take this offline and directed at LE /GAC members
02:48:08 Vittorio Bertola: @Jacqueline: This is indeed something that was not mentioned in the presentation; one of the issues is, if the application chooses a DoH resolver different from the ISP’s and then that resolver doesn’t work, who does the user call? They will still call the ISP and ask why “the Internet is not working”, but the ISP won’t be able to help them.
02:49:00 Joanna Kulesza: <Q> granted the time, could we get comments on this case here: https://www.wired.com/story/iran-dns-hijacking/ <Q> <headline: A Worldwide Hacking Spree Uses DNS Trickery to Nab Data; Security researchers suspect that Iran has spent the last two years pilfering data from telecoms, governments, and more.>
02:49:03 Jacqueline Morris: @Vitorio exactly. That's going to be a major end-user issue, I predict.
02:49:29 john.crain: @jaqueline and @ Vittorio absolutely real issues
02:49:56 Peter Koch: LE comes in different flavors; to the extent that law or regulation is enforced by ‘government enhanced DNS responses’, circumvention has always been possible (remember 8.8.8.8 painted on walls); to that extent, DoH makes access to circumvention easier (an Emperor’s Clothes issue); however, at the end of the day, the regulatory surface will shrink, i.e. LE needs to focus on lesser resolver operators (thanks centraliziation)
02:50:07 Justin Mack (MarkMonitor): Won't ISPs run their own DoH resolvers? (Users could still override.)
02:50:40 Jacqueline Morris: @Justin That is assuming a lot of the end user

02:50:49 Vittorio Bertola: @Justin: Yes, many big ISPs already have public experimental DoH resolvers. But again, this does not change anything if the browser is not willing to use them.
02:50:53 john.crain: @Peter I see those discussions going on. Like all of these issues it's always a mixed bag
02:51:08 Vittorio Bertola: (I will also note that Chrome and Windows *are* willing to use them.)
02:51:42 Suzanne Woolf: @John the SSAC paper discusses in detail that a lot of the costs and benefits of Do* (esp. DoH) depend on your perspective
02:52:18 Suzanne Woolf: One tussle is who users trust to protect them on the internet, or who's best equipped, application writers, ISPs, or someone else
02:52:54 john.crain: @Suzanne yes "Trust" is a big question here. Who do YOU trust and what do you mean by that
02:53:22 Vittorio Bertola: In the end, you would expect the user to pick who they trust, each user having a different view. But then, the problem becomes how can users make informed choices.
02:53:54 Sara: +1 with Vittorio.
02:53:58 Roberto: +1 Alan about trust - who do you trust
02:54:08 Jacqueline Morris: @Vittorio Exactly. There's a huge educational requirement there
02:54:17 Suzanne Woolf: @vittorio in practice this comes down to choosing your "trust proxy". My friends at Mozilla feel strongly they are better guardians of users' interests than ISPs; my friends at ISPs often feel otherwise
02:54:18 Roberto: +1 Vittorio
02:54:20 Lucien Castex: +1
02:54:32 Jonathan Zuck: As there is on so many security related issues, eh?
02:55:13 Suzanne Woolf: @Jonathan this is how we ended up organizing the SSAC paper around the perspectives of different actors in the ecosystem
02:55:15 Roberto: @Suzanne - but at the end of the day the question is whether the user trusts more the ISP or the browser
02:55:34 Joanna Kulesza: So there is no technical solution for ensuring trust? ;)
02:55:37 Suzanne Woolf: @Roberto I think that risks over-simplification, looking forward to your views of the SSAC paper
02:55:48 Jacqueline Morris: @suzanne There's also a cultural and geographic issue as to who is best suited to manage the under interest with respect to this
02:56:11 Jacqueline Morris: *user* interest not *Under*
02:56:20 Roberto: @Suzanne - will surely read it carefully
02:56:30 Vittorio Bertola: @Suzanne we actually miss a way for the user to make that choice and communicate it to all the parties. You could theoretically configure a "trusted party" that is authorized to configure all your apps for you. But nothing like that exists (and also, securing it looks hard).
02:57:10 Suzanne Woolf: @jacquline we felt quite strongly there are many such issues, and we tried to provide some perspective on sorting through them….we wanted at the beginning to have a few simple, clear recommendations, and ultimately coudn't.

02:57:26 Barry Leiba: I like that: “We are the ultimate you."
02:57:54 Sivasubramanian Muthusamy: Is it technically feasible for a certain part of DNS, say a ccTLD, to require (and provide assistance to Registrants) ALL domain names in that space to be on DoH?
02:57:55 Judith Hellerstein: i have been waiting a while so i guess I am next
02:58:15 Alan Greenberg: You are Judith (in the hands up queue)
02:58:25 Suzanne Woolf: It took a lot of work to get to a consensus version of the paper, because of the complexities we’ve been grappling with in this session (and some others)
02:58:30 Justin Mack (MarkMonitor): If the authoritative resolvers all supported encryption, users could run their own resolvers, both bypassing their ISP and a centralized resolver. (Trust is then with the authoritative resolver, where it should be.)
02:58:30 claudia.ruiz: @Judith yes, you are next
03:00:05 Sivasubramanian Muthusamy: (expanded) Is it technically feasible for a certain part of DNS, say a ccTLD, to require (and provide assistance to Registrants) ALL domain names in that space to be on DoH? I.e. DoH by default across the TLD space...
03:00:09 Jacqueline Morris: @Justin how will this be a simple, easy thing for end-users, who generally just install a browser with default settings and start to browse, to implement?
03:00:53 Vittorio Bertola: @Justin: That could have pretty bad performance due to lack of caching and slow connectivity (not to mention all filtering-related issues).
03:01:13 Peter Koch: @SM DoH/DoT are controlled by the consumer, not the publisher
03:01:14 Jacqueline Morris: @Justin I'm thinking about my 81 year old father, or my 72 year old aunt...
03:01:57 Sivasubramanian Muthusamy: @peter understood. The question remains.
03:03:47 Justin Mack (MarkMonitor): @Jacqueline: For example on my linux machine, I run "unbound" - a recursive resolver that only contacts authoritative servers. If the authoritative servers all supported encryption, then all my DNS queries would be private. If browsers and operating systems are implementing DoH stub resolvers, they could just as easily implement DoH recursive resolvers. (Yes, caching would only be local to each device, putting more load on authoritative servers, but DNS is relatively cheap, right?)
03:04:17 Rudi Daniel: Comment: if browsers prefer doh and i think content delivery may prefer that, and leave dot behind, ...then this highlights a new trust issue at what could become a centralized (some say more robust) resolver zone. but there seem to be a need to know the difference between the two deployments at the u
03:04:36 Suzanne Woolf: @Justin the TLD data is separate from the configuration of the server used to hand it to users. Whether DoH is supported is determined by the server configuration, not the data. And that’s hard for end users to determine
03:04:57 Sivasubramanian Muthusamy: @Peter The question is about a scenario where the (cc) TLD is in a position to 'inspire' all Registrants and prospects to embrace DoH, recommend hosting services etc.
03:05:09 Peter Koch: @SM the registrant isn’t “on” DoH; what is beinhg discussed is running authoritative DNS servers that offer encryption, most likely with DoT rather than DoH then and at least initially in an opportunistic fashion, i.e., without identifying the end point.
03:07:25 Rudi Daniel: Comment: if browsers prefer doh and i think content delivery may prefer that, and leave dot behind, ...then this highlights a new trust issue at what could

become a centralized (some say more robust) resolver zone. but there seem to be a need to know the difference between the two deployments at the various kinds of users.
03:08:31 Jonathan Zuck: Exactly, ALL the time!
03:09:52 Alan Greenberg: If we are looking for clarity and simplistic answers, we will not be happy!
03:10:41 Heidi Ullrich: Time check - 15 mins remaining in this session.
03:10:55 Edmon: for At-Large, I think it is relevant to think through whether the user should have a bit more say/control over this (and advocate for it) than in the past where such decisions are made on user's behalf as paul just mentioned
03:11:38 Justine Chew: +1 Edmon, and whether users have a reasonable understanding of the impact of their choices
03:12:22 Edmon: we have to understand that the new generation of users are more tech savvy
03:12:25 Edmon: and literate
03:12:55 Edmon: unlike the last 20 years with expansion to less tech literate users
03:12:56 Gangesh Varma: +1 Edmon
03:13:11 Vittorio Bertola: +1 for Edmon, and at least you have to ensure that smart users always have the option for full choice, even if you accept that “basic” users might trust someone else to choose on their behalf
03:13:27 Vittorio Bertola: That would be a good focus for the ALAC.
03:13:33 Edmon: +1 vittorio
03:13:52 Gangesh Varma: and it's good to have these discussions making it part of the 'digital literacy' discourse
03:14:08 Justine Chew: I don't think that is an assumption we should make. I have come across many younger users who I don't consider as tech savvy at all. Just saying.
03:14:17 Hadia Elminiawi: @Edmon this does not necessarily apply to the next billion users whom we are looking forward to have
03:14:33 Satish Babu: It's a mixed bag...agree with @Justine
03:15:46 Gangesh Varma: important that next billion users may also be exposed to these deliberations even if they don't fully engage with it or understand it. would definitely trickle down to aspects that matter to them and make choices when they further deepen their use of the internet
03:15:49 Suzanne Woolf: @hadia +1, and newer devices often provide users with less choice, and less visibility into the choices the vendor/system is making for them.
03:16:13 Suzanne Woolf: Walled gardens of various kinds, by default
03:16:43 Jonathan Zuck: Good point, @Judith! I think this generation are more used to controllers than keyboards. I was just just discussing with a parent how their kid should still go to a typing class.
03:16:55 Suzanne Woolf: to me that’s not the open Internet— people may choose walled gardens sometimes or for some reasons, but I want to keep other possible ways of having the Internet open too!
03:17:14 Vittorio Bertola: @Suzanne: That looks like a problem that needs non-technical direction, i.e. regulation! Fortunately we have the European Commission here :-) (sorry Thomas)

03:17:36 Vittorio Bertola: But it'd be nice if the industry agreed on fair rules by itself
03:17:44 Jonathan Zuck: In a rather…um, lawless, country…
03:18:03 Maureen Hilyard (ALAC): I wouldn't go there. JZ
03:18:21 paf: What Thomas talks about is a situation that already today is accepted in Europe, that the access provider by blocking certain domain names in their full service resolver is living up to whatever requirements the courts require the access provider to do. Objecting or questioning that view of the law enforcement and courts is something different than answering the question of Thomas.
03:19:36 Heidi Ullrich: Timecheck - 7 mins
03:19:58 Jonathan Zuck: wow, haven't heard that name in a while. Lessig is the king of effective powerpoint.
03:20:34 Suzanne Woolf: I'm kind of a fan of architecture & protocols as norms. I think the technologists lost some time and potential influence by insisting on the framing of tech as policy-neutral even when it wasn't. (I can say that as a technologist who's always had a secret policy habit.)
03:20:54 Suzanne Woolf: @paf thanks
03:22:09 Hadia Elminiawi: @Suzanne +1 technology is not policy neutral
03:22:11 Vittorio Bertola: @Suzanne: If you go down that path, you will find people asking how can the technical lawmakers be held accountable to citizens the way the traditional, non-technical lawmakers are :-)
03:23:21 paf: For me the problem is that the access provider that moves IP packets is expected to act on transactions (content) in a completely different layer in the value chain. From a pure technical standpoint, that is completely nuts. From many other views, it makes complete sense :-)
03:23:23 Suzanne Woolf: @vittorio I know
03:23:45 Heidi Ullrich: We can add that to the agenda
03:23:55 Kathy Schnitt: https://docs.google.com/presentation/d/1tT3S5ppZ7AJTC_Mo-XpJZJ8P9EBuloDnk1RBtqxt74A/edit#slide=id.g7e6fce402e_0_4
03:24:00 Suzanne Woolf: And I think there are different kinds of accountability, with different applicability, but that's a better discussion for the next in-person meeting with adult beverages :-)
03:24:04 Jonathan Zuck: The "policy" nature of technology is really coming to the forefront with China's standards body infiltration…or "robust" participation!
03:24:04 Heidi Ullrich: Thanks, Kathy!
03:24:15 Gangesh Varma: thank you all. this has been a fantastic discussion and lots of learning. look forward to reading the resources shared.
03:24:17 john.crain: The solution that MSFT says that in the solution it is implementing they will respect the local DNS configuration choices. It's an interesting approach and has different issues
03:24:19 john.crain: https://techcommunity.microsoft.com/t5/networking-blog/windows-will-improve-user-privacy-with-dns-over-https/ba-p/1014229
03:24:23 Dave Kisssoondoyal - ALAC: Thanks a lot for the panelists for the presentation and for answering our questions
03:24:29 Satish Babu: Thanks for great session!

03:24:30 Judith Hellerstein: yes. very interesting session
03:24:34 Jonathan Zuck: Great session everyone!
03:24:36 Olivier MJ Crepin-Leblond: Another excellent session - thank you!
03:24:38 Maureen Hilyard (ALAC): Thank you everyone for a great session with great presentations, interactions and interventions.
03:24:41 Ricardo Holmquist: thanks Holly nice session
03:24:42 paf: Very very well done! Including everyone asking questions!
03:24:42 Korry Luke: Thanks for a great session! Extremely informative
03:24:45 Justin Mack (MarkMonitor): Thanks everyone!
03:24:49 Andrew McConachie: https://docs.google.com/presentation/d/1tT3S5ppZ7AJTC_Mo-XpJZJ8P9EBuloDnk1RBtqxt74A/edit#slide=id.g7e6fce402e_0_4
03:24:50 Dev Anand Teelucksingh: Thanks all
03:24:51 Glenn McKnight, Foundation for Building Sustainable Communities: Thanks bye
03:24:51 Hadia Elminiawi: Thank you
03:24:51 nigel hickson: Thank you; really excellent.
03:24:51 Matthias M. Hudobnik: very interesting session
03:24:52 Jaap Akkerhuis: bye all
03:24:52 Maureen Hilyard (ALAC): Thanks Holly. great work
03:24:54 Andrew McConachie: Presentation on SSAC paper
03:24:54 Jaewon Son: thank you for the great presentation and session
03:24:54 paf: bye
03:24:56 Andrew McConachie: https://docs.google.com/presentation/d/1tT3S5ppZ7AJTC_Mo-XpJZJ8P9EBuloDnk1RBtqxt74A/edit#slide=id.g7e6fce402e_0_4
03:24:57 Vittorio Bertola: Thanks everyone